时间反转OFDM系统中增强安全性能的功率分配与人工噪声设计

雷维嘉[1,2],毕文佳[1,2*],雷宏江[1,2],唐 宏[1,2]
(1. 重庆邮电大学通信与信息工程学院,重庆 400065;2. 重庆邮电大学移动通信技术重庆市重点实验室,重庆 400065)

摘 要: 时间反转技术特有的时空聚焦特性使其具有抗窃听能力.本文对提高时间反转正交频分复用系统安全性能的优化方案进行研究.首先,通过应用时间反转预滤波的时空聚焦特性来提高合法接收端相对于窃听端的信号强度;然后,以最大化保密速率为目标对子载波的功率分配进行优化.为进一步提升系统保密传输能力,利用循环前缀提供的自由度实现零空间人工噪声,在对窃听端形成有效干扰的同时,不对合法接收端造成影响.通过对子载波功率分配和人工噪声协方差阵进行联合优化,最大化系统的保密传输速率.仿真结果表明,所提优化方案能显著提高系统的保密速率.

关键词: 物理层安全;正交频分复用;时间反转;功率分配;人工噪声
基金项目: 国家自然科学基金(No.61971080)
中图分类号: TN918 **文献标识码:** A **文章编号:** 0372-2112(2024)05-1570-12
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220725

Power Allocation and Artificial Noise Design of Time-Reversal OFDM System to Enhance Security Performance

LEI Wei-jia[1,2], BI Wen-jia[1,2*], LEI Hong-jiang[1,2], TANG Hong[1,2]
(1. *School of Communication and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*;
2. *Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: Time reversal technology has natural anti-eavesdropping capability due to its unique spatial and temporal focusing capability. In this paper, an optimization scheme to improve the security performance of time reversal OFDM system is studied. Firstly, the temporal and spatial focusing characteristics of time reversal pre-filtering are applied to improve the signal strength of the legitimate receiver relative to the eavesdropper, and then the power of the subcarriers is optimized to maximize the security rate. In order to further improve the secure capability of the system, the zero-space artificial noise is realized by employing the degree of freedom provided by the circular prefix, which can effectively interfere with the eavesdropper, while does not interfere with the legitimate receiver. Then, the subcarrier power and the covariance matrix of the artificial noise are optimized to maximize the security transmission rate. Simulation results show that the proposed scheme can significantly promote the security rate of the system.

Key words: physical layer security; orthogonal frequency division multiplexing; time reversal; power allocation; artificial noise
Foundation Item(s): National Natural Science Foundation of China (No.61971080)

收稿日期:2022-06-24;修回日期:2022-11-17;责任编辑:孙瑶
*通讯作者:毕文佳

1 引言

信息传输的安全是通信领域研究的重点问题之一. 由于传输媒介的开放性、无线信道的广播特性以及网络结构的不稳定性等,无线通信系统很容易受到攻击,信息传输的可靠性和安全性面临着重大的挑战. 物理层安全是一种不依赖上层加密的防窃听技术,是利用无线信道的随机性和多样性,通过采用信号处理、编码等技术在物理层上实现信息的安全传输[1]. 实现物理层安全的主要方法是通过多天线、波束赋形、人工噪声(Artificial Noise,AN)和其他信号处理技术,增大主信道和窃听信道的质量差异,再通过安全信道编码,在合法接收端能可靠接收信息的同时防止窃听,实现信息的保密传输. 很多增强物理层安全性能的方案都是基于多天线系统提供的空间自由度[2],通过采用波束赋形将信号指向合法接收端、将零陷对准窃听端来增强合法接收端相对于窃听端接收信号的质量优势. 人工噪声是一种通过主动干扰的方式增强物理层安全性能的技术,常与多天线技术联合使用. 利用多个发射天线提供的空间自由度,通过波束赋形控制人工噪声的发射方向,对窃听者形成有效的干扰,即使可能对合法接收端造成轻微的影响,也能显著提高系统保密传输能力[3~5]. 文献[4]提出了联合使用波束赋形和人工噪声的物理层安全方案,通过利用波束赋形将发送信号指向合法接收端,同时将人工噪声置于合法信道的零空间中,在不对合法接收端形成干扰的同时,对潜在的窃听者形成了有效的干扰,提高了系统保密容量. 文献[5]针对存在多个窃听者的多输入单输出(Multiple-Input Single-Output,MISO)系统,研究了在人工噪声辅助下的波束赋形设计的优化问题,在保密中断概率的约束下最大化系统的保密速率. 该文献的研究结果表明人工噪声不仅可以干扰窃听节点,还能在特定情况下改善合法用户的性能. 波束赋形和人工噪声是增强物理层安全的重要方法,但需要依靠多天线系统的空间自由度才能获得较好的效果. 在某些受到体积、功耗等限制的节点上,由于只能配备单根天线,物理层安全传输性能的提升受到了很大程度的制约.

时间反转(Time Reversal,TR)技术利用无线信道的多径传输实现信号在时域和空域上的能量聚焦,能以很低的系统复杂度提高接收信号的强度. TR传输系统中,信号在送入信道之前先要经过TR滤波器滤波,TR预滤波器的脉冲响应为信道脉冲响应(Channel Impulse Response,CIR)的时间反转共轭,这使多径信道成为发送信号的匹配滤波器. 经过TR滤波和多径信道传输后的信号在特定时刻会在目标接收机处出现明显的能量峰值,而在偏离峰值的时刻能量有明显的衰减. 文献[6]验证了TR的时空聚焦特性,证明了TR预处理能在提高目标接收机信号强度的同时,降低在非目标接收机处的能量泄露. TR技术的空时聚焦特性使其非常适合应用到物理层安全传输系统中. 文献[7]研究了TR多输入多输出(Multiple-Input Multiple-Output,MIMO)系统的保密传输性能,结果表明TR传输技术能显著提高系统的保密容量,通过TR技术与人工噪声技术的结合,在单发送天线下也能有效地提高系统物理层安全性能. 文献[8]研究了TR多用户下行多址系统中,针对窃听信道状态信息(Channel State Information,CSI)是否已知两种情况下的安全传输方案,通过采用TR预处理利用信道中的多径,获得类似于多发送天线的效果. 当窃听信道CSI未知时,通过TR预处理获得全向辐射但位于合法信道零空间中的人工噪声,进一步在每个用户信干噪比(Signal to Interference plus Noise Ratio,SINR)目标约束下优化信息信号的TR预滤波器,最小化发送信号所需的功率,从而最大化人工噪声功率,最小化窃听速率;当窃听信道CSI已知时,则联合优化信息信号的TR预滤波器和人工噪声的协方差阵以最大化保密速率. 文献[9]研究了联合人工噪声和TR技术提高系统安全传输性能的方案,针对窃听信道CSI是否已知两种条件,提出了3种联合优化TR预滤波器和人工噪声的安全传输方案,并通过仿真验证了所提方案的安全性能优于采用常规匹配预滤波时的方案.

正交频分复用(Orthogonal Frequency Division Multiplexing,OFDM)是第4代、第5代移动通信系统中的关键技术,也将是新一代移动通信系统的关键技术. TR的空时聚焦效应同样对提高OFDM系统的性能有益. 文献[10]研究了应用TR技术来缩短OFDM系统的循环前缀(Cyclic Prefix,CP)长度、提高系统频谱效率的问题. 在CP长度不足的情况下,文献[10]应用TR的时空聚焦特性减轻符号间干扰(Inter Symbol Interference,ISI)和载波间干扰(Inter Carrier Interference,ICI). 文献[11]研究了大规模MIMO OFDM系统中天线数量与SINR间的关系,理论分析和仿真结果表明,在没有CP的情况下,即使天线数无限增长,ISI和ICI也不会持续下降,但在增加TR预滤波后,ISI和ICI则能随天线数的增加而趋近于零. 对于OFDM系统,在时域上进行的TR预处理也可以在频域上实现. 文献[12]提出了一种在MISO OFDM通信系统中进行频域TR预编码的方法,推导了接收信号的均方根误差的闭式表达式,分析了均方根误差与不同速率回退因子(Rate Back-off Factor,BOF)之间的关系. 仿真结果表明,增加BOF或天线

数量可以提高系统的信噪比(Signal to Noise Ratio, SNR)增益. OFDM系统中的物理层安全也是学术界研究的重点问题之一. 功率分配、波束成形、人工噪声、区别信道估计等技术是研究较多的、增强OFDM系统的保密传输能力的技术. 文献[13]提出了一种通过优化设计OFDM的波形增强物理层安全的方法,并通过合法双方共享的密钥随机调整CP时长从而随机化OFDM符号的时长,增加了窃听节点的检测复杂度. 文献[14]研究了离散输入字符集条件下,联合功率分配和人工噪声提高OFDM系统安全性能的方案,在单天线场景下利用OFDM系统CP提供的自由度,将人工噪声放置在合法接收机信道的零空间中,并提出了一种基于拉格朗日对偶优化的迭代优化算法,显著提升了系统保密速率. TR的空间聚焦效应同样也能提高OFDM的安全性能. 文献[15]从可达保密速率方面比较了MISO OFDM系统中TR预编码和最大比传输(Maximum Ratio Transmission, MRT)预编码技术的安全性能. 结果显示:当发射天线数较少时,TR方案可实现的保密速率要优于MRT方案;当发射天线数量较大时,两种预编码技术的保密性能几乎相同. 文献[16]研究了SISO OFDM通信系统中联合频域TR预编码与人工噪声实现安全通信的方法,并通过仿真对所提方案的性能进行了验证.

