DOI:10.11918/j.issn.0367-6234.201606111

广义空间调制系统中的物理层抗窃听传输方案

雷维嘉, 兰顺福

(移动通信技术重庆市重点实验室(重庆邮电大学),重庆 400065)

摘 要: 为实现信息的保密传输,提出一种基于广义空间调制技术的物理层安全方案. 发射端根据合法信道的状态信息对信号进行预处理,使合法接收者接收到来自各激活发射天线的信号相位对齐,并对不同激活天线组合的信号进行不同的相位旋转,提高合法接收者的接收性能. 而窃听者接收到的信号相位仍然为随机分布,接收性能远低于合法接收者,有效地保护通过天线索引传输的信息. 发送端同时发送指向窃听者的人工噪声,保护通过幅相调制携带的信息不被窃听. 对保密容量、误码性能和信号与人工噪声的功率分配进行理论分析,仿真结果表明,通过合理分配功率,合法接收者的误码性能明显优于窃听者,能获得可观的系统保密容量.

关键词: 物理层安全;广义空间调制;人工噪声;保密容量;抗窃听

中图分类号: TN918.91 **文献标志码**: A **文章编号**: 0367-6234(2017)05-0087-07

Anti-eavesdropping transmission method with generalized spatial modulation in physical layer

LEI Weijia, LAN Shunfu

(Chongqing Key Laboratory of Mobile Communication Technology(Chongqing University of Posts and Telecommunications), Chongqing 400065, China)

Abstract: For safety transmission, a security method in the physical layer is proposed based on generalized spatial modulation technique. The transmitter pretreats the signals according to the state information of the legal channel so that phases of all signals sent by different antennas are identical at the legal receiver. At the same time, different additional phase shift is imposed when different combination of the activated antennas is used, so the performance of the legitimate user is improved. However, phases of signals sent by different antennas are random at the eavesdropper, thus its performance is significantly lower than that of the legitimate user so that the information conveyed by the antenna index is protected. Artificial noise pointed to the eavesdropper is sent simultaneously at the transmitter to safeguard the information conveyed by amplitude and phase modulation symbols. Then the secrecy capacity, error performance and power assignment between signal and artificial noise are analyzed. The simulation results show that the legitimate receiver's error performance is superior to that of the eavesdropper, and a considerable secrecy capacity can be obtained.

Keywords: physical layer security; generalized spatial modulation; artificial noise; secrecy capacity; anti-eavesdropping

无线通信中,由于信号传输的开放性,信息的安全传输是一个重要的问题. 采用保密编码的加密技术是信息保密的传统技术,而近年来利用无线信道随机性的物理层安全方法正越来越受到关注. 应用多天线技术实现信息的安全传输是物理层安全技术研究中的热点问题之一. 文献[1]提出使用波束赋形的技术来实现物理层安全,中继和协作干扰技术也是提高无线通信保密传输性能的有效手段[2-4].

空间调制 SM(spatial modulation)技术[5]是一种多天线传输技术,通过不同收发天线间信道特性的差异来传递消息. 在 SM 的调制器中,比特信息分为两部分:一部分在信号域进行传统的幅相调制 APM (amplitude and phase modulation); 另一部分在空间域进行调制,选择性地激活一根天线来传输信号. 广义空间调制 GSM(generalized spatial modulation)技术[6]则对发射天线进行不同组合,每次由多根激活天线发送信号. 相比较 SM 系统,GSM 系统具有更高的频谱效率,但系统复杂度也更高. SM 和 GSM 系统中,只同时激活部分天线,发射机需要的射频单元数量少于传统的多天线系统,在射频部分具有更高的能量效率[7]. 文献[8-10]讨论了 GSM 信号的检

收稿日期: 2016-06-30
基金项目: 国家自然科学基金(61471076);重庆市基础与前沿研究计划(cstc2015jcyjA40047);长江学者和创新团队发展计划(IRT1299);重庆市科委重点实验室专项经费
作者简介: 雷维嘉(1969—),男,教授
通信作者: 兰顺福,L3315568@126.com

测方法,文献[11]分析了 GSM 系统的互信息,并对系统误码性能进行了分析. 目前,有少量的文献对空间调制技术在保密传输中的应用进行了研究. 文献[12]假设发送端能获得窃听者信道状态信息 CSI (channel state information),对 SM 系统的误码率和保密互信息进行了推导,提出在发射端对信息进行预处理,可使合法接收者能正常进行 SM 调制信号的解调,但窃听者不能区分发送天线,无法解调映射到天线索引上的信息. 文献[13]采用接收天线索引来表示信息,通过合理设计发送端的预处理向量,可使接收端能够判断哪根接收天线上有接收信号,从而根据接收天线索引获得发送的信息,而窃听者不能区分,这样能获得一定的保密传输速率.

本文研究多发送天线系统中应用 GSM 技术实现信息的保密传输. 系统中的发射端在发送空间调制后的信号前进行预处理,使各激活天线发送的信号到达合法接收者天线时具有相同的相位,增强接收信号信噪比,同时使合法接收者处的空间星座点等相位间隔分布,降低误码率. 而各激活天线发送的信号到达窃听者接收天线时的相位是随机的,其空间调制部分的解调误码率远高于合法接收者,有效保护通过天线索引部分携带的信息.

