空间调制系统中的人工噪声抗窃听安全传输方案

雷维嘉，兰顺福

(重庆邮电大学移动通信技术重庆市重点实验室 重庆 南岸区 400065)

【摘要】提出一种空间调制系统中利用人工噪声的物理层安全方案。通过发送天线序号和幅相调制符号来传输信息，而未发射幅相调制符号的天线发送位于合法信道零空间上的人工噪声，不影响合法接收者的信号检测，但干扰窃听者的信号检测过程。对系统保密速率、合法接收者和窃听者的误比特率上界进行理论分析，并进行仿真验证。理论和仿真结果表明合法接收者的误特率明显低于窃听者，误比特率在0.5附近，能获得可观的系统保密传输速率。

关 键 词 人工噪声； 误比特率； 物理层安全； 保密速率； 空间调制

中图分类号 TN918 **文献标志码** A doi:10.3969/j.issn.1001-0548.2018.01.002

An Anti-Eavesdropping Secure Transmission Scheme Using Artificial Noise with Spatial Modulation

LEI Wei-jia and LAN Shun-fu

(Key Lab of Mobile Communications Technology, Chongqing University of Posts and Telecommunications Nan'an Chongqing 400065)

Abstract This paper proposes a security method in the physical layer by using artificial noise and spatial modulation technique. The information is conveyed by the transmitting antenna index and amplitude-phase modulated symbol. The other antennas transmit the artificial noise located in the null space of the legitimate channel to interfere with the eavesdropper's signal detection without affecting that of the legitimate receiver. The achievable secrecy rate and bit error rate bound of both the legitimate receiver and the eavesdropper are analyzed, and the simulation is done to verify the secrecy performance of the scheme. The results show that the legitimate receiver has a much lower bit error rate than the eavesdropper, whose bit error rate is about 0.5. Thus the secrecy rate can be improved considerably.

Key words artificial noise; error bit rate; physical layer security; secrecy rate; spatial modulation

信息的安全传输是通信系统中的关键问题之一。由于无线信道传输的广播特性，传输的信号易于被非期望的接收机截获，使无线通信中信息的安全传输问题更显重要。基于计算复杂度实现信息安全的保密编码[1]是目前广泛采用的信息安全方法。物理层安全技术是另一种实现信息安全传输的途径，它利用无线信道的随机性和唯一性，通过信号处理和信道编码技术实现信息的保密传输。

物理层安全中的信号处理技术主要包括多天线技术和人工噪声技术两大类，常用的技术包括波束赋形、协作干扰和区别信道估计技术等[2]。

空间调制(spatial modulation，SM)技术是近年来新提出的一种多天线发送技术[3]，与常规的多发送天线方案中同时使用所有的天线进行信号发射不同，SM方案中每次只使用一根天线发射信号，通过不同发送天线与接收端间的信道特性差异来承载信息。SM调制器中，要传输的信息分为两部分，一部分信息对载波进行传统的幅相调制(amplitude and phase modulation, APM)，通过载波的幅度和相位传输信息；另一部分信息则控制选择一根天线发送信号，通过发送天线的序号(索引)携带信息，称为空间域调制。由于同时只有一根天线发送信号，理论上SM系统的发射机只需要配备一个射频单元，设备复杂度低于常规的多发送天线系统，同时射频部分的能量效率也更高。由于SM系统一次只使用一根发送天线，因此频谱效率不如常规的多发送天线系统，但由于其能够提高射频部分的能量效率[4-5]，设备射频部分的复杂度也更低，因此受到广泛的关注。空移键控(space shift keying, SSK)调制[6]是SM的简化形式，信息只由天线序号表征，不进行幅相调制，

收稿日期：2016－05－17；修回日期：2017－06－05
基金项目：国家自然科学基金(61471076)；重庆市教委科学技术研究项目(KJ1600413)；长江学者和创新团队发展计划(IRT1299)
作者简介：雷维嘉(1969－)，男，博士，教授，主要从事无线和移动通信技术方面的研究.

可降低调制和解调的复杂度。

有文献对SM技术在物理层安全传输中的应用进行了研究。文献[7]分析了SM系统的误码率，并对存在窃听者时合法接收者的保密互信息进行了推导，在此基础上提出了一种在发射端对发送信号进行预处理的方法，在不影响合法接收者接收的条件下，使窃听者不能检测出发送天线序号，避免其获得通过空间域调制传输的信息。文献[8]在空间调制系统中使用人工噪声，提高保密传输速率。文献[9]对存在窃听者、不采用物理层安全措施时，空间调制系统的可达保密速率进行了推导。文献[10]提出了一种多接收天线系统中空间域调制方案，与常规的SM不同，该方案采用接收天线序号来承载信息，通过发送机的预处理，可使合法者的不同接收天线上接收到的信号有明显的强度差异，从而能检测出承载的信息，而窃听者则不能，保护传输的信息不被窃听。