本文研究OFDM系统中应用TR技术的时空聚焦特性来增大合法接收机与窃听者间的信号质量差异,并通过对子载波功率分配进行优化来提高保密传输速率的方案,同时,给出一种利用OFDM系统的循环前缀的人工噪声方法,进一步提高保密传输速率. 与其他相关文献相比,本文的主要特点包括:(1)在发送端对信号进行TR预处理,增大子载波间信道增益差,再通过对子载波的功率分配进行优化,提高了保密传输速率;(2)给出了子载波功率优化分配的闭式表达式;(3)给出了一种利用OFDM系统的循环前缀构造零空间人工噪声的方法,避免了对多发送天线的要求;(4)给出了子载波功率分配和人工噪声协方差矩阵联合优化的迭代算法,最大化系统可达保密速率.

本文中,带下划线的字母表示频域符号,没有下划线的表示时域符号;小写粗斜体字母表示矢量,大写粗斜体字母表示矩阵,白斜体字母表示标量;$|\cdot|$,$(\cdot)^{\mathrm{T}}$,$(\cdot)^{*}$,$(\cdot)^{\mathrm{H}}$,$\otimes$,$\mathrm{tr}(\boldsymbol{A})$,$\boldsymbol{A}\succcurlyeq 0$分别表示求绝对值或模值、转置、共轭、共轭转置、卷积运算、求迹以及半正定;$[x]^{+}$表示x与0之间的较大值.

2 系统模型

本文研究的时间反转正交频分复用(Time Reversal-Orthogonal Frequency Division Multiplexing, TR-OFDM)系统的模型如图1所示. 系统包括一个发送端Alice和两个接收端,均为系统中的用户. 发送端向其中一个接收端传输信息时,不希望另一个接收端获得传输的信息. 将当前时刻信息传输的目标接收端称为合法接收端Bob,而另一个接收端称为窃听端Eve. 由于都是系统中的用户,因此本文假设发送端可以获得其与两个接收端之间信道的CSI. 两个接收端配备单根天线,先考虑发送端配备单根天线的情况,然后再推广到多根天线的场景. 信道为准静态频率选择性衰落信道,信道状态至少在一个OFDM符号周期内保持不变. 为了表述方便,本文假设发送端到两个接收端信道的CIR长度都为L,发送端到合法接收端、窃听端信道的CIR记为$h_m[l]$, $l=0,1,\cdots,L-1$, $m\in\{\mathrm{B},\mathrm{E}\}$,其矢量表示形式为$\boldsymbol{h}_m=\left[h_m[0],h_m[1],\cdots,h_m[L-1]\right]^{\mathrm{T}}$, $m\in\{\mathrm{B},\mathrm{E}\}$. TR预滤波器采用常规的匹配滤波器的形式,其抽头数为L,抽头系数为合法信道的CIR的时间反转共轭,即TR预滤波器的脉冲响应为

$$g[l]=\frac{h_{\mathrm{B}}^{*}[L-1-l]}{\sqrt{\sum_{l=0}^{L-1}\left|h_{\mathrm{B}}[l]\right|^{2}}}=Gh_{\mathrm{B}}^{*}[L-1-l] \tag{1}$$

其中,$G=\left(\sum_{l=0}^{L-1}\left|h_{\mathrm{B}}[l]\right|^{2}\right)^{-\frac{1}{2}}$,为归一化系数,目的是确保信号经过TR滤波器滤波后功率不发生变化. 把TR预滤波器和多径信道的级联看成等效信道,其脉冲响应的长度为$2L-1$,则合法信道和窃听信道的等效

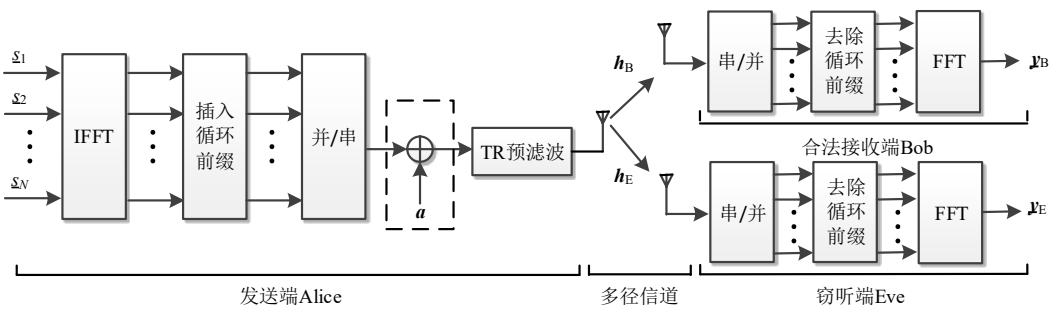


图1 系统模型

CIR分别为

$$h_{m,\mathrm{TR}}[l]=g[l]\otimes h_m[l], m\in\{\mathrm{B},\mathrm{E}\} \tag{2}$$

发射机首先通过快速逆傅里叶变换(Inverse Fast Fourier Transform, IFFT)将频域符号$\underline{\boldsymbol{s}}$变换为时域符号,其中,$\underline{\boldsymbol{s}}=\left[\underline{s}_1,\underline{s}_2,\cdots,\underline{s}_N\right]^{\mathrm{T}}$,是零均值、单位方差的信息符号矢量,$N$为OFDM子载波个数. 时域符号序列插入CP后形成OFDM符号. 时域符号中的样值序列经过并/串转换、TR预滤波器后送入信道. 信号经过多径信道传输到达接收端,接收机经过串/并转换、去除CP,然后通过快速傅里叶变换(Fast Fourier Transform, FFT)将时域符号变换到频域. IFFT可以表示为频域序列$\underline{\boldsymbol{s}}$与$N\times N$维的IFFT矩阵$\boldsymbol{F}^{\mathrm{H}}$相乘. 类似地,FFT可以表示为时域序列与FFT矩阵$\boldsymbol{F}$相乘,$\boldsymbol{F}$的定义为

$$\boldsymbol{F}=\begin{bmatrix} W^0 & W^0 & W^0 & \cdots & W^0 \\ W^0 & W^{1\times 1} & W^{2\times 1} & \cdots & W^{(N-1)\times 1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ W^0 & W^{1\times(N-1)} & W^{2\times(N-1)} & \cdots & W^{(N-1)\times(N-1)} \end{bmatrix} \tag{3}$$

其中,$W=\mathrm{e}^{-\mathrm{j}\frac{2\pi}{N}}$. 为消除符号间干扰,CP的长度$N_{\mathrm{cp}}$应大于等效信道时延扩展,插入CP的过程可以表示为IFFT后的时域序列与加CP矩阵$\boldsymbol{T}^{\mathrm{cp}}=\left[\boldsymbol{E}^{\mathrm{T}}_{N_{\mathrm{cp}}\times N}\boldsymbol{I}_N\right]^{\mathrm{T}}$相乘,其中$\boldsymbol{E}_{N_{\mathrm{cp}}\times N}$表示$N\times N$维单位矩阵$\boldsymbol{I}_N$的后$N_{\mathrm{cp}}$行;去除CP的过程可以表示为接收OFDM符号与去CP矩阵$\boldsymbol{R}^{\mathrm{cp}}=\left[\boldsymbol{0}_{N\times N_{\mathrm{cp}}}\boldsymbol{I}_N\right]^{\mathrm{T}}$相乘,其中$\boldsymbol{0}_{N\times N_{\mathrm{cp}}}$表示$N\times N_{\mathrm{cp}}$维零矩阵. 定义等效合法信道和等效窃听信道对应的$\left(N+N_{\mathrm{cp}}\right)\times\left(N+N_{\mathrm{cp}}\right)$维Toeplitz信道矩阵为

$$\boldsymbol{H}_m=\begin{bmatrix} h_{m,\mathrm{TR}}[0] & 0 & 0 & \cdots & 0 \\ \vdots & h_{m,\mathrm{TR}}[0] & 0 & \cdots & 0 \\ h_{m,\mathrm{TR}}[2L-2] & \vdots & \vdots & \ddots & \vdots \\ \vdots & h_{m,\mathrm{TR}}[2L-2] & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & h_{m,\mathrm{TR}}[2L-2] & \cdots & h_{m,\mathrm{TR}}[0] \end{bmatrix} \tag{4}$$

其中,$m\in\{\mathrm{B},\mathrm{E}\}$. OFDM符号经过TR预滤波和多径信道的过程为OFDM符号中的样值序列与等效信道的脉冲响应进行卷积运算,等价为OFDM符号样值矢量与Toeplitz信道矩阵相乘. 合法接收端和窃听端接收到的频域符号可以表示为

$$\underline{\boldsymbol{y}}_m=\boldsymbol{F}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_m\left(\boldsymbol{T}^{\mathrm{cp}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{P}^{1/2}\underline{\boldsymbol{s}}+\boldsymbol{a}\right)+\underline{\boldsymbol{w}}_m,\ m\in\{\mathrm{B},\mathrm{E}\} \tag{5}$$