1 系统模型

系统模型如图 1 所示,包括 3 个节点, 其中 Alice 为装备 N_t 根天线的发送端,向两个单天线节点发送信息. 两个单天线节点都是系统的用户,但发送给其中一个节点的信息需要对另一个节点保密. 不失一般性,称某时刻接收保密信息的节点为合法接收者 Bob,而另一个节点称为窃听者 Eve. 记每传输时隙 Alice 的发射信号为 $\boldsymbol{X}$,$\boldsymbol{H}_b \in \mathbb{C}^{1\times N_t}$ 为 Alice 与 Bob 间的信道系数组成的向量, $\boldsymbol{H}_e \in \mathbb{C}^{1\times N_t}$ 为 Alice 与 Eve 间的信道系数组成的向量. 因为 Bob 和 Eve 都是系统用户,都需要接收来自发送端 Alice 的消息,Alice 可要求他们向其反馈 CSI,因此假设 Alice 可获得所有信道准确的 CSI. 本文方案中信号和人工噪声的处理权值以信道的 CSI 为依据进行设置. 无线信道是时变信道,在信道的相干时间相比较传输符号周期较大时,信道为慢衰落信道. 在信道相干时间范围内,信道特性的变化很小,发送端采用相同的信号和人工噪声处理权值. 终端根据信道的变化速度周期性地向发送端反馈 CSI,发送端据此调整权值.

每传输时隙,Alice 将 B 比特的信息序列 $a(n)$ 分成 B_1 比特和 B_2 比特两部分,$B = B_1 + B_2$. 每组数据的前 B_1 比特用来选择所有发射天线组合 2^{B_1} 中的一种,激活天线组合的数目为 $N_c = 2^{B_1}$, 其中 $B_1 = \lfloor \log_2(C_{N_t}^{N_a}) \rfloor$,$\lfloor\cdot\rfloor$ 表示向下取整函数, C_m^n 是二项式系数,N_a 为每次传输时所激活的天线数目,$1 \leqslant N_a < N_t$. 另外 B_2 比特数据则进行 M 阶 APM 调制, $B_2 = \log_2(M)$,M 是 APM 调制的阶数,调制后的符号为 s_i,$i \in \{1, 2, \cdots, M\}$, 满足 $E[|s_i|^2] = 1$,$E[\cdot]$ 表示求期望运算. 发送端根据其与 Bob 间的 CSI 对 s_i 进行预处理,得到激活天线的发送信号向量 $\boldsymbol{x}_{mi} \in \mathbb{C}^{N_a\times 1}$, 其中下标 $m \in \{1, 2, \cdots, N_c\}$ 表示选择的激活天线组合中的第 m 种. x_{mi} 包含经过预处理的 APM 符号和人工噪声 $\boldsymbol{n}$: $\boldsymbol{x}_{mi} = \boldsymbol{w}_m s_i + \boldsymbol{n}_m$. $\boldsymbol{w}_{mi} \in \mathbb{C}^{N_a\times 1}$ 是预处理向量,其作用是使各激活天线发送的信号在到达 Bob 接收天线时在同一相位上对齐,增强接收信号强度;同时使不同激活天线组合发射的同一 APM 符号间在相邻 APM 星座点间是等相位间隔分布的,改善误码性能. 而 Eve 的接收信号并不具备上述特性. $\boldsymbol{n} = \boldsymbol{g}_m z \in \mathbb{C}^{N_a\times 1}$ 是人工噪声, 其中 $\boldsymbol{g}_m$ 表示干扰信号的波束赋形矢量,z 是一个服从均值为 0、方差为 $\sigma_z^2 = 1$ 的复高斯随机变量. 人工噪声定向指向窃听者,对其产生极大干扰. 经过以上处理,Bob 的接收性能要明显优于 Eve 的接收性能. 天线发射的信号向量为 $\boldsymbol{X} = [\cdots, 0, x_{mi,1}, 0, \cdots, 0, x_{mi,2}, 0, \cdots, 0, x_{mi,N_a}, 0, \cdots]^T$, 上标 T 表示转置运算. $\boldsymbol{X}$ 中共有 N_a 个不为 0 的元素,其所在的位置表示激活状态的天线序号,该天线发射信号为 $x_{mi,k}$,$1 \leqslant k \leqslant N_a$.