本文提出一种在多发送天线的SM系统中的安全传输方案。根据要传输的信息选择一根天线发送APM信号，而其他天线则发送人工噪声，并采用预编码技术，在干扰窃听者的同时不影响合法接收者的接收。对人工噪声波束赋形矢量进行设计，并推导保密速率和误比特率的上界，最后进行仿真。

1 系统模型

系统模型如图1所示。其中，Alice为配备N_t根天线的发送端，Bob和Eve分别为配备单天线的合法接收者和窃听者。记Alice的发送信号矢量为$\boldsymbol{x}$，包括携带信息的APM信号和人工噪声。$\boldsymbol{h}_b$、$\boldsymbol{h}_e \in \mathbb{C}^{1\times N_t}$ 分别为Alice与Bob、Eve间的信道系数行向量，$\boldsymbol{h}_b=[h_{ba}\ \boldsymbol{h}_{bn}]$，$\boldsymbol{h}_e=[h_{ea}\ \boldsymbol{h}_{en}]$，其中$h_{ba}$、$h_{ea}$分别是Alice发送APM信号的天线与Bob、Eve间的信道系数，$\boldsymbol{h}_{en}$、$\boldsymbol{h}_{bn} \in \mathbb{C}^{1\times(N_t-1)}$ 分别是发送人工噪声的天线与Bob、Eve间的信道系数行向量。

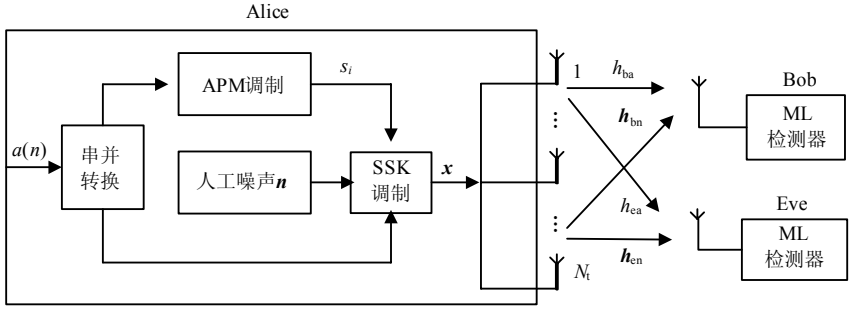

图1 系统模型

Alice将要传输的b比特信息序列$a(n)$分成长度分别为b_1和b_2比特的两部分，$b=b_1+b_2$。b_1比特用来选择发送天线，满足$N_t=2^{b_1}$；b_2比特则进行M阶APM调制，满足$b_2=\log_2(M)$，调制后的符号为s_i，$i\in\{1,2,\cdots,M\}$，且$\mathrm{E}[|s_i|^2]=1$，E[·]表示求期望运算。其他N_t-1根天线发送人工噪声$\boldsymbol{n}=\boldsymbol{w}z\in\mathbb{C}^{(N_t-1)\times 1}$，其中$\boldsymbol{w}\in\mathbb{C}^{(N_t-1)\times 1}$为人工噪声的波束赋形矢量，$z$是服从均值为0、方差为$\sigma_z^2=1$的复高斯随机变量。$\boldsymbol{w}$应使人工噪声不影响合法接收者的接收，但对窃听者产生尽可能大的干扰，同时满足人工噪声发送功率的约束。假设Alice激活第m根天线发送APM符号s_i，发送信号记为$\boldsymbol{x}_m=[\sqrt{P_s}x_{mi}\quad \boldsymbol{n}]^{\mathrm{T}}$，$P_s$为信息信号的功率，$x_{mi}$表示由第$m$根天线传输APM符号$s_i$，其中$m\in\{1,2,\cdots,N_t\}$。Bob和Eve的接收信号分别为：

$$\begin{cases} y_b=\boldsymbol{h}_{bm}\boldsymbol{x}_m+n_b=\sqrt{P_s}h_{bam}s_i+\boldsymbol{h}_{bnm}\boldsymbol{w}z+n_b \\ y_e=\boldsymbol{h}_{em}\boldsymbol{x}_m+n_e=\sqrt{P_s}h_{eam}s_i+\boldsymbol{h}_{enm}\boldsymbol{w}z+n_e \end{cases} \tag{1}$$