其中,$\boldsymbol{P}=\mathrm{diag}(P_1,P_2,\cdots,P_N)$,是子信道功率分配对角矩阵;$\boldsymbol{P}^{1/2}$表示对矩阵$\boldsymbol{P}$中元素开方;$\boldsymbol{a}$为人工噪声序列,是$(N+N_{\mathrm{cp}})$维零均值复高斯随机向量;$\underline{\boldsymbol{w}}_m=\left[\underline{w}_{m1},\underline{w}_{m2},\cdots,\underline{w}_{mN}\right]^{\mathrm{T}}$,$m\in\{\mathrm{B},\mathrm{E}\}$,为合法端和窃听端的信道加性噪声矢量,其元素是零均值、单位方差的独立复高斯随机变量. 将发送端IFFT到接收端FFT间的发送、接收处理过程和多径信道看成等价的频域并行信道,即令

$$\underline{\boldsymbol{H}}_m=\boldsymbol{F}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_m\boldsymbol{T}^{\mathrm{cp}}\boldsymbol{F}^{\mathrm{H}}=\mathrm{diag}(\underline{H}_{m1},\underline{H}_{m2},\cdots,\underline{H}_{mN}) \tag{6}$$

其中,$\underline{H}_{mi}(m\in\{\mathrm{B},\mathrm{E}\})$分别表示从发送端到合法端和窃听端的第$i$个子信道的复系数,则式(5)可等价表示为$N$个子信道的接收符号的表达式:

$$\begin{aligned}&\underline{y}_{mi}=\underline{H}_{mi}\sqrt{P_i}\,\underline{s}_i+\boldsymbol{f}_i^{\mathrm{T}}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_m\boldsymbol{a}+\underline{w}_{mi},\\&i=1,2,\cdots,N\end{aligned} \tag{7}$$

其中,$\boldsymbol{f}_i^{\mathrm{T}}$是FFT矩阵$\boldsymbol{F}$的第$i$行.

3　功率分配的优化

本节先讨论没有人工噪声$\boldsymbol{a}$时,通过优化子信道功率分配来提高保密速率的问题. 物理层安全通信中,可达保密传输速率是描述安全传输性能的常用指标,定义为合法信道容量与窃听信道容量的差值. 在此系统模型下,可达保密速率为

$$\begin{aligned}R_{\mathrm{s}}(\boldsymbol{P})=\frac{1}{N}\sum_{i=1}^{N}\Bigg[&\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)\\&-\log_2\left(1+\left|\underline{H}_{\mathrm{E}i}\right|^2P_i\right)\Bigg]^+\end{aligned} \tag{8}$$

在发送总功率的限制下,对发送端各子载波的功率分配进行优化,最大化可达保密速率,优化问题可表示为

$$\begin{aligned}\max_{\boldsymbol{P}\succcurlyeq 0}\quad & R_{\mathrm{s}}(\boldsymbol{P})\\ \text{s.t.}\quad & \frac{1}{N}\sum_{i=1}^{N}P_i\leqslant P_{\max}\end{aligned} \tag{9}$$

其中，$P_{\max}$是子信道平均最大发射功率. 由式(8)易知，当$\left|\underline{H}_{\mathrm{B}i}\right|<\left|\underline{H}_{\mathrm{E}i}\right|$时，窃听子信道的质量优于合法子信道，不应分配发送功率，即$P_i=0$. 当$\left|\underline{H}_{\mathrm{B}i}\right|>\left|\underline{H}_{\mathrm{E}i}\right|$时，式(8)对$P_i$求二阶偏导，有

$$\frac{\left(\left|\underline{H}_{\mathrm{E}i}\right|^2-\left|\underline{H}_{\mathrm{B}i}\right|^2\right)\left(2\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\underline{H}_{\mathrm{E}i}\right|^2P_i+\left|\underline{H}_{\mathrm{E}i}\right|^2+\left|\underline{H}_{\mathrm{B}i}\right|^2\right)}{\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)^2\left(1+\left|\underline{H}_{\mathrm{E}i}\right|^2P_i\right)^2}<0 \tag{10}$$

因此，$R_{\mathrm{s}}(\boldsymbol{P})$为上凸函数，一定存在极大值，式(9)为凸优化问题，可用KKT条件求解. 式(9)的拉格朗日函数为

$$L(\boldsymbol{P},\lambda)=\frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\left|\underline{H}_{\mathrm{E}i}\right|^2P_i\right)\right]^+ +\lambda\left(P_{\max}-\frac{1}{N}\sum_{i=1}^{N}P_i\right) \tag{11}$$

其中，$\lambda\geqslant0$，为与功率约束相关的拉格朗日乘子. 式(11)对P_i求一阶偏导并令其为0，有

$$\lambda\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\underline{H}_{\mathrm{E}i}\right|^2P_i^2+\lambda\left(\left|\underline{H}_{\mathrm{B}i}\right|^2+\left|\underline{H}_{\mathrm{E}i}\right|^2\right)P_i +\lambda+\left|\underline{H}_{\mathrm{E}i}\right|^2-\left|\underline{H}_{\mathrm{B}i}\right|^2=0 \tag{12}$$

求解该方程，得到功率的最优解为

$$P_i^*=\begin{cases}\dfrac{1}{2\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\underline{H}_{\mathrm{E}i}\right|^2}\left[\sqrt{C_i^2-\dfrac{4\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\underline{H}_{\mathrm{E}i}\right|^2\left(\lambda+\left|\underline{H}_{\mathrm{E}i}\right|^2-\left|\underline{H}_{\mathrm{B}i}\right|^2\right)}{\lambda}}-C_i\right], & \left|\underline{H}_{\mathrm{B}i}\right|^2-\left|\underline{H}_{\mathrm{E}i}\right|^2>\lambda\\ 0, & \text{其他}\end{cases} \tag{13}$$

其中，$C_i=\left|\underline{H}_{\mathrm{B}i}\right|^2+\left|\underline{H}_{\mathrm{E}i}\right|^2$. 最优解$P_i^*$是关于$\lambda$的函数，而$\lambda$由功率约束条件确定，即

$$\frac{1}{N}\sum_{i=1}^{N}P_i^*=P_{\max} \tag{14}$$

观察式(13)给出的P_i^*的解，直接求解满足式(14)的λ非常困难. 令

$$f(\lambda)=\frac{1}{N}\sum_{i=1}^{N}P_i^*-P_{\max} \tag{15}$$

求$f(\lambda)$的一阶导，得到

$$f'(\lambda)=\sum_{i=1}^{N}\left(\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2-\left|\underline{H}_{\mathrm{B}i}\right|^2}{\lambda^2\sqrt{C_i^2-\dfrac{4\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\underline{H}_{\mathrm{E}i}\right|^2\left(\lambda+\left|\underline{H}_{\mathrm{E}i}\right|^2-\left|\underline{H}_{\mathrm{B}i}\right|^2\right)}{\lambda}}}\right) \tag{16}$$

注意到，当$\left|\underline{H}_{Bi}\right|^2>\left|\underline{H}_{\mathrm{E}i}\right|^2$时，$f'(\lambda)$严格小于零，即$f(\lambda)$是关于$\lambda$严格单调递减的函数；当$\lambda\to0$时，$f(\lambda)\to+\infty$；$\lambda\to\infty$时，$f(\lambda)<0$. 所以一定存在满足式(14)的、非负的$\lambda$，可以采用数值方法求解. 首先采用一维进退搜索法找到包含$f(\lambda)$零点的区间$[a,b]$，再用二分搜索法找到$f(\lambda)$的零点，也就是满足$\frac{1}{N}\sum_{i=1}^{N}P_i^*=P_{\max}$的解$\lambda^*$. 求解拉格朗日乘子的算法总结在算法1中，其中$\varepsilon_1$是迭代终止时要求的区间端点的相对差值，即收敛因子.

得到最优拉格朗日乘子λ^*后，将其代入式(13)中可得到各子载波的功率，但可能存在为负值的功率. 对于分配的功率为负值的子信道，直接将功率置0，再重新求解满足约束的最优拉格朗日乘子. 迭代功率分配算法总结在算法2中. 首先将$\left|\underline{H}_{\mathrm{B}i}\right|^2<\left|\underline{H}_{\mathrm{E}i}\right|^2$的子信道功率置零，通过算法1求解满足$\frac{1}{N}\sum_{i=1}^{N}P_i=P_{\max}$的拉格朗日乘子$\lambda^{(1)}$，带入式(13)中得到所有子信道的功率分配$\left\{P_i\right\}_{i=1}^{N}$. 若此时有子信道的功率为负值，则将这些子信道的功率置0，重新求解满足约束$\frac{1}{N}\sum_{i=1}^{N}P_i=P_{\max}$的拉格朗日乘子$\lambda^{(2)}$，以及对应的子载波功率分配. 重复上述过程，直至所有子信道的功率分配结果均为正值或0.