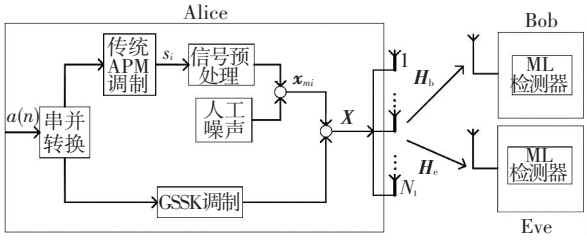


图 1 GSM 安全传输系统模型

Fig.1 Model of secure transmission system with GSM

经过信道传输后,Bob 和 Eve 接收到信号为

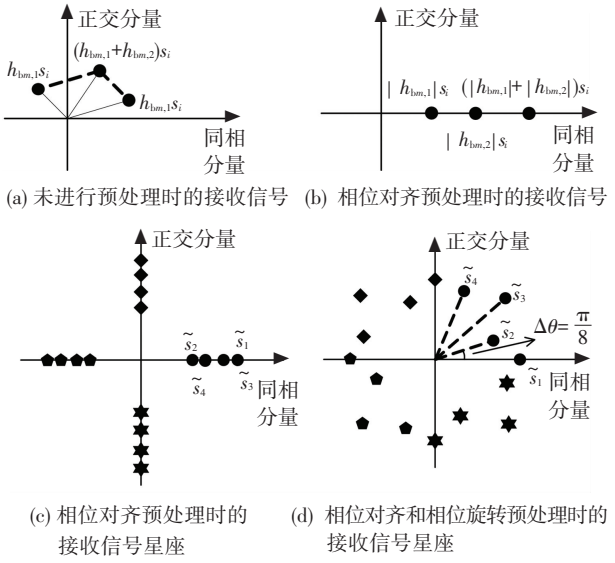
$$\begin{cases} y_b = \boldsymbol{H}_{bm}\boldsymbol{X} + n_b = \sum_{k=1}^{N_a}(h_{bm,k}x_{mi,k}) + n_b = \boldsymbol{h}_{bm}\boldsymbol{x}_{mi} + n_b, \\ y_e = \boldsymbol{H}_{em}\boldsymbol{X} + n_e = \sum_{k=1}^{N_a}(h_{em,k}x_{mi,k}) + n_e = \boldsymbol{h}_{em}\boldsymbol{x}_{mi} + n_e. \end{cases} \tag{1}$$

式中: $\boldsymbol{h}_{bm} = [h_{bm,1}, h_{bm,2}, \cdots, h_{bm,N_a}]$、$\boldsymbol{h}_{em} = [h_{em,1}, h_{em,2}, \cdots, h_{em,N_a}]$ 分别表示 Alice 的激活天线与 Bob、Eve 接收天线间的信道系数向量,对于瑞利衰落信道,其元素为服从独立同分布的复高斯随机变量; n_b、n_e 是均值为 0,方差为 σ_b^2、σ_e^2 的复高斯白噪声. 将 $\boldsymbol{x}_{mi} = \boldsymbol{w}_m s_i + \boldsymbol{n}$ 代入(1),接收信号可进一步表示为

$$y_{\mathrm{b}} = \boldsymbol{h}_{\mathrm{bm}}(\boldsymbol{w}_m s_i + \boldsymbol{n}) + n_{\mathrm{b}} = \boldsymbol{h}_{\mathrm{bm}}\boldsymbol{w}_m s_i + \boldsymbol{h}_{\mathrm{bm}}\boldsymbol{g}_m z + n_{\mathrm{b}},$$
$$y_{\mathrm{e}} = \boldsymbol{h}_{em}(\boldsymbol{w}_m s_i + \boldsymbol{n}) + n_{\mathrm{e}} = \boldsymbol{h}_{em}\boldsymbol{w}_m s_i + \boldsymbol{h}_{em}\boldsymbol{g}_m z + n_{\mathrm{e}}. \quad (2)$$

2　预处理向量和人工噪声向量的设计

预处理向量 $\boldsymbol{w}_{\mathrm{m}}$ 设计的目标是使各激活天线发射的承载信息的幅相调制符号 s_i 到达 Bob 的接收天线时在相位上是对齐的，同时使不同激活天线组合的合成信号相位在相邻的 APM 调制符号的相位间隔范围内是等相位间隔分布的. 图 2 给出了 $N_{\mathrm{t}} = 4$、$N_{\mathrm{a}} = 2$，采用 QPSK 调制时，发送信号的预处理过程示意图，图中表示的都是无噪声情况下的信号. 图 2(a)表示 Alice 未对信号进行预处理时，到达 Bob 接收天线的两个信号及其合成信号的示意图，s_i 为 APM 调制符号，这里假设其相位为 0，$(h_{\mathrm{bm},1} + h_{\mathrm{bm},2})s_i$ 为合成信号. 由于信道的随机性，两个激活天线发射的信号在达到 Bob 接收天线时相互叠加的结果有可能使信号增强，也可能使信号减弱. 图 2(b)中，Alice 根据信道的特性对发送信号用因子 $\mathrm{e}^{-\mathrm{j}\theta_k}$ 进行预加权，使各激活天线发送的信号到达 Bob 接收天线时相位都对齐到 0 相位，增强接收信号. 图 2(c)是 Alice 对信号进行相位对齐预处理后 Bob 接收信号的星座图，同相和正交轴上的 4 组信号点分别对应 QPSK 的 4 种符号. 为了增大同一个 APM 符号下不同激活天线组合对应信号点间的距离，Alice 在发送信号上进一步附加一个不同相位偏移，使这些信号点在相位相邻的两个 APM 符号间等相位间隔分布，如图 2(d)所示. 对于幅相调制采用 QPSK 的情形，对激活天线组合 m 附加的相位偏移为 $\theta_m = (m-1)\pi/8$.



(a) 未进行预处理时的接收信号　(b) 相位对齐预处理时的接收信号

(c) 相位对齐预处理时的接收信号星座　(d) 相位对齐和相位旋转预处理时的接收信号星座

图 2　信号预处理过程示意

Fig.2　Diagram of signal pretreatment

由上述分析可得，向量 $\boldsymbol{w}_m$ 为

$$\boldsymbol{w}_m = \sqrt{P_{\mathrm{s}}}\boldsymbol{A}\mathrm{e}^{\mathrm{j}\theta_m},\ \boldsymbol{A} = [\mathrm{e}^{-\mathrm{j}\theta_1}\ \mathrm{e}^{-\mathrm{j}\theta_2}\cdots\mathrm{e}^{-\mathrm{j}\theta_{N_{\mathrm{a}}}}]^{\mathrm{T}}. \quad (3)$$

式中：P_s 为发射信号的功率；$\boldsymbol{A}$ 使各激活天线发射的信号在到达 Bob 时相位对齐；θ_m 是相位旋转因子，$\theta_m = (m-1)\Delta\varphi/N_{\mathrm{c}}$，其中 $\Delta\varphi$ 是 APM 星座中星座点间的最小相位间隔，对于 MPSK，$\Delta\varphi = 2\pi/M$.