式中，h_{bam}、h_{eam}分别为Alice发送信号的天线与Bob、Eve间的信道系数；$\boldsymbol{h}_{bnm}=\left[h_{bn,1},h_{bn,2},\cdots,h_{bn,m-1},h_{bn,m+1},\cdots,h_{bn,N_t}\right]$、$\boldsymbol{h}_{enm}=\left[h_{en,1},h_{en,2},\cdots,h_{en,m-1},h_{en,m+1},\cdots,h_{en,N_t}\right]$分别为Alice发送人工噪声的天线与Bob、Eve间的信道系数矢量。当信道为瑞利衰落信道时，信道系数为相互独立的、服从复高斯分布的随机变量；n_b、n_e为信道噪声，服从均值为0，方差为σ_b^2、σ_e^2的复高斯分布。

Bob对接收信号进行APM和SM联合最大似然(maximum-likelihood, ML)检测：

$$[\hat{m},\hat{i}]=\arg\min_{\substack{m\in\{1,2,\cdots,N_t\}\\ i\in\{1,2,\cdots,M\}}}\left\{\left|y_b-\sqrt{P_s}h_{bam}s_i\right|^2\right\} \tag{2}$$

Eve也对接收信号进行同样的联合检测：

$$[\hat{m},\hat{i}]=\arg\min_{\substack{m\in\{1,2,\cdots,N_t\}\\ i\in\{1,2,\cdots,M\}}}\left\{\left|y_e-\sqrt{P_s}h_{eam}s_i\right|^2\right\} \tag{3}$$

2 人工噪声波束赋形矢量的设计

人工噪声不对Bob的接收产生影响，同时对窃听者产生最大的干扰，人工噪声波束赋形矢量的优化问题可表示为：

$$\begin{aligned}&\max_{\boldsymbol{w}} |\boldsymbol{h}_{en}\boldsymbol{w}|^2\\ &\text{s.t.}\quad \boldsymbol{h}_{bn}\boldsymbol{w}=0\\ &\qquad \mathrm{tr}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}})=P_{\boldsymbol{n}}\end{aligned}\tag{4}$$

式中，$P_{\boldsymbol{n}}$为人工噪声功率；$|\cdot|$表示求模运算；tr(·)表示矩阵的迹；约束条件$\boldsymbol{h}_{bn}\boldsymbol{w}=0$表示人工噪声在合法接收者处为零。

设$\boldsymbol{U}_{\perp}$为$\boldsymbol{h}_{bn}$零空间的投影矩阵，$\boldsymbol{h}_{bn}\boldsymbol{U}_{\perp}=0$，$\boldsymbol{U}_{\perp}=\boldsymbol{I}_{N_t-1}-\boldsymbol{h}_{bn}^{\mathrm{H}}(\boldsymbol{h}_{bn}\boldsymbol{h}_{bn}^{\mathrm{H}})^{-1}\boldsymbol{h}_{bn}$ [11]。令$\boldsymbol{w}=\boldsymbol{U}_{\perp}\boldsymbol{w}'$。为使$|\boldsymbol{h}_{en}\boldsymbol{w}|^2=|\boldsymbol{h}_{en}\boldsymbol{U}_{\perp}\boldsymbol{w}'|^2$最大，$\boldsymbol{w}'$应与$\boldsymbol{h}_{en}\boldsymbol{U}_{\perp}$共线，故$\boldsymbol{w}'=\boldsymbol{U}_{\perp}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}$，则$\boldsymbol{w}'=\boldsymbol{U}_{\perp}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}$，因此$\boldsymbol{w}=\boldsymbol{U}_{\perp}\boldsymbol{U}_{\perp}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}$。由$\boldsymbol{U}_{\perp}$的表达式可知$\boldsymbol{U}_{\perp}=\boldsymbol{U}_{\perp}^{\mathrm{H}}$和$\boldsymbol{U}_{\perp}\boldsymbol{U}_{\perp}=\boldsymbol{U}_{\perp}$，所以$\boldsymbol{w}=\boldsymbol{U}_{\perp}\boldsymbol{h}_{en}^{\mathrm{H}}$。进一步得到满足功率约束条件$\mathrm{tr}(\boldsymbol{w}\boldsymbol{w}^{\mathrm{H}})=P_{\boldsymbol{n}}$的波束赋形矢量为$\boldsymbol{w}=\dfrac{\sqrt{P_{\boldsymbol{n}}}\boldsymbol{U}_{\perp}\boldsymbol{h}_{en}^{\mathrm{H}}}{\left\|\boldsymbol{U}_{\perp}\boldsymbol{h}_{en}^{\mathrm{H}}\right\|}=\sqrt{P_{\boldsymbol{n}}}\boldsymbol{g}$，其中$\boldsymbol{g}=\dfrac{\boldsymbol{U}_{\perp}\boldsymbol{h}_{en}^{\mathrm{H}}}{\left\|\boldsymbol{U}_{\perp}\boldsymbol{h}_{en}^{\mathrm{H}}\right\|}$。