算法1 最优拉格朗日乘子的求解

1. 设置初始点x_0，初始步长d，步长控制因子r，$x_1=x_0$，$x_2=x_0+r\times d$
2. 判断$f(x_1)>0$是否满足. 若是，转步骤3；否则转步骤6
3. 判断$f(x_2)>0$是否满足. 若是，转步骤4；否则转步骤8
4. 置$r=2r$，$x_1=x_2$，$x_2=x_1+r\times d$
5. 判断$f(x_2)<0$是否满足. 若是，转步骤8；否则转步骤4
6. 置$r=0.5r$，$x_2=x_1$，$x_1=x_2-r\times d$
7. 判断$f(x_1)>0$是否满足. 若是，转步骤8；否则转步骤6
8. 输出$a=x_1$，$b=x_2$，得到二分区间$[a,b]$
9. 置$\lambda=\frac{1}{2}(a+b)$，判断$f(\lambda)<0$是否满足. 若是，置$b=\lambda$；否则置$a=\lambda$
10. 判断$\frac{b-a}{b}\leqslant\varepsilon_1$是否满足. 若是，输出最优解$\lambda^*=b$；否则转步骤9

4 人工噪声设计与分析

在物理层安全通信系统中，通过合理地使用人工噪声，能在对窃听端形成有效干扰的同时，不对合法端造成影响，能有效增大合法者和窃听者接收信号的质量差异，提升系统的安全性能. 大多数的人工噪声方案依赖由多个发射天线提供的空间自由度，在单天线系

算法2　子载波功率分配的迭代求解

1. 将信道增益$\left|\underline{H}_{\mathrm{B}i}\right|^2<\left|\underline{H}_{\mathrm{E}i}\right|^2$的子信道功率初始化为0,$k$=0
2. 循环
3. k=k+1
4. 根据算法1计算满足$\frac{1}{N}\sum_{i=1}^{N}P_i=P_{\max}$的零点$\lambda^{(k)}$
5. 根据式(13)计算$\boldsymbol{P}^{(k)}$
6. 判断$\boldsymbol{P}^{(k)}\geqslant 0$是否满足. 若是,跳出循环;否则置$\{P_i\}_{i=1}^{N}=\left[\{P_i\}_{i=1}^{N}\right]^{+}$,转步骤3继续迭代
7. 输出最优功率分配结果$\boldsymbol{P}^{\mathrm{opt}}=\boldsymbol{P}^{(k)}$

统中是不可用的. 本文借鉴文献[14]的思想,利用OFDM系统的CP提供的时间自由度,设计一种针对单天线OFDM窃听信道的人工噪声方案,进一步根据人工噪声对窃听者干扰情况的分析结果,优化人工噪声的功率安排,提高人工噪声的功率效率,同时还能降低优化复杂度.

如图1中虚线框中所示,人工噪声矢量$\boldsymbol{a}$叠加在TR预处理前、添加了CP的时域序列上,经过TR滤波和多径信道传输后,合法接收者和窃听者接收到的频域符号序列可以表示为

$$\underline{\boldsymbol{a}}_{\mathrm{E}}=\boldsymbol{F}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{E}}\boldsymbol{Q}\boldsymbol{z}=\boldsymbol{F}\left[\boldsymbol{0}_{N\times(N_{\mathrm{cp}}-L_{\mathrm{TR}})}\tilde{\boldsymbol{G}}_{N\times(N+L_{\mathrm{TR}})}\right]\begin{bmatrix}\boldsymbol{W}_{(N+N_{\mathrm{cp}})\times(N_{\mathrm{cp}}-L_{\mathrm{TR}})} & \boldsymbol{0}_{(N_{\mathrm{cp}}-L_{\mathrm{TR}})\times L_{\mathrm{TR}}}\\ & \boldsymbol{V}_{(N+L_{\mathrm{TR}})\times L_{\mathrm{TR}}}\end{bmatrix}\boldsymbol{z}_{N_{\mathrm{cp}}\times 1} \tag{20}$$

其中,$\tilde{\boldsymbol{G}}$是去除CP后的等效窃听信道矩阵$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{E}}$的非零列;$\tilde{\boldsymbol{Q}}=\boldsymbol{F}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{E}}\boldsymbol{Q}$,表示人工噪声经过窃听信道并包括去除CP和FFT处理的等效信道矩阵,$\tilde{\boldsymbol{Q}}$的秩为L_{TR},$\tilde{\boldsymbol{Q}}$零列数为$N_{\mathrm{cp}}-L_{\mathrm{TR}}$. 式(20)可重新表述为

$$\underline{\boldsymbol{a}}_{\mathrm{E}}=\boldsymbol{F}\left[\boldsymbol{0}_{N\times(N_{\mathrm{cp}}-L_{\mathrm{TR}})}\ \boldsymbol{U}_{N\times L_{\mathrm{TR}}}\right]\boldsymbol{z}_{N_{\mathrm{cp}}\times 1} \tag{21}$$

其中,$\boldsymbol{U}_{N\times L_{\mathrm{TR}}}$表示$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{E}}\boldsymbol{Q}$矩阵的非零列. 观察式(21)可以发现,人工噪声矢量$\boldsymbol{z}$的前$(N_{\mathrm{cp}}-L_{\mathrm{TR}})$个噪声符号会因为与等效信道矩阵$\tilde{\boldsymbol{Q}}$的全零列相乘而未对窃听端形成干扰,只有后$L_{\mathrm{TR}}$个噪声符号才能对窃听者形成干扰. 因此,为更有效地利用发送功率,应将人工噪声协方差矩阵对角线的前$(N_{\mathrm{cp}}-L_{\mathrm{TR}})$个元素置0,对后面$L_{\mathrm{TR}}$个对角元素以最大化保密速率为目标进行优化.

由于将人工噪声$\boldsymbol{a}$设置在了合法信道的零空间,子信道i上的接收信号可以表示为

$$\begin{aligned}&\underline{y}_{\mathrm{B}i}=\underline{H}_{\mathrm{B}i}\sqrt{P_i}\,\underline{s}_i+\underline{w}_{\mathrm{B}i}\\&\underline{y}_{\mathrm{E}i}=\underline{H}_{\mathrm{E}i}\sqrt{P_i}\,\underline{s}_i+\boldsymbol{f}_i^{\mathrm{T}}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{E}}\boldsymbol{Q}\boldsymbol{z}+\underline{w}_{\mathrm{E}i}\\&i=1,2,\cdots,N\end{aligned} \tag{22}$$

系统可达保密速率为

$$\begin{aligned}\underline{\boldsymbol{y}}_m&=\boldsymbol{F}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_m\left(\boldsymbol{T}^{\mathrm{cp}}\boldsymbol{F}^{\mathrm{H}}\boldsymbol{P}^{1/2}\underline{\boldsymbol{s}}+\boldsymbol{a}\right)+\underline{\boldsymbol{w}}_m\\&=\underline{\boldsymbol{H}}_m\boldsymbol{P}^{1/2}\underline{\boldsymbol{s}}+\boldsymbol{F}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_m\boldsymbol{a}+\underline{\boldsymbol{w}}_m,\\&m\in\{\mathrm{B},\mathrm{E}\}\end{aligned} \tag{17}$$

为了不干扰合法接收机,人工噪声应位于合法信道的零空间中,可将人工噪声设计成$\boldsymbol{a}=\boldsymbol{Q}\boldsymbol{z}$. 其中$\boldsymbol{z}$是一个高斯随机向量,服从$\boldsymbol{z}\sim\mathrm{CN}\left(0,\boldsymbol{\Sigma}_z\right)$,$\boldsymbol{\Sigma}_z$为$\boldsymbol{z}$的对角协方差矩阵;$\boldsymbol{Q}$为半酉矩阵,其列向量张成$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}$的零空间,维度为$N_{\mathrm{cp}}$,满足$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}\boldsymbol{Q}=0$. 记$L_{\mathrm{TR}}$为等效合法信道和等效窃听信道的最大时延扩展,$L_{\mathrm{TR}}=2L-2$. $\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}$中包含$(N_{\mathrm{cp}}-L_{\mathrm{TR}})$个零列,也就是

$$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}=\left[\boldsymbol{0}_{N\times(N_{\mathrm{cp}}-L_{\mathrm{TR}})}\ \tilde{\boldsymbol{H}}_{N\times(N+L_{\mathrm{TR}})}\right] \tag{18}$$

其中,$\tilde{\boldsymbol{H}}$是去除CP后的等效合法信道矩阵$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}$的非零列,$\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}$的零空间包含$(N_{\mathrm{cp}}-L_{\mathrm{TR}})$个标准正交基,即

$$\boldsymbol{Q}=\mathrm{Null}\left(\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{B}}\right)=\begin{bmatrix}\boldsymbol{W}_{(N+N_{\mathrm{cp}})\times(N_{\mathrm{cp}}-L_{\mathrm{TR}})} & \boldsymbol{0}_{(N_{\mathrm{cp}}-L_{\mathrm{TR}})\times L_{\mathrm{TR}}}\\ & \boldsymbol{V}_{(N+L_{\mathrm{TR}})\times L_{\mathrm{TR}}}\end{bmatrix} \tag{19}$$

其中,Null(·)表示求零空间运算;$\boldsymbol{W}=\begin{bmatrix}\boldsymbol{I}_{N_{\mathrm{cp}}-L_{\mathrm{TR}}} & \boldsymbol{0}_{(N+L_{\mathrm{TR}})\times(N_{\mathrm{cp}}-L_{\mathrm{TR}})}\end{bmatrix}^{\mathrm{T}}$;$\boldsymbol{V}=\mathrm{Null}(\tilde{\boldsymbol{H}})$;$\boldsymbol{I}$为单位矩阵. 窃听端Eve处接收到的频域人工噪声序列可表示为

$$R_{\mathrm{s}}(\boldsymbol{P})=\frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^{+} \tag{23}$$