人工噪声 n 应尽可能不对 Bob 的接收产生影响，理想情况下应满足 $\boldsymbol{h}_{\mathrm{bm}}\boldsymbol{g}_m = 0$，同时应该对窃听者产生最大的干扰. 人工噪声波束赋形矢量的设计可表示为优化问题：

$$\max_{\boldsymbol{g}_m} |\boldsymbol{h}_{em}\boldsymbol{g}_m|^2,$$
$$\text{s.t. } \boldsymbol{h}_{\mathrm{bm}}\boldsymbol{g}_m = 0,\ \mathrm{tr}(\boldsymbol{g}_m\boldsymbol{g}_m^{\mathrm{H}}) = P_{\mathrm{n}}.$$

式中：上标 H 表示共轭转置，P_{n} 为发送人工噪声的功率，$|\cdot|$ 表示求模，$\mathrm{tr}(\cdot)$ 表示矩阵的迹. 约束条件 $\boldsymbol{h}_{\mathrm{bm}}\boldsymbol{g}_m = 0$ 表示人工噪声对合法接收者不产生影响.

设 $\boldsymbol{U}_\perp$ 为信道 $\boldsymbol{h}_{\mathrm{bm}}$ 零空间的投影矩阵，$\boldsymbol{h}_{\mathrm{bm}}\boldsymbol{U}_\perp = 0$，由文献[14]可知 $U_\perp = \boldsymbol{I}_{N_{\mathrm{a}}} - \boldsymbol{h}_{\mathrm{bm}}^{\mathrm{H}}(\boldsymbol{h}_{\mathrm{bm}}\boldsymbol{h}_{\mathrm{bm}}^{\mathrm{H}})^{-1}\boldsymbol{h}_{\mathrm{bm}}$. 得到 $\boldsymbol{U}_\perp$ 后，可设 $\boldsymbol{g}_m = \boldsymbol{U}_\perp \boldsymbol{g}'_m$，为使 $|\boldsymbol{h}_{em}\boldsymbol{g}_m|^2 = |\boldsymbol{h}_{em}\boldsymbol{U}_\perp\boldsymbol{g}'_m|^2$ 最大化，只需 $\boldsymbol{g}'_m$ 与 $\boldsymbol{h}_{em}\boldsymbol{U}_\perp$ 共线，故 $\boldsymbol{g}'_m = a\boldsymbol{U}_\perp^{\mathrm{H}}\boldsymbol{h}_{em}^{\mathrm{H}}$，其中 a 为实系数. 可设 $a = 1$，则 $\boldsymbol{g}'_m = \boldsymbol{U}_\perp^{\mathrm{H}}\boldsymbol{h}_{em}^{\mathrm{H}}$，那么 $\boldsymbol{g}_m = \boldsymbol{U}_\perp\boldsymbol{U}_\perp^{\mathrm{H}}\boldsymbol{h}_{em}^{\mathrm{H}}$. 由 $\boldsymbol{U}_\perp$ 的表达式有 $\boldsymbol{U}_\perp = \boldsymbol{U}_\perp^{\mathrm{H}}$ 和 $\boldsymbol{U}_\perp\boldsymbol{U}_\perp = \boldsymbol{U}_\perp$，所以 $\boldsymbol{g}_m = \boldsymbol{U}_\perp\boldsymbol{h}_{em}^{\mathrm{H}}$. 在满足人工噪声功率约束条件 $\mathrm{tr}(\boldsymbol{g}_m\boldsymbol{g}_m^{\mathrm{H}}) = \boldsymbol{P}_{\mathrm{n}}$ 时，最优波束赋形矢量为 $\boldsymbol{g}_m = \dfrac{\sqrt{P_{\mathrm{n}}}\boldsymbol{U}_\perp\boldsymbol{h}_{em}^{\mathrm{H}}}{\|\boldsymbol{U}_\perp\boldsymbol{h}_{em}^{\mathrm{H}}\|} \in \mathbb{C}^{N_a\times 1}$. 令 $\boldsymbol{R}_m = \dfrac{\boldsymbol{U}_\perp\boldsymbol{h}_{em}^{\mathrm{H}}}{\|\boldsymbol{U}_\perp\boldsymbol{h}_{em}^{\mathrm{H}}\|}$，那么 $\boldsymbol{g}_m = \sqrt{P_{\mathrm{n}}}\boldsymbol{R}_m$，人工噪声对窃听者产生最大干扰. 最终发送的人工噪声为

$$\boldsymbol{n} = \boldsymbol{g}_m z = \sqrt{P_{\mathrm{n}}}\boldsymbol{R}_m z. \quad (4)$$

将式(3)和式(4)代入式(2)中，Bob 和 Eve 的接收信号可表示为

$$y_{\mathrm{b}} = \boldsymbol{h}_{\mathrm{bm}}\sqrt{P_{\mathrm{s}}}\boldsymbol{A}\mathrm{e}^{\mathrm{j}\theta_m}s_i + \boldsymbol{h}_{\mathrm{bm}}\sqrt{P_{\mathrm{n}}}\boldsymbol{R}_m z + n_{\mathrm{b}} = \sqrt{P_{\mathrm{s}}}c_{\mathrm{m}}s_i + n_{\mathrm{b}},$$
$$y_{\mathrm{e}} = \boldsymbol{h}_{em}\sqrt{P_{\mathrm{s}}}\boldsymbol{A}\mathrm{e}^{\mathrm{j}\theta_m}s_i + \boldsymbol{h}_{em}\sqrt{P_{\mathrm{n}}}\boldsymbol{R}_m z + n_{\mathrm{e}} = \sqrt{P_{\mathrm{s}}}d_m s_i + \sqrt{P_{\mathrm{n}}}\boldsymbol{h}_{em}\boldsymbol{R}_m z + n_{\mathrm{e}}.$$

式中，$c_m = \sum_{k=1}^{N_a}|h_{\mathrm{bm},k}|\mathrm{e}^{\mathrm{j}\theta_m}$，$d_m = \boldsymbol{h}_{em}\boldsymbol{A}\mathrm{e}^{\mathrm{j}\theta_m}$.