将$\boldsymbol{w}=\sqrt{P_{\boldsymbol{n}}}\boldsymbol{g}$代入式(1)，Bob和Eve的接收信号又可表示为：

$$\begin{cases}y_{\mathrm{b}}=\sqrt{P_s}h_{bam}s_i+n_{\mathrm{b}}\\ y_{\mathrm{e}}=\sqrt{P_s}h_{eam}s_i+\sqrt{P_{\boldsymbol{n}}}\boldsymbol{h}_{enm}\boldsymbol{g}_m z+n_{\mathrm{e}}\end{cases}\tag{5}$$

3 保密性能分析

3.1 保密速率和信号与人工噪声的功率分配

Alice的发射功率分别用于发送APM信号和人工噪声。设总功率为P，分配给APM信号的功率为$P_s=\rho P$，其中ρ为功率分配因子，相应分配给人工噪声的功率为$P_{\boldsymbol{n}}=(1-\rho)P$。经过与文献[12]类似的推导过程，可得Alice与Bob和Eve间的瞬时信道容量分别为：

$$\begin{cases}C_{\mathrm{b}}=\log_2\left(1+\dfrac{P_s}{N_t\sigma_{\mathrm{b}}^2}\left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2\right)\\ C_{\mathrm{e}}=\log_2\left(1+\dfrac{P_s\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2}{N_t\left(\left|\boldsymbol{h}_{en}\boldsymbol{w}\right|^2+\sigma_{\mathrm{e}}^2\right)}\right)=\log_2\left(1+\dfrac{P_s\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2}{N_t(P_{\boldsymbol{n}}\boldsymbol{h}_{en}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}+\sigma_{\mathrm{e}}^2)}\right)\end{cases}\tag{6}$$

式中，$\|\cdot\|$表示向量的范数。瞬时可达保密速率为：

$$\begin{aligned}R_{\mathrm{s}}=&[C_{\mathrm{b}}-C_{\mathrm{e}}]^+=\left[\log_2\left(1+\frac{P_s}{N_t\sigma_{\mathrm{b}}^2}\left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2\right)-\right.\\ &\left.\log_2\left(1+\frac{P_s\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2}{N_t(P_{\boldsymbol{n}}\boldsymbol{h}_{en}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}+\sigma_{\mathrm{e}}^2)}\right)\right]^+=\\ &\left[\log_2\left(1+\frac{\rho P}{N_t\sigma_{\mathrm{b}}^2}\left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2\right)-\right.\\ &\left.\log_2\left(1+\frac{\rho P\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2}{N_t((1-\rho)P\boldsymbol{h}_{en}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}+\sigma_{\mathrm{e}}^2)}\right)\right]^+\end{aligned}\tag{7}$$

式中，$[\alpha]^+=\max\{0,\alpha\}$。可见保密速率是功率分配因子$\rho$的函数，其取值范围为$0<\rho\leqslant 1$。通过分析$\rho$对合法接收者和窃听者的影响可知，保密容量不是$\rho$的单调函数，存在使系统保密速率最大的$\rho$值。

记$a_1=\left\|\boldsymbol{h}_{\mathrm{b}}\right\|^2$，$a_2=\left\|\boldsymbol{h}_{\mathrm{e}}\right\|^2$，$a_3=\sigma_{\mathrm{b}}^2$，$a_4=\sigma_{\mathrm{e}}^2$，$a_5=N_t$，$a_6=\boldsymbol{h}_{en}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}$。保密速率可简写为：

$$R_{\mathrm{s}}=\left[\log_2\left(1+\frac{a_1P\rho}{a_3a_5}\right)-\log_2\left(1+\frac{a_2P\rho}{a_5(a_6P(1-\rho)+a_4)}\right)\right]^+\tag{8}$$

令：

$$\begin{aligned}f(\rho)=&\log_2\left(1+\frac{a_1P\rho}{a_3a_5}\right)-\\ &\log_2\left(1+\frac{a_2P\rho}{a_5(a_6P(1-\rho)+a_4)}\right)\end{aligned}\tag{9}$$

最优的ρ值是在其取值范围内使$f(\rho)$最大的值，可能是$f(\rho)$函数的极值点，即其一阶导数为零时在(0,1)范围内的解，也可能是边界点1。$f(\rho)$的一阶导数如式(10)所示，其为零的解也就是其分子为零的解，即式(11)所示的一元二次方程的解，如式(12)所示。式(12)在(0,1)内的解为极值点，其对应的保密速率与边界点1对应的保密速率中的最大值即为该信道条件下最大可达保密速率。

$$\frac{\mathrm{d}f(\rho)}{\mathrm{d}\rho}=\frac{1}{\ln 2}\left(\frac{a_1P(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)}{(a_1P\rho+a_3a_5)(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)}-\right.$$
$$\left.\frac{(a_1P\rho+a_3a_5)(a_2a_4a_5P+a_2a_5a_6P^2)}{(a_1P\rho+a_3a_5)(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)}\right) \tag{10}$$

$$a_1P(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)-(a_1P\rho+a_3a_5)(a_2a_4a_5P+a_2a_5a_6P^2)=0 \tag{11}$$

$$\rho=\frac{a_1a_4a_5a_6+a_1a_5a_6^2P\pm\sqrt{a_1a_2a_5a_6(a_4+a_6P)(a_1a_4-a_2a_3+a_3a_5a_6+a_1a_6P)}}{a_1a_5a_6^2P-a_1a_2a_6P} \tag{12}$$