其中,$\boldsymbol{q}_i=\boldsymbol{f}_i^{\mathrm{T}}\boldsymbol{R}^{\mathrm{cp}}\boldsymbol{H}_{\mathrm{E}}\boldsymbol{Q}$. 使保密速率最大化的子载波功率分配和人工噪声的协方差矩阵的联合优化问题可以表述为

$$\begin{aligned}&\max_{\boldsymbol{P}\geqslant 0,\boldsymbol{\Sigma}_z\geqslant 0}\ \frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^{+}\\&\text{s.t.}\quad\frac{1}{N}\left[\sum_{i=1}^{N}P_i+\mathrm{tr}(\boldsymbol{\Sigma}_z)\right]\leqslant P_{\max}\end{aligned} \tag{24}$$

式(24)是双优化变量的非凸问题,且优化变量$\boldsymbol{P}$和$\boldsymbol{\Sigma}_z$均为矩阵,求解较为困难. 本文采用逐次凸逼近算法交替优化$\boldsymbol{P}$和$\boldsymbol{\Sigma}_z$,优化一个变量时,固定另一个变量,通过交替迭代优化获得最优解. 但注意到在$\boldsymbol{P}$和$\boldsymbol{\Sigma}_z$的迭代求解过程中要求发送的数据符号和人工噪声的功率是给定的,而原问题即

式(24)中约束的是二者的总功率,这意味着还需要对发送数据符号和人工噪声的功率分配比进行优化.引入功率分配因子$\alpha\in[0,1]$为人工噪声功率与总功率的比值,则$(1-\alpha)$为分配给数据符号功率的比例.这样,式(24)可以等价表示为

$$\begin{aligned}\max_{\alpha,\boldsymbol{P}\geqslant 0,\boldsymbol{\Sigma}_z\geqslant 0}\ & \frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^+\\ \text{s.t.}\ & \frac{1}{N}\sum_{i=1}^{N}P_i\leqslant(1-\alpha)P_{\max}\\ & \frac{1}{N}\mathrm{tr}(\boldsymbol{\Sigma}_z)\leqslant\alpha P_{\max}\\ & 0\leqslant\alpha\leqslant 1\end{aligned}\tag{25}$$

进一步将式(25)转换为一个等价的两层优化问题.第一层优化问题为在α的取值范围内寻找使目标函数最大的$\varphi(\alpha)$:

$$\begin{aligned}\max_{\alpha}\ & \varphi(\alpha)\\ \text{s.t.}\ & 0\leqslant\alpha\leqslant 1\end{aligned}\tag{26}$$

其中,$\varphi(\alpha)$为α固定情况下以$\boldsymbol{P}$和$\boldsymbol{\Sigma}_z$为变量的保密速率的最大值,即$\varphi(\alpha)=\max\limits_{\boldsymbol{P}\geqslant 0,\boldsymbol{\Sigma}_z\geqslant 0}\ \frac{1}{N}\sum\limits_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^+$.而求取该最大值就是第二层优化问题:

$$\begin{aligned}\max_{\boldsymbol{P}\geqslant 0,\boldsymbol{\Sigma}_z\geqslant 0}\ & \frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^+\\ \text{s.t.}\ & \frac{1}{N}\sum_{i=1}^{N}P_i\leqslant(1-\alpha)P_{\max}\\ & \frac{1}{N}\mathrm{tr}(\boldsymbol{\Sigma}_z)\leqslant\alpha P_{\max}\end{aligned}\tag{27}$$

对于第一层优化问题,易知一定存在一个最优的α^*使保密速率最大化,本文采用黄金分割法进行求解.求解的搜索过程中,需要根据黄金分割点对应的α值进行第二层优化问题的求解.通过迭代的方式不断缩小搜索区间,直至区间对应的两个α值的保密速率之间的差值小于某个预先设定的值.求解最优功率分配因子α^*的算法总结在算法3中.

第二层优化问题为在功率分配因子给定的情况下,人工噪声协方差矩阵和功率分配的优化.将其分解为两个需要进行迭代求解的子问题.子问题1为在人工噪声的协方差阵$\boldsymbol{\Sigma}_z$固定下,优化子载波的功率分配$\boldsymbol{P}$使保密速率最大化:

算法3 式(26)的迭代求解

1. 设置初始点$c=0,d=1,\alpha_1=d-0.618(d-c),\alpha_2=c+0.618(d-c),k=0$,根据$\alpha_1$和$\alpha_2$求解第二层优化问题,分别得到区间两个端点对应的保密速率$R_{\mathrm{s}1}^{(k)}$和$R_{\mathrm{s}2}^{(k)}$
2. 循环
3. $k=k+1$
4. 判断$R_{\mathrm{s}1}^{(k-1)}>R_{\mathrm{s}2}^{(k-1)}$是否满足.若是,置$c=\alpha_1,\alpha_1=\alpha_2,\alpha_2=c+0.618(d-c),R_{\mathrm{s}1}^{(k)}=R_{\mathrm{s}2}^{(k-1)}$,重新求解第二层优化问题得到$R_{\mathrm{s}2}^{(k)}$;否则置$d=\alpha_2,\alpha_2=\alpha_1,\alpha_1=d-0.618(d-c),R_{\mathrm{s}2}^{(k)}=R_{\mathrm{s}1}^{(k-1)}$,重新求解第二层优化问题得到$R_{\mathrm{s}1}^{(k)}$
5. 判断$\left|R_{\mathrm{s}1}^{(k)}-R_{\mathrm{s}2}^{(k)}\right|<\varepsilon_2$是否满足.若是,跳出循环,否则转步骤3迭代
6. 输出最优功率分配因子$\alpha=\frac{1}{2}(\alpha_1+\alpha_2)$

$$\begin{aligned}\max_{\boldsymbol{P}\geqslant 0}\ & \frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^+\\ \text{s.t.}\ & \frac{1}{N}\sum_{i=1}^{N}P_i\leqslant(1-\alpha)P_{\max}\end{aligned}\tag{28}$$

子问题2为在子载波的功率分配$\boldsymbol{P}$固定的情况下,优化人工噪声的协方差阵$\boldsymbol{\Sigma}_z$使窃听信道容量最小化:

$$\begin{aligned}\min_{\boldsymbol{\Sigma}_z\geqslant 0}\ & \frac{1}{N}\sum_{i=1}^{N}\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\\ \text{s.t.}\ & \frac{1}{N}\mathrm{tr}(\boldsymbol{\Sigma}_z)\leqslant\alpha P_{\max}\end{aligned}\tag{29}$$

在人工噪声的协方差阵$\boldsymbol{\Sigma}_z$给定的情况下,子问题1为一个凸优化问题,可以用一阶KKT条件求解.子问题1的拉格朗日函数为

$$\begin{aligned}L(\boldsymbol{p},\mu)=&\frac{1}{N}\sum_{i=1}^{N}\left[\log_2\left(1+\left|\underline{H}_{\mathrm{B}i}\right|^2P_i\right)-\log_2\left(1+\frac{\left|\underline{H}_{\mathrm{E}i}\right|^2P_i}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}\right)\right]^+\\&+\mu\left((1-\alpha)P_{\max}-\frac{1}{N}\sum_{i=1}^{N}P_i\right)\end{aligned}\tag{30}$$

其中,$\mu\geqslant 0$,为与约束相关的拉格朗日乘子,通过求解 $\frac{\partial L}{\partial P_i}=0$,得到功率最优解的表达式为

$$P_i^*=\begin{cases}\dfrac{1}{2\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\tilde{\underline{H}}_{\mathrm{E}i}\right|^2}\left[\sqrt{\hat{C}_i^2-\dfrac{4\left|\underline{H}_{\mathrm{B}i}\right|^2\left|\tilde{\underline{H}}_i\right|^2\left(\lambda+\left|\tilde{\underline{H}}_{\mathrm{E}i}\right|^2-\left|\underline{H}_{\mathrm{B}i}\right|^2\right)}{\mu}}-\hat{C}_i\right], & \left|\underline{H}_{\mathrm{B}i}\right|^2-\left|\tilde{\underline{H}}_{\mathrm{E}i}\right|^2>\mu\\ 0, & \text{其他}\end{cases}\tag{31}$$

其中,$\left|\tilde{\underline{H}}_{\mathrm{E}i}\right|^2=\dfrac{\left|\underline{H}_{\mathrm{E}i}\right|^2}{\boldsymbol{q}_i\boldsymbol{\Sigma}_z\boldsymbol{q}_i^{\mathrm{H}}+1}$,$\hat{C}_i=\left|\underline{H}_{\mathrm{B}i}\right|^2+\left|\tilde{\underline{H}}_{\mathrm{E}i}\right|^2$. 对比式(31)与式(13)发现,该优化子问题与无人工噪声时的功率分配问题完全类似,因此可用算法2求解.