需要说明的是，实现人工噪声不对合法接收者的接收产生影响，同时对窃听者的干扰最大化的前提是能获得合法信道和窃听信道准确的 CSI. 如果该条件不满足，则人工噪声会对合法接收者的接收会有一定的影响.

Bob 对接收信号的幅相调制和空间调制采用最

大似然 ML(maximum-likelihood)准则联合检测:

$$[\hat{m},\hat{s}_i]=\arg\min_{\substack{m\in\{1,2,\cdots,N_c\}\\ i\in\{1,2,\cdots,M\}}}\{\|y_b-\sqrt{P_s}c_m s_i\|^2\}.$$

Eve 对接收信号的幅相调制和空间调制也进行 ML 准则联合检测:

$$[\hat{m},\hat{s}_i]=\arg\min_{\substack{m\in\{1,2,\cdots,N_c\}\\ i\in\{1,2,\cdots,M\}}}\{\|y_e-\sqrt{P_s}d_m s_i\|^2\}.$$

3 保密性能分析

3.1 保密容量和最优功率分配因子分析

保密容量是系统可以达到的最大保密传输速率,是反映系统性能一个极限值. 发射端的发射功率分为两部分,一部分用于发射承载信息的信号,另一部分发射人工噪声. 假设总发射功率为 P,功率分配因子为ρ,发射信号的功率为 $P_s=E[\|\boldsymbol{w}_m s_i\|^2]=\rho P$,而发射人工噪声的功率为 $P_n=E[\boldsymbol{n}^H\boldsymbol{n}]=(1-\rho)P$. 由于 GSM 信号包含发射天线索引信息和 APM 调制信息两部分,所以接收信号与发送信号间的互信息也由两部分组成. 采用与文献[7]求 GSM 信道容量方法,可得 Bob 和 Eve 的瞬时信道容量分别为

$$C_b=\log_2\left(1+\frac{P_s}{N_a N_c\sigma_b^2}\boldsymbol{H}_b\boldsymbol{G}\boldsymbol{H}_b^H\right),$$

$$C_e=\log_2\left(1+\frac{P_s}{N_a N_c(P_n\boldsymbol{h}_{em}\boldsymbol{R}_m\boldsymbol{R}_m^H\boldsymbol{h}_{em}^H+\sigma_e^2)}\boldsymbol{H}_e\boldsymbol{G}\boldsymbol{H}_e^H\right).$$

式中,$\boldsymbol{G}$ 表示在所有激活天线组合中,各天线被使用的次数所组成的对角矩阵. 如当 $N_t=4$,$N_a=2$ 时,$N_c=4$,选择 6 个组合中的 4 组激活天线组合,分别为(1, 2)、(1, 3)、(1, 4)、(2, 3),天线 1 使用 3 次,天线 2 使用 2 次,天线 3 使用 2 次,天线 4 使用 1 次,故 $\boldsymbol{G}=\mathrm{diag}(3,2,2,1)$. 瞬时保密容量为

$$C_s=[C_b-C_e]^+=\left[\log_2\left(1+\frac{\rho P}{N_a N_c\sigma_b^2}\boldsymbol{H}_b\boldsymbol{G}\boldsymbol{H}_b^H\right)-\log_2\left(1+\frac{\rho P}{N_a N_c((1-\rho)P\boldsymbol{h}_{em}\boldsymbol{R}_m\boldsymbol{R}_m^H\boldsymbol{h}_{em}^H+\sigma_e^2)}\boldsymbol{H}_e\boldsymbol{G}\boldsymbol{H}_e^H\right)\right]^+. \tag{5}$$

式中 $[\alpha]^+=\max\{0,\alpha\}$,即保密容量 C_s 取值大于 0 或等于 0. 保密容量是ρ 的函数,但不是ρ 的单调函数,存在一个最优的ρ 值使系统的保密容量最大.

记 $a_1=\boldsymbol{H}_b\boldsymbol{G}\boldsymbol{H}_b^H$,$a_2=\boldsymbol{H}_e\boldsymbol{G}\boldsymbol{H}_e^H$,$a_3=\sigma_b^2$,$a_4=\sigma_e^2$,$a_5=N_a N_c$,$a_6=\boldsymbol{h}_{em}\boldsymbol{R}_m\boldsymbol{R}_m^H\boldsymbol{h}_{em}^H$,式(5)可简记为

$$C_s=\left[\log_2\left(1+\frac{a_1P\rho}{a_3a_5}\right)-\log_2\left(1+\frac{a_2P\rho}{a_5(a_6P(1-\rho)+a_4)}\right)\right]^+.$$