遍历保密速率为：

$$R_{\mathrm{se}}=E_{h_{\mathrm{ba}},h_{\mathrm{ea}},\boldsymbol{h}_{\mathrm{bn}},\boldsymbol{h}_{en}}\left\{\left[\log_2\left(1+\frac{P_s}{N_{\mathrm{t}}\sigma_{\mathrm{b}}^2}\|\boldsymbol{h}_{\mathrm{b}}\|^2\right)-\right.\right.$$
$$\left.\left.\log_2\left(1+\frac{P_s\|\boldsymbol{h}_{\mathrm{e}}\|^2}{N_{\mathrm{t}}(P_{\boldsymbol{n}}\boldsymbol{h}_{en}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}_{en}^{\mathrm{H}}+\sigma_{\mathrm{e}}^2)}\right)\right]^+\right\} \tag{13}$$

式中，$E_{h_{\mathrm{ba}},h_{\mathrm{ea}},\boldsymbol{h}_{\mathrm{bn}},\boldsymbol{h}_{en}}\{\cdot\}$表示对Alice与Bob、Eve间的信道系数求统计平均；$\|\boldsymbol{h}_{\mathrm{b}}\|^2=|h_{\mathrm{b1}}|^2+|h_{\mathrm{b2}}|^2+\cdots+|h_{\mathrm{b}N_{\mathrm{t}}}|^2$和$\|\boldsymbol{h}_{\mathrm{e}}\|^2=|h_{\mathrm{e1}}|^2+|h_{\mathrm{e2}}|^2+\cdots+|h_{\mathrm{e}N_{\mathrm{t}}}|^2$为特殊形式的广义卡方分布随机变量[13]；$\boldsymbol{h}_{en}$和$\boldsymbol{g}$是高斯随机变量；求解式(13)需要进行非常复杂的多重积分，无法得到解析表达式。

3.2 Bob和Eve的错误概率

由于精确的误比特率难以获得，这里改为通过推导成对差错概率来获得平均误比特率的上界。

SM信号进行ML检测后，误比特率$P_{(s,m)}$的联合上界为：

$$P_{(s,m)}\leqslant\frac{1}{N_{\mathrm{t}}M}\sum_{m=1}^{N_{\mathrm{t}}}\sum_{i=1}^{M}\sum_{\substack{k=1\\(k,j)\neq(m,i)}}^{N_{\mathrm{t}}}\sum_{j=1}^{M}$$
$$\{d(x_{mi},x_{kj})\mathrm{E}[P_{\mathrm{r}}(x_{mi}\to x_{kj})]\} \tag{14}$$

式中，$P_{\mathrm{r}}(x_{mi}\to x_{kj})$表示将激活天线$m$、APM符号$s_i$组合错判成激活天线$n$、APM符号$s_j$组合的成对差错概率；$\frac{1}{N_{\mathrm{t}}M}\sum_{m=1}^{N_{\mathrm{t}}}\sum_{i=1}^{M}\sum_{\substack{k=1\\(k,j)\neq(m,i)}}^{N_{\mathrm{t}}}\sum_{j=1}^{M}$为对所有APM符号和激活天线组合求平均；$d(x_{mi},x_{kj})$表示激发天线$m$、APM符号$s_i$组合所对应的比特序列与激活天线$k$、APM符号$s_j$组合所对应的比特序列的汉明距离。

对于Bob，其$P_{\mathrm{r}}(x_{mi}\to x_{nj})$为：

$$\mathrm{P_r}(x_{mi}\to x_{kj})=$$
$$P_{\mathrm{r}}(\left|y_{\mathrm{b}}-\sqrt{P_s}h_{\mathrm{bam}}s_i\right|^2>\left|y_{\mathrm{b}}-\sqrt{P_s}h_{\mathrm{bak}}s_j\right|^2)=$$
$$P_{\mathrm{r}}(P_s|h_{\mathrm{bam}}|^2|s_i|^2-2\mathrm{Re}(y_{\mathrm{b}}^*\sqrt{P_s}h_{\mathrm{bam}}s_i)>$$
$$P_s|h_{\mathrm{bak}}|^2|s_j|^2-2\mathrm{Re}(y_{\mathrm{b}}^*\sqrt{P_s}h_{\mathrm{bak}}s_j))=$$
$$P_{\mathrm{r}}(\mathrm{Re}(n_{\mathrm{b}}\sqrt{P_s}h_{\mathrm{bak}}^*s_j^*)-\mathrm{Re}(n_{\mathrm{b}}\sqrt{P_s}h_{\mathrm{bam}}^*s_i^*)>$$
$$P_s|h_{\mathrm{bam}}s_i-h_{\mathrm{bak}}s_j|^2/2) \tag{15}$$