将求解子问题1得到的功率分配结果代入子问题2中,易知这是一个凸优化问题,可以用CVX工具箱进行求解. 优化人工噪声协方差矩阵的复杂度为 $\sqrt{N_{\mathrm{cp}}}\left[n_1^3+n_1^2(N_{\mathrm{cp}})^2+n_1(N_{\mathrm{cp}})^3\right]$,其中,$n_1=O(L_{\mathrm{TR}})$. 而文献[14]的优化人工噪声的复杂度为 $\sqrt{N_{\mathrm{cp}}}\left[n_2^3+n_2^2(N_{\mathrm{cp}})^2+n_2(N_{\mathrm{cp}})^3\right]$,其中 $n_2=O(N_{\mathrm{cp}})$. 由于 $N_{\mathrm{cp}}>L_{\mathrm{TR}}$,故在优化人工噪声方面,本文的复杂度要低于文献[14].

为得到功率分配因子α给定下最大的保密速率,也就是求解最优的子载波的功率分配$\boldsymbol{P}$和人工噪声的协方差阵$\boldsymbol{\Sigma}_z$,需要在子问题1和子问题2的求解间进行迭代. 首先将人工噪声协方差矩阵对角线的前$(N_{\mathrm{cp}}-L_{\mathrm{TR}})$个元素置0,后面$L_{\mathrm{TR}}$个元素的初始值设为$\dfrac{N\alpha P_{\max}}{L_{\mathrm{TR}}}$,即 $\boldsymbol{\Sigma}_z^{(0)}=\mathrm{diag}(\underbrace{0,0,\cdots,0}_{N_{\mathrm{cp}}-L_{\mathrm{TR}}},\underbrace{p_z,p_z,\cdots,p_z}_{L_{\mathrm{TR}}})$,其中 $p_z=\dfrac{N\alpha P_{\max}}{L_{\mathrm{TR}}}$. 在该$\boldsymbol{\Sigma}_z^{(0)}$下求解子问题1,得到功率分配$\boldsymbol{P}^{(1)}$,代入子问题2中,求解得到人工噪声协方差阵$\boldsymbol{\Sigma}_z^{(1)}$,再代入子问题1中,进行第2轮迭代. 如此重复迭代,直到收敛. 该迭代算法总结在算法4中. 其中,$\boldsymbol{P}^{(k)}$和$\boldsymbol{\Sigma}_z^{(k)}$分别为第$k$次迭代得到的子载波功率分配和人工噪声协方差矩阵;$\varepsilon_3$是迭代终止时要求的两次迭代间保密速率差值的最大值,即收敛因子. 由于子问题1是给定人工噪声协方差阵下优化子载波功率分配,最大化保密速率一定能使保密速率提高;而子问题2是在功率分配固定下对人工噪声协方差矩阵进行优化,最小化窃听信道容量同样也能使保密速率提高. 因此每一次迭代都能使保密速率在上一次迭代的基础上有所提高,因此迭代过程一定是收敛的.

算法4　式(27)的迭代求解

1. 设置人工噪声协方差矩阵的初始值$\boldsymbol{\Sigma}_z^{(0)}$,$k$=0
2. 循环
3. k=k+1
4. 根据$\boldsymbol{\Sigma}_z^{(k-1)}$求解式(28),计算子载波功率分配$\boldsymbol{P}^{(k)}$
5. 将$\boldsymbol{P}^{(k)}$带入式(29),通过CVX求解$\boldsymbol{\Sigma}_z^{(k)}$
6. 根据$\boldsymbol{P}^{(k)}$和$\boldsymbol{\Sigma}_z^{(k)}$计算保密速率$R_{\mathrm{s}}^{(k)}$
7. 判断$\left|R_{\mathrm{s}}^{(k)}-R_{\mathrm{s}}^{(k-1)}\right|\leqslant\varepsilon_3$是否满足. 若是,跳出循环;否则转步骤3迭代
8. 输出优化问题解$R_{\mathrm{s}}^{\mathrm{opt}}=R_{\mathrm{s}}^{(k)}$

5　多发送天线场景下的推广

前面给出了单发送天线下的优化方案,该方案经过简单的推广就可应用到多发送天线场景下. 多天线系统模型如图2所示.

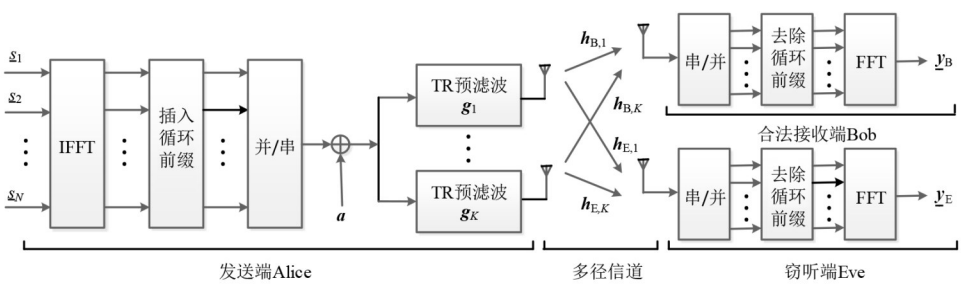


图2　多天线系统模型图

假设发送端配备K根天线,所有信道的CIR长度都为L. 发送端第k根天线到合法接收端和窃听端的CIR表示为$h_{m,k}[l]$,$l=0,1,\cdots,L-1$,其矢量形式为$\boldsymbol{h}_{m,k}=\left[h_{m,k}[0],h_{m,k}[1],\cdots,h_{m,k}[L-1]\right]^{\mathrm{T}}$,$m\in\{\mathrm{B},\mathrm{E}\}$. 每根发送天线都有一个TR预滤波器,其脉冲响应为该天线与合法接收端间CIR的时间反转共轭,即第k根天线的TR预滤波器的脉冲响应为

$$g_k[l]=G_K h_{\mathrm{B},k}^*[L-1-l]\tag{32}$$

其中，$G_K=\left(\sum_{k=1}^{K}\sum_{l=0}^{L-1}\left|h_{\mathrm{B},k}[l]\right|^2\right)^{-\frac{1}{2}}$为归一化系数，保证所有天线的发送功率符合发送功率的限制．TR预滤波器和多径信道级联的等效CIR的长度为$2L-1$．等效合法信道和等效窃听信道的CIR分别为

$$\tilde{h}_{m,\mathrm{TR}}[l]=\sum_{k=1}^{K}g_k[l]\otimes h_{m,k}[l],\ m\in\{\mathrm{B},\mathrm{E}\} \quad (33)$$

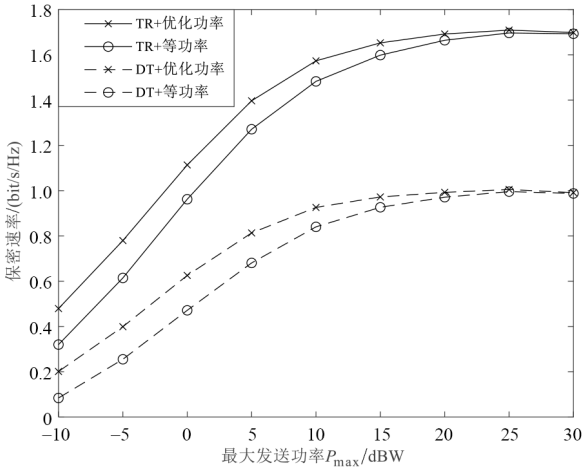
多天线场景下的信道矩阵$\boldsymbol{H}_{\mathrm{B}}$和$\boldsymbol{H}_{\mathrm{E}}$分别是第一列为$\left[\tilde{h}_{\mathrm{B,TR}}[0],\tilde{h}_{\mathrm{B,TR}}[1],\cdots,\tilde{h}_{\mathrm{B,TR}}[2L-2],0,\cdots,0\right]^{\mathrm{T}}$和$\left[\tilde{h}_{\mathrm{E,TR}}[0],\tilde{h}_{\mathrm{E,TR}}[1],\cdots,\tilde{h}_{\mathrm{E,TR}}[2L-2],0,\cdots,0\right]^{\mathrm{T}}$的$(N+N_{\mathrm{cp}})$维Toeplitz矩阵．利用多天线下的$\boldsymbol{H}_{\mathrm{B}}$和$\boldsymbol{H}_{\mathrm{E}}$，合法接收者和窃听者接收到的频域符号序列可以用式(7)来描述，其中的$\underline{H}_{\mathrm{B}i}$和$\underline{H}_{\mathrm{E}i}$由多天线下$\boldsymbol{H}_{\mathrm{B}}$和$\boldsymbol{H}_{\mathrm{E}}$通过式(6)得到．功率分配优化问题的表达式仍为式(9)，人工噪声和功率分配的联合优化问题依旧描述为式(24)，因此可以采用第3节、第4节给出的优化算法进行求解．本文提出的功率分配优化方案(包括信息信号与人工噪声间的功率分配和子载波功率分配)、人工噪声优化方案取决于等效信道矩阵．由于TR预滤波的存在，发送天线数变化时等效信道矩阵的维度并不会变化，因此优化方案可直接应用于任意发送天线数情况下，优化复杂度也不会随发送天线数的增加而增加．