对每传输时隙而言,信道系数 $\boldsymbol{H}_b$、$\boldsymbol{H}_e$、$\boldsymbol{h}_b$、$\boldsymbol{h}_e$ 为定值,那么 $a_1\sim a_6$ 的值都是确定的. 令

$$f(\rho)=\log_2\left(1+\frac{a_1P\rho}{a_3a_5}\right)-\log_2\left(1+\frac{a_2P\rho}{a_5(a_6P(1-\rho)+a_4)}\right), \tag{6}$$

式(6)是ρ 的连续函数,最优的功率分配因子ρ 值就是在[0, 1]间使 $f(\rho)$ 最大的值,最大值点可能是 $f(\rho)$ 函数一阶导数为零时在[0, 1]之间的解,也可能是 0、1 边界点. $f(\rho)$ 的一阶导数为

$$\frac{\mathrm{d}f(\rho)}{\mathrm{d}\rho}=\frac{1}{\ln 2}\left(\frac{a_1P(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)}{(a_1P\rho+a_3a_5)(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)}-\frac{(a_1P\rho+a_3a_5)(a_2a_4a_5P+a_2a_5a_6P^2)}{(a_1P\rho+a_3a_5)(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)}\right). \tag{7}$$

式(7)为零的解,就是其分子为零的解:

$$a_1P(a_4a_5+a_5a_6P+a_2P\rho-a_5a_6P\rho)(a_4a_5+a_5a_6P-a_5a_6P\rho)-(a_1P\rho+a_3a_5)(a_2a_4a_5P+a_2a_5a_6P^2)=0, \tag{8}$$

式(8)为一元二次方程,其解为

$$\rho=\frac{a_1a_4a_5a_6+a_1a_5a_6^2P\pm\sqrt{a_1a_2a_5a_6(a_4+a_6P)(a_1a_4-a_2a_3+a_3a_5a_6+a_1a_6P)}}{a_1a_5a_6^2P-a_1a_2a_6P}. \tag{9}$$

式(9)在[0, 1]内的那个解为极值点,其所对应的保密容量与边界点 0 和 1 对应的保密容量中的最大值即为该信道条件下最大保密容量. 每次传输时最优的功率分配因子与最大保密容量对应.

3.2 误码性能分析

保密容量是衡量系统保密传输能力的理论极限值,系统要获得达到保密容量的保密传输速率,要求发送的信号必须为高斯分布的信号,这在实际应用中是不可能的. 实际系统中采用的是有限阶数的数字调制信号,此时可通过比较合法接收者和窃听者间的误码性能差距来衡量系统的保密传输能力. 窃听者的误码率越高于合法接收者,系统的保密传输能力越高. 由于精确的误码率难以获得,这里通过求 Bob 和 Eve 的成对差错概率 $\Pr(\boldsymbol{x}_{mi}\to\boldsymbol{x}_{lj})$ 来获得平均误比特率 $P_{(s,m)}$ 的联合上界.

$P_{(s,m)}$ 的表达式为

$$P_{(s,m)}\leqslant\frac{1}{N_c M\log_2(N_c M)}\sum_{m=1}^{N_c}\sum_{i=1}^{M}\sum_{\substack{l=1\\(l,j)\neq(m,i)}}^{N_c}\sum_{j=1}^{M}d(\boldsymbol{x}_{mi},\boldsymbol{x}_{lj})\cdot E[\Pr(\boldsymbol{x}_{mi}\to\boldsymbol{x}_{lj})]. \tag{10}$$

式中:$\Pr(\boldsymbol{x}_{mi}\to\boldsymbol{x}_{lj})$ 表示将幅相调制符号 s_i、激活天

线组合为 m 错判成幅相调制符号 s_j、激活天线组合为 l 的成对差错概率；$\frac{1}{N_c M}\sum_{m=1}^{N_c}\sum_{i=1}^{M}\sum_{\substack{l=1\\(l,j)\neq(m,i)}}^{N_c}\sum_{j=1}^{M}[\cdot]$ 表示对所有幅相调制和激活天线组合求取平均；$d(\boldsymbol{x}_{mi},\boldsymbol{x}_{lj})$ 表示激发天线组合为 m、幅相调制符号为 s_i 对应的比特序列与激活天线组合为 n、幅相调制符号为 s_j 对应的比特序列的汉明距离. $\frac{d(\boldsymbol{x}_{mi},\boldsymbol{x}_{lj})}{\log_2(N_c M)}$ 将误符号率转换为误比特率.

对于 Bob，其 $\Pr(\boldsymbol{x}_{mi}\to\boldsymbol{x}_{lj})$ 为

$$\begin{aligned}\Pr(\boldsymbol{x}_{mi}\to\boldsymbol{x}_{lj}) &= \Pr(\|y_b-\sqrt{P_s}c_m s_i\|^2 > \|y_b-\sqrt{P_s}c_l s_j\|^2) = \Pr(P_s|c_m|^2|s_i|^2 - \\ &2\mathrm{Re}(y_b^*\sqrt{P_s}c_m s_i) > P_s|c_l|^2|s_j|^2 - 2\mathrm{Re}(y_b^*\sqrt{P_s}c_l s_j)) = \Pr(\mathrm{Re}(n_b\sqrt{P_s}c_l^* s_j^*) - \\ &\mathrm{Re}(n_b\sqrt{P_s}c_m^* s_i^*) > P_s|c_m s_i - c_l s_j|^2/2).\end{aligned}$$