式中，最后一个等号右边$\mathrm{P_r}$内大于号的左边为均值为0、方差为$P_s\left|h_{\mathrm{bam}}s_i-h_{\mathrm{bak}}s_j\right|^2\sigma_{\mathrm{b}}^2/2$的高斯随机变量，因此有：

$$P_{\mathrm{r}}(x_{mi}\to x_{kj})=Q\left(\sqrt{\frac{P_s\left|h_{\mathrm{bam}}s_i-h_{\mathrm{bak}}s_j\right|^2}{2\sigma_{\mathrm{b}}^2}}\right) \tag{16}$$

代入式(14)，得Bob误比特率的上界为：

$$P_{(s,m),\mathrm{b}}\leqslant\frac{1}{N_{\mathrm{t}}M}\sum_{m=1}^{N_{\mathrm{t}}}\sum_{i=1}^{M}\sum_{\substack{k=1\\(k,j)\neq(m,i)}}^{N_{\mathrm{t}}}\sum_{j=1}^{M}$$
$$\left\{d(x_{mi},x_{kj})\mathrm{E}\left[Q\left(\sqrt{\frac{P_s\left|h_{\mathrm{bam}}s_i-h_{\mathrm{bak}}s_j\right|^2}{2\sigma_{\mathrm{b}}^2}}\right)\right]\right\} \tag{17}$$

在瑞利衰落信道下，上式中h_{bam}和h_{bak}为复高斯随机变量，类似文献[14]，求取统计平均后得到：

$$P_{(s,m),\mathrm{b}}\leqslant\frac{N_{\mathrm{t}}}{M}\sum_{i=1}^{M}\sum_{\substack{j=1\\j\neq i}}^{M}\left\{d(x_i,x_j)\frac{1}{2}\left(1-\sqrt{\frac{\sigma_{\mathrm{lb}}^2}{1+\sigma_{\mathrm{lb}}^2}}\right)\right\} \tag{18}$$

式中，$\sigma_{\mathrm{lb}}^2=\sigma_{\mathrm{b}\boldsymbol{h}}^2\gamma_{\mathrm{b}}(|s_i|^2+|s_j|^2)$；$\gamma_{\mathrm{b}}=P_s/4\sigma_{\mathrm{b}}^2$；$\sigma_{\mathrm{b}\boldsymbol{h}}^2$为Alice与Bob间的信道系数方差。

对Eve而言，其接收信号y_{e}中的噪声包括人工噪声和信道噪声，即$n_{\mathrm{ea}}=\boldsymbol{h}_{en}\boldsymbol{n}+n_{\mathrm{e}}$，服从均值为0、方差为$\sigma_{n_{\mathrm{ea}}}^2=P_{\boldsymbol{n}}\boldsymbol{h}_{en}\boldsymbol{g}\boldsymbol{g}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{en}}^{\mathrm{H}}+\sigma_{\mathrm{e}}^2$的复高斯分布。将Eve的接收信号改写为：

$$y_{\mathrm{e}}=\sqrt{P_s}h_{\mathrm{eam}}s_i+n_{\mathrm{ea}} \tag{19}$$

采用与推导Bob误比特率类似的方法，可得Eve的误比特率的上界为：

$$P_{(s,m),\mathrm{e}} \leqslant \frac{N_\mathrm{t}}{M}\sum_{i=1}^{M}\sum_{\substack{j=1\\ j\neq i}}^{M}\left\{d(x_i,x_j)\frac{1}{2}\left(1-\sqrt{\frac{\sigma_{\mathrm{1e}}^2}{1+\sigma_{\mathrm{1e}}^2}}\right)\right\} \quad (20)$$

式中，$\sigma_{\mathrm{1e}}^2=\sigma_{\mathrm{e}\boldsymbol{h}}^2\gamma_\mathrm{e}(|s_i|^2+|s_j|^2)$；$\gamma_\mathrm{e}=P_s/4\sigma_{n_\mathrm{ea}}^2$；$\sigma_{\mathrm{e}\boldsymbol{h}}^2$为Alice与Eve间的信道系数方差。