6 仿真结果分析

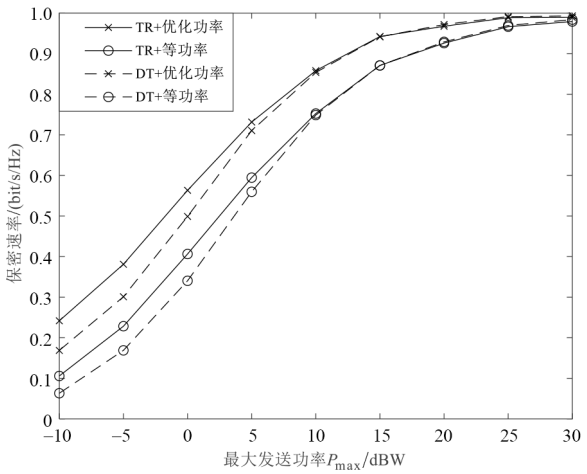
本节对所提算法的性能进行仿真验证．以下每个图中的保密速率的仿真结果是1×10^4组信道样本下的平均值．仿真中，OFDM子载波数量$N=64$，循环前缀长度$N_{\mathrm{cp}}=16$；信道路径数L=8，信道带宽$B=10$ MHz；信道为瑞利衰落信道，信道系数服从零均值的复高斯分布，合法信道和窃听信道第l径系数的方差分别为$E\left[\left|h_{\mathrm{B}}[l]\right|^2\right]=\eta_{\mathrm{B}}\mathrm{e}^{-\frac{lT_{\mathrm{s}}}{\sigma_{\mathrm{T}}}}$和$E\left[\left|h_{\mathrm{E}}[l]\right|^2\right]=\eta_{\mathrm{E}}\mathrm{e}^{-\frac{lT_{\mathrm{s}}}{\sigma_{\mathrm{T}}}}$，$l=0,1,\cdots,L-1$，其中，$\sigma_{\mathrm{T}}=5/B$，为信道的均方根延迟；$T_{\mathrm{s}}=1/B$为采样周期；$\eta_{\mathrm{B}}$和$\eta_{\mathrm{E}}$分别为合法信道和窃听信道的大尺度衰落系数，仿真中归一化为1，噪声功率归一化为1，算法1、算法3、算法4中的收敛因子为$\varepsilon_1=1\times10^{-4}$，$\varepsilon_2=\varepsilon_3=1\times10^{-3}$．

图3是无人工噪声时TR预滤波方案与直接传输方案在是否进行功率分配优化两种情况下可达保密速率随发送功率变化的仿真结果．图中，TR表示信号进行了时间反转预滤波；DT(Direct Transmission)表示直接传输，即发送符号不经过TR预滤波器．直接传输方案也采用本文第3节中给出的算法进行功率分配的优化．未进行功率分配优化时两种方案均采用等功率分配，即在所有合法信道增益高于窃听信道增益的子信道上均匀分配功率．从图3(a)可以看到，不论是否经过TR预滤波，经过功率分配优化后保密速率都有明显的提高，且发送功率越小，提高的程度越明显，这证明了优化功率分配对改善保密传输性能的有效性．对比TR传输和直接传输在相同功率分配方案下的仿真结果，可以看到TR传输在低发送功率时的保密速率要高于直接传输，高发送功率时则二者相近．这是由于TR预滤波器的脉冲响应为合法信道CIR的时间反转共轭，发送信号与其进行卷积在频域相当于给在每个子信道上传输的符号乘以该子信道系数的共轭，会增大子信道增益之间的差异．对于非期望接收机，则没有类似的效果．换句话说，经过TR预滤波后，合法信道增益高的子信道会有相对于窃听子信道更高的质量优势，而增益低的子信道则变得比窃听信道对应子信道更差．通过功率分配优化后，子信道性能差异的改变就表现为合法信道和窃听信道容量差异扩大，因此提高了保密传输速率．而发送功率较高时，功率分配对传输速率的改善效果下降，所以通过TR预滤波提升保密速率的效果也会下降．图3(b)为两根天线下的仿真结果，可以看到两天线场景下，TR预滤波方案相较于直接传输方案的性能优势要明显高于单发送天线场景．这是由于TR预处理是针对合法信道进行的，天线数增大相当于路径数增多，空时聚焦效果更加明显，合法信道容量会有更明显的提升，而窃听信道容量则不会有明显的变化．图3的仿真结果说明：(1)通过对子载波的功率分配进行优化，可以提高系统的保密速率，特别是在发送总功率较低时；(2)TR预处理也能提高保密速率，天线数越多，效果越明显；(3)经过TR预处理后，优化子载波功率分配对保密速率的提升效果更加明显．

图4是有无人工噪声方案的保密速率对比，分别给出了TR传输和直接传输时的仿真结果．TR传输和直接传输在无人工噪声时都采用本文第3节给出的算法对子载波的功率进行了优化分配，有人工噪声时都采用第4节给出的算法进行了子载波功率分配和人工噪声协方差矩阵的联合优化．如图4(a)所示，加入人工噪声后，TR传输系统和直接传输系统的保密速率都有显著的提升，且发送功率越高，提升越明显．在无人工噪声时，保密速率会随发送功率的增加而逐渐逼近一个上限；而有人工噪声时，保密速率会随发送功率的增加而持续增加．这是因为在没有人工噪声时，尽管以保密速率最大化进行了子载波功率分配的优化，但当发送功率增加到一定程度后，合法信道容量和窃听信道容量随发送功率增加的速度仍会逐渐趋于一致，导致保密速率的增长速度逐渐降低，最后趋于一个定值．而采用人工噪声的方案中，由于人工噪声不会对合法端造

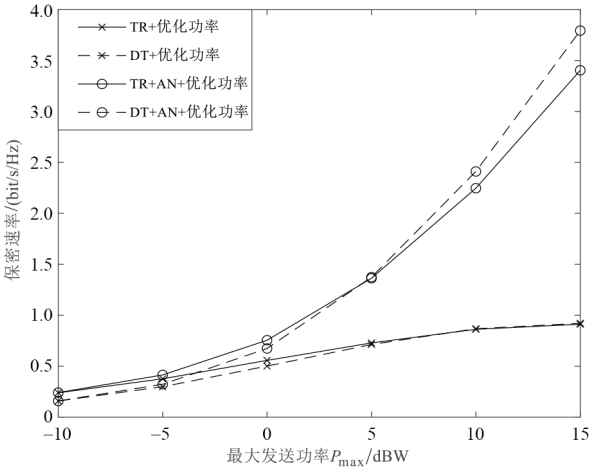


(*a*) 发送天线数*K*=1

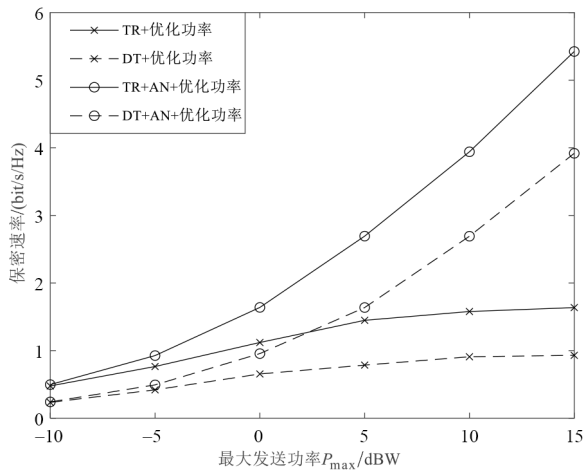


(*b*) 发送天线数*K*=2

图3　无人工噪声时的保密速率



(*a*) 发送天线数*K*=1



(*b*) 发送天线数*K*=2

图4　有无人工噪声时保密速率的对比

成影响,发送功率增加时,合法信道容量增加,窃听信道容量的增加速度要明显低于合法信道,因此保密速率会随总发送功率的增加而持续增加. 比较图4(*a*)和(*b*),天线数由1根增至2根时,直接传输系统的保密速率仅有少量增长,而TR传输系统的保密速率则有明显的增加. 这是因为TR传输利用信道多径将传输的能量聚集在合法接收端,天线数增加时,TR传输的空时聚焦效果增强,合法端的接收信号强度增加,从而使TR传输的保密速率有较为明显的提升. 这说明增加天线数能够提供更多的空间自由度,TR传输能更充分地利用多径信道获得空时聚焦效果,从而改善物理层安全性能.

图5对比了本文第3节、第4节中给出的有无人工噪声的两种优化方案和采用文献[14]的人工噪声方案的保密速率的仿真结果. 为比较公平,文献[14]方案也采用了本文第3节、第4节中给出的算法对子载波功率分配、信息信号与人工噪声功率分配进行优化. 由于文

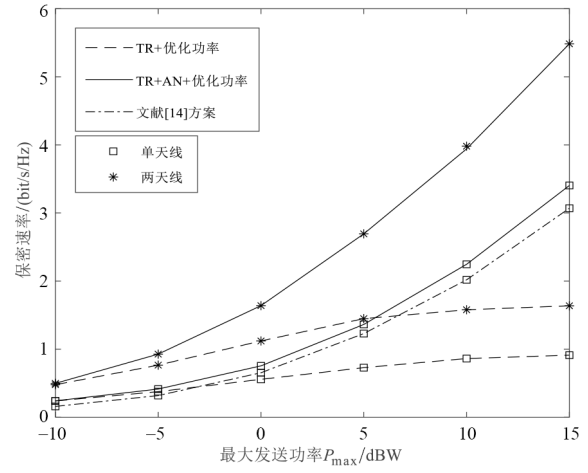


图5　不同天线数目下的保密速率

献[14]中只给出了单发送天线下的方案,因此这里只给出了单天线下的仿真结果. 从仿真结果可以得到:(1)随着发送功率的增加,采用本文和文献[14]人工噪

声方案的保密速率的增加速度明显高于未采用人工噪声的方案，本文采用人工噪声的方案在整个功率范围内的保密速率都要高于未采用人工噪声的方案，说明采用人工噪声能有效地提高安全性能；(2)采用本文人工噪声方案的保密速率在整个功率范围内都要高于采用文献[14]人工噪声方案的保密速率，证明本文方案通过将不起干扰作用的人工噪声符号功率置0，提高了人工噪声功率的使用效率；(3)发送天线数增加，本文有无人工噪声的两种方案的保密速率都有明显提升，有人工噪声时的提升更加显著，这是因为天线数增多提供了更多的信号传输路径，TR预滤波获得的时空聚焦效果增强，从而有效地提高合法接收端的信号强度和合法信道容量，而在有人工噪声的方案中，当发送功率增加时，分配给人工噪声的功率增大，对窃听端的干扰增强，从而进一步提升了保密速率.