其中上标 $*$ 表示取共轭. 上式最后一行中，大于号的左边为服从均值为 0，方差为 $P_s|c_m s_i - c_l s_j|^2\sigma_b^2/2$ 的高斯随机变量. 成对差错概率为

$$\Pr(\boldsymbol{x}_{mi}\to\boldsymbol{x}_{lj}) = Q\left(\sqrt{\frac{P_s|c_m s_i - c_l s_j|^2}{2\sigma_b^2}}\right),$$

代入式(10)得 Bob 的误比特率为

$$P_{(s,m),b} \leqslant \frac{1}{N_c M\log_2(N_c M)}\sum_{m=1}^{N_c}\sum_{i=1}^{M}\sum_{\substack{l=1\\(l,j)\neq(m,i)}}^{N_c}\sum_{j=1}^{M} d(\boldsymbol{x}_{mi},\boldsymbol{x}_{lj})E\left[Q\left(\sqrt{\frac{P_s|c_m s_i - c_l s_j|^2}{2\sigma_b^2}}\right)\right].$$

在瑞利衰落信道下，采用文献[15]的方法对期望运算进行推导，最后可得

$$P_{(s,m),b} \leqslant \frac{1}{2M\log_2(N_c M)}\sum_{i=1}^{M}\sum_{\substack{i=1\\j\neq i}}^{M}\left\{\left[\frac{N_c^2\log_2(N_c)}{2} + N_c(N_c-1)d(x_i,x_j)\right]\left(1-\sqrt{\frac{\sigma_{1b}^2}{1+\sigma_{1b}^2}}\right)\right\}.$$

式中 $\sigma_{1b}^2 = \sigma_{bh}^2\gamma_b(|s_i|^2+|s_j|^2)$，$\gamma_b = P_s/4\sigma_b^2$，$\sigma_{bh}^2$ 表示 Alice 与 Bob 间信道系数方差.

对 Eve 而言，将其接收信号 y_e 中的人工噪声和信道噪声一起记为 $n_{ea} = \sqrt{P_n}\boldsymbol{h}_{em}\boldsymbol{R}_m z + n_e$，是均值为 0，方差为 $\sigma_{n_{ea}}^2 = P_n\boldsymbol{h}_{em}\boldsymbol{R}_m\boldsymbol{R}_m^H\boldsymbol{h}_{em}^H + \sigma_e^2$ 的复高斯随机变量. 则

$$y_e = \sqrt{P_s}d_m s_i + n_{ea}.$$

与 Bob 误比特率的推导过程类似，可以推导得到 Eve 的误比特率为

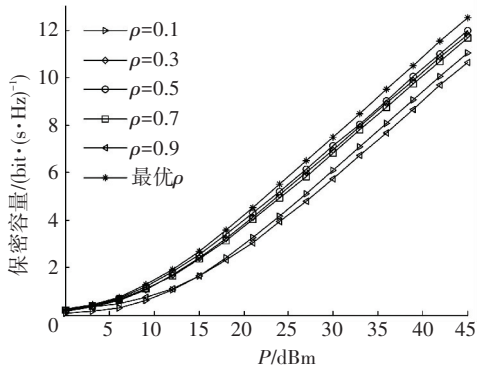
$$P_{(s,m),e} \leqslant \frac{1}{2M\log_2(N_c M)}\sum_{i=1}^{M}\sum_{\substack{i=1\\j\neq i}}^{M}\left\{\left[\frac{N_t^2\log_2(N_t)}{2} + N_t(N_t-1)d(\boldsymbol{x}_i,\boldsymbol{x}_j)\right]\left(1-\sqrt{\frac{\sigma_{1e}^2}{1+\sigma_{1e}^2}}\right)\right\}.$$

式中 $\sigma_{1e}^2 = \sigma_{eh}^2\gamma_e(|s_i|^2+|s_j|^2)$，$\gamma_e = P_s/4\sigma_{n_{ea}}^2$，$\sigma_{eh}^2$ 表示 Alice 与 Eve 间信道系数方差.

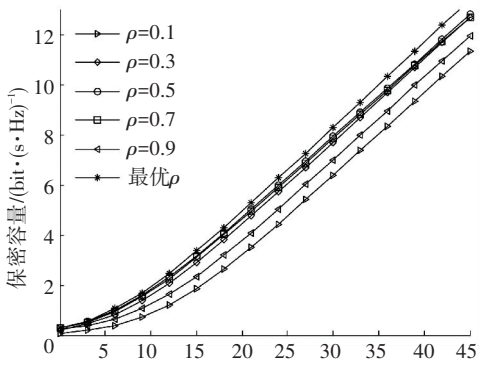
4　仿真分析

仿真中信道为相互独立的瑞利平坦衰落信道，信道衰落由大尺度衰落和小尺度衰落组成. 假设所有信道的大尺度衰落因子均为 −120 dB = 10^{-12}，小尺度衰落因子为均值为 0、方差为 1 的复高斯随机变量，这样所有信道的信道系数的方差均为 10^{-12}. 假设所有信道噪声方差均为 −120 dBm. 本节所给出的仿真结果是信道变化 5×10^5 次所得结果的平均值.

图 3 给出系统发送天线数 $N_t = 4$，在不同功率分配因子 ρ 值下的保密容量，其中图 3(a)为激活天线数 $N_a = 2$ 时的值，图 3(b)为 $N_a = 3$ 时的值. 可看到采用最优功率分配因子比采用其他功率分配因子时，系统的保密容量更大，具有更好的保密传输能力.