4　仿真分析

对系统的保密速率、Bob和Eve的误比特率进行仿真。仿真中所有信道均是相互独立、方差为1的瑞利平坦衰落信道，所有信道噪声的方差均归一化为0 dBm。

图2为N_t=4时，不同功率分配因子ρ值下平均保密速率随总功率P变化的曲线。可见，相比较采用固定的ρ值，采用优化后的ρ值可获得更大的保密速率。

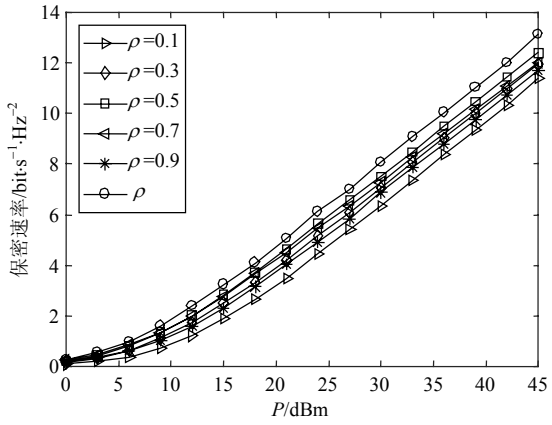

图2　不同功率分配因子时的保密速率

图3为N_t=4时，APM采用QPSK星座时，不同ρ值下Bob和Eve的误比特率随总功率P的变化曲线。图中实线为仿真值，虚线为理论上界。可见仿真值与理论上界值非常接近，表明本文推导得到的上界是一个紧界。而ρ越大，信号功率越大，人工噪声功率越小，Bob和Eve的误比特率就越低。Bob的误比特率要远低于Eve的误比特率，二者误比特率的差距越大，则保密速率就越大。ρ取最优值时，Eve的误比特率保持在0.5附近，说明其基本不能获得任何Alice发送的信息。

图4是本文方案与文献[7]方案Bob和Eve误比特率的对比。与本文类似，文献[7]方案也采用空间调制技术，不同之处在于该方案在发送端对发送信号进行预处理，在不影响合法接收者接收的前提下，使窃听者不能检测发送天线，无法获取通过天线索引携带的信息，但没有采用人工噪声。仿真中N_t=4，APM采用QPSK星座，两方案的频谱效率相同。由于本文方案中人工噪声消耗了部分功率，因此本文方案Bob的误比特率稍高。但文献[7]方案中没有针对APM符号信息的保护措施，相应Eve的误比特率也要低于本文方案的Eve的误比特率(本文方案约为0.5)。因此本文方案中窃听者几乎不能窃取到任何有用信息，保密性能优于文献[7]方案。