图6是采用了人工噪声的方案中，利用本文第4节中的算法对信号功率与人工噪声功率的分配因子进行优化与功率分配因子固定取值时的可达保密速率的对比(天线数K=1). 功率分配因子固定取值时子载波功率分配和人工噪声协方差阵同样用本文第4节中的算法4进行了优化. 如图6所示，保密速率随发送功率增加而增大，但不论发送功率如何设置，对功率分配因子α进行优化后的保密速率始终优于固定α的情况，说明优化α对提升保密速率有效. 当$P_{\max}$=−10 dBW时，保密速率随着α的增大而减小，说明在可用总功率较低时，由于人工噪声不携带信息，给其分配较少比例的功率或不使用人工噪声更优. 当$P_{\max}$=−5 dBW，$P_{\max}$=0 dBW，$P_{\max}$=10 dBW时，保密速率都是先随着α的增大而增大，再随α的增大而减小. 当$P_{\max}$=−5 dBW时，保密速率在α≈0.2时达到峰值，当$P_{\max}$=0 dBW，$P_{\max}$=10 dBW时，保密速率都在α≈0.3时达到峰值，说明可用功率增加时，适当增加人工噪声功率的比重有利于提升保密速率，但分配过多的人工噪声功率反而引起保密性能的下降. 仿真结果表明，人工噪声是一种高功率效率的、提升安全性能的有效技术手段，通过设置合适的人工噪声功率，保密速率能得到显著的提升.

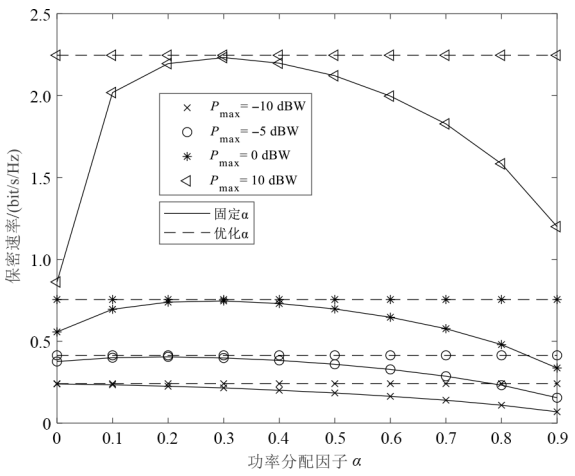


图6 不同功率分配因子α下的保密速率

7 结论

本文针对增强TR-OFDM系统安全性能的方案进行研究. 系统模型中包括一个发送端、一个合法接收者和一个窃听者. 在发送端，信号在通过天线发送前先经过TR预滤波器进行预处理，利用TR的时空聚焦特性提升系统抗窃听能力. 本文分别给出了有无人工噪声时，以最大化保密速率为目标的优化算法. 在没有人工噪声辅助时，通过对发送端子载波功率分配进行优化提高保密速率. 该优化问题通过寻找满足KKT一阶必要条件的解的方式求解，给出了子载波功率分配的闭式解和拉格朗日乘子的数值求解算法. 为进一步提升系统安全性能，利用OFDM系统的循环前缀提供的自由度构造了在单发送天线情况下也可使用的零空间人工噪声，并通过对子载波功率分配和人工噪声的协方差矩阵进行联合优化，最大化系统保密速率. 原始优化问题被转换为一个两层优化问题，并通过迭代获得优化问题的解. 本文在单发送天线下给出的优化方案可以很容易地推广到多发送天线的场景. 所提方案与直接传输、非优化或部分优化等方案进行了可达保密速率的仿真对比. 仿真结果表明：(1)对子载波的功率分配进行优化，可以提高系统的保密速率，在发送总功率较低时效果更明显，且TR预处理可以增强子载波功率分配对保密速率的提升效果；(2)相较于直接传输，TR预处理可在一定程度上提高保密速率，且增加天线数可以提供更多的信号传输路径，TR预处理获得的时空聚焦效果更加显著，保密速率的提升越大；(3)采用零空间人工噪声，对可达保密速率有非常明显的提升效果，且保密速率能随发送功率的增加而持续提高；(4)联合优化后系统的可达保密速率相较于未优化的系统或部分优化的系统有明显提高，说明联合优化方案不是简单的方法组合，而是能产生“1+1>2”的效果.

参考文献

[1] MUKHERJEE A, ALI A FAKOORIAN S, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: A survey[J]. IEEE Communications Surveys & Tutorials, 2014, 16(3): 1550-1573.

[2] CHEN X M, NG D W K, GERSTACKER W H, et al. A survey on multiple-antenna techniques for physical layer security[J]. IEEE Communications Surveys & Tutorials,

2017, 19(2): 1027-1053.

[3] HUO Y, TIAN Y Q, MA L R, et al. Jamming strategies for physical layer security[J]. IEEE Wireless Communications, 2018, 25(1): 148-153.

[4] KHISTI A, WORNELL G W. Secure transmission with multiple antennas I: The MISOME wiretap channel[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3088-3104.

[5] WANG B, MU P C, LI Z Z. Artificial-noise-aided beamforming design in the MISOME wiretap channel under the secrecy outage probability constraint[J]. IEEE Transactions on Wireless Communications, 2017, 16(11): 7207-7220.

[6] WANG B B, WU Y L, HAN F, et al. Green wireless communications: A time-reversal paradigm[J]. IEEE Journal on Selected Areas in Communications, 2011, 29(8): 1698-1710.

[7] TAN V T, HA D B, TRAN D D. Evaluation of physical layer secrecy in MIMO Ultra-WideBand system using Time-Reversal techniques[C]//2014 International Conference on Computing, Management and Telecommunications (ComManTel). Piscataway: IEEE, 2014: 70-74.

[8] LEI W J, ZHANG W H, YANG M M, et al. Optimization of pre-processing filter for time-reversal multi-user secure transmission systems based on artificial noise[J]. Digital Signal Processing, 2021, 109: 102933.

[9] XU Q, REN P Y, DU Q H, et al. Security-aware waveform and artificial noise design for time-reversal-based transmission[J]. IEEE Transactions on Vehicular Technology, 2018, 67(6): 5486-5490.

[10] LIU Z Q, YANG T C. On the design of cyclic prefix length for time-reversed OFDM[J]. IEEE Transactions on Wireless Communications, 2012, 11(10): 3723-3733.

[11] AMINJAVAHERI A, FARHANG A, REZAZADEHREYHANI A, et al. OFDM without CP in massive MIMO [J]. IEEE Transactions on Wireless Communications, 2017, 16(11): 7619-7633.

[12] NGUYEN T H, MONFARED S, DETERME J F, et al. Performance analysis of frequency domain precoding time-reversal MISO OFDM systems[J]. IEEE Communications Letters, 2020, 24(1): 48-51.

[13] SAMARA L, ALABBASI A O, GOUISSEM A, et al. A novel OFDM waveform with enhanced physical layer security[J]. IEEE Communications Letters, 2021, 25(2): 387-391.

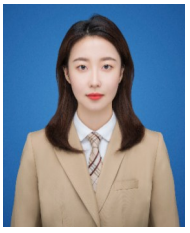
[14] QIN H H, SUN Y, CHANG T H, et al. Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs[J]. IEEE Transactions on Wireless Communications, 2013, 12(6): 2717-2729.

[15] CAO W, LI X T, LEI J, et al. Secure performance of time reversal precoding technique in MISO OFDM systems[C]//2014 Communications Security Conference (CSC 2014). Beijing: IET Press, 2014: 1-5. DOI: 10.1049/cp.2014.0753.

[16] GOLSTEIN S, NGUYEN T H, HORLIN F, et al. Physical layer security in frequency-domain time-reversal SISO OFDM communication[C]//2020 International Conference on Computing, Networking and Communications (ICNC). Piscataway: IEEE, 2020: 222-227.

作者简介

雷维嘉　男,1969年出生,云南元谋人. 博士、教授. 主要研究方向为无线和移动通信技术.
E-mail: leiwj@cqupt.edu.cn



毕文佳　女,1997年出生,河北唐山人. 硕士研究生. 主要研究方向为无线通信.
E-mail: 810316413@qq.com