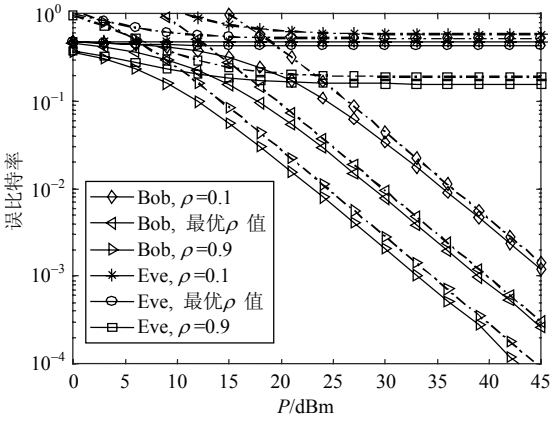

图3　不同功率分配因子下Bob和Eve的误比特率

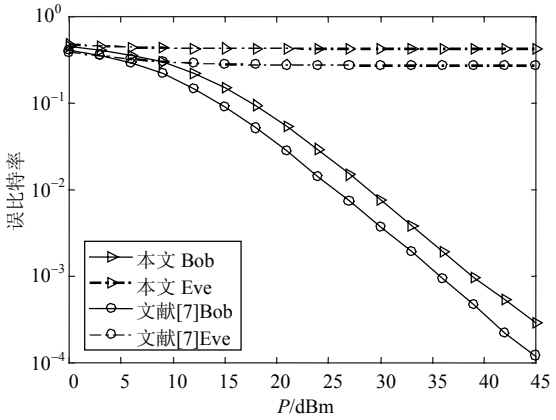

图4　本文方案与文献[7]方案误比特率的对比

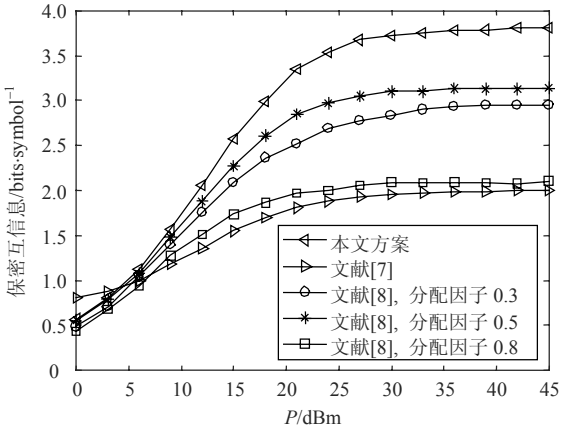

图5　本文方案与文献[7-8]方案保密互信息对比

图5是本文方案与文献[7-8]方案的保密互信息的对比，保密互信息采用文献[7]的方法计算。仿真

中N_t=4，APM采用QPSK星座，频谱效率所有方案均相同。文献[8]方案中，由于窃听者信道状态信息未知，不能进行功率分配的优化，仿真中选取了0.3、0.5、0.8的3个功率分配因子进行仿真。在极低信噪比下，文献[7]方案的性能较好，但信噪比增加时，其保密互信息的增长速度低于文献[8]方案和本文方案，在高信噪比下性能反而较差。而本文方案的保密互信息始终高于文献[8]方案，能获得更好的保密传输性能，主要原因在于本文方案对功率分配因子进行了优化。

5 结 束 语

本文给出了一种空间调制系统中利用人工噪声的安全传输方案。通过利用未发送APM信号的天线发送人工噪声，干扰窃听者对APM信号和发送天线序号的检测，同时设计人工噪声的波束赋形矢量，使其不对合法接收者造成影响。对系统的保密速率、合法接收者和窃听者的误比特率上界进行了推导；对消息信号和人工噪声的功率分配进行了优化。对系统保密速率、合法接收者和窃听者的误比特率进行了仿真，误比特率上界正确，而且是一个紧界。另外还与其他方案进行了性能的仿真对比，表明本文方案具有较好的保密传输性能。在发送端天线数较多的情况下，可以考虑同时激活多根发送天线改为采用广义空间调制。通过优化安排激活的发送信号天线和发送人工噪声天线的数量，并采用适当的发送信号预编码方案，可进一步提高安全传输性能，这是下一步深入研究的问题。

参 考 文 献

[1] MASSEY J L. An introduction to contemporary cryptology[J]. IEEE Proceeding, 1988, 76(5): 533-549.

[2] SHIU Y S, CHANG S Y, WU H C, et al. Physical layer security in wireless networks: a tutorial[J]. IEEE Wireless Communications, 2011, 18(2): 66-74.

[3] RENZO M D, HAAS H, SINANOVIC S, et al. Spatial modulation[J]. IEEE Transactions on Vehicular Technology, 2008, 57(4): 2228-2241.

[4] ZHENG J P, SUN Y. Energy-efficient spatial modulation over MIMO frequency-selective fading channels[J]. IEEE Transactions on Vehicular Technology, 2015, 64(5): 2204-2209.

[5] KEIGO T. Spatial modulation achieves information theoretically optimal energy efficiency[J]. IEEE Wireless Communications Letters, 2015, 19(7): 1133-1136.

[6] RENZO M D, LEONARDIS D D, GRAZIOSI F, et al. Space shift keying (SSK-) MIMO with practical channel estimates[J]. IEEE Transactions on Communications, 2012, 60(4): 998-1012.

[7] GUAN X R, CAI Y M, YANG W W. On the secrecy mutual information of spatial modulation with Finite alphabet[C]//International Conference on Wireless Communications and Signal Processing (WCSP). Huangshan: [s.n.], 2012: 1-4.

[8] WANG L, BASHAR S F, WEI Y M, et al. Secrecy enhancement analysis against unknown eavesdropping in spatial modulation[J]. IEEE Wireless Communications Letters, 2015, 19(8): 1351-1354.

[9] SINANOVIC S, SREAFIMOVSKI N, RENZO M D, et al. Secrecy capacity of space keying with two antennas[C]// IEEE Vehicular Technology Conference. Quebec: IEEE, 2012: 1-5.

[10] WU F L, YANG L L, wANG W J, et al. Secret precoding-aided spatial modulation[J]. IEEE Wireless Communications Letters, 2015, 19(9): 1544-1547.

[11] DONG L, HAN Z, PETROPULU A P, et al. Improving wireless physical layer security via cooperating relays[J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875-1888.

[12] YOUNIS A, BASNAYAKA D A, HAAS H. Performance analysis for generalised spatial modulation[C]//20th European Wireless Conference. Barcelona, Spain: VED, 2014: 1-6.

[13] BJÖRNSON E, HAMMARWAII D, OTTERSTEN B. Exploiting quantized channel norm feedback through conditional statistics in arbitrarily correlated MIMO systems[J]. IEEE Transactions on Signal Processing, 2009, 57(10): 4027-4041.

[14] JEGANATHAN J, GHRAYEB A, SZCZECINSKI L. Spatial modulation: Optimal detection and performance analysis[J]. IEEE Communications Letters, 2008, 12(8): 545-547.

编 辑 税 红