(a) $N_a = 2$



(b) $N_a = 3$

图 3　不同 ρ 时系统保密容量随 P 变化的情况，$N_t=4$

Fig.3　Security capacities with different ρ and P, $N_t=4$

图 4 为本文方案在 $N_t = 4$、$N_a = 2$ 时，幅相调制采用 QPSK 调制，不同 ρ 值下 Bob 和 Eve 的误比特率随发送总功率 P 的变化曲线. 图 4 中实线为仿真值，虚线为理论上界值. 可以看到，对同一 P 值，功率分配因子 ρ 越大，发射有用信号的功率越大，而发射人工噪声的功率越小，对于 Bob 和 Eve 而言都是误码率越低. 但不管 ρ 如何取值，Bob 的误码率都要

优于 Eve 的误码率. 而二者的误码率差距越大,系统的保密通信能力越强.

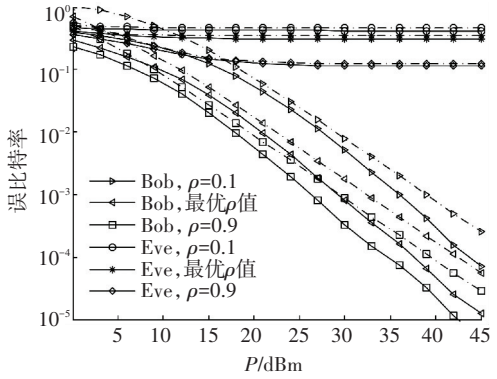
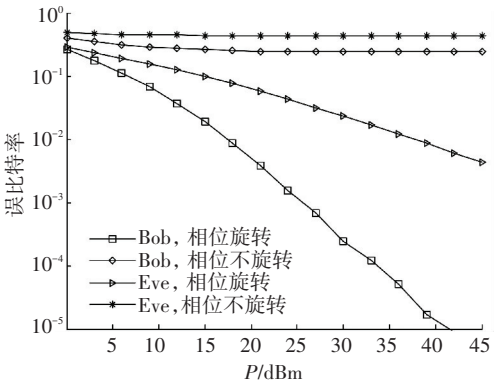


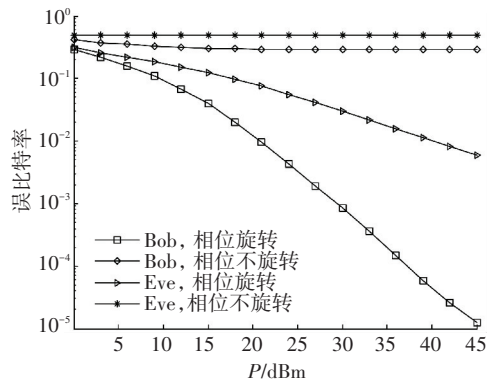
图 4 不同 ρ 时 Bob 和 Eve 的误比特率随 P 变化的情况, $N_t=4, N_a=2$

Fig.4 Bit error rates of Bob and Eve with different ρ and P, $N_t = 4$, $N_a = 2$

图 5 给出了 $N_t=4$、$N_a=2$, 幅相调制采用 BPSK 和 QPSK 调制,对激活天线发送信号是否进行相位旋转时,系统的误码性能随发送总功率 P 变化的仿真结果. 从图 5 可以看到,不论是采用 BPSK 还是 QPSK 调制,进行了相位旋转处理后,Bob 的误码性能有明显的改善,而 Eve 的误码率则无明显的变化.



(a) BPSK 调制

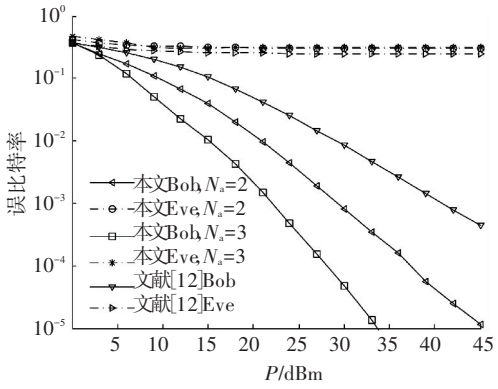


(b) QPSK 调制

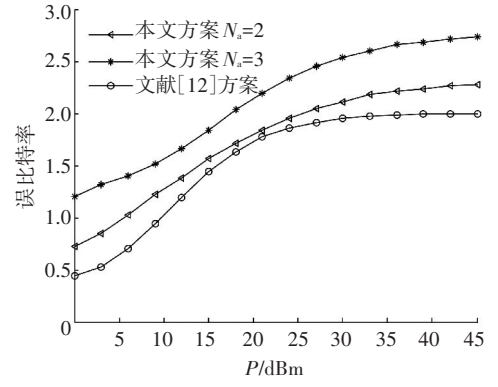
图 5 是否进行相位旋转的误比特率比较, $N_t=4, N_a=2$

Fig.5 Bit error rates with and without phase shift, $N_t = 4$, $N_a = 2$

图 6 为本文方案与文献[12]方案中 Bob 和 Eve 误码性能和保密互信息的仿真对比,保密互信息(即合法接收端从每个接收符号中获得的保密信息量)采用文献[12]方法计算. 文献[12]的 SM 系统中,在发送端已知所有信道 CSI 的条件下,发射端根据窃听信道的 CSI,对发送信号进行预处理,使各发送天线与窃听者接收天线间的等效信道特性相同,使窃听者不能分辨发送的天线,无法解调映射到天线索引上的信息. 这样的预处理对合法接收者则无影响. 仿真中,本文方案和文献[12]方案的发送天线数都是 $N_t = 4$,幅相调制都采用 QPSK. 本文方案中每次激活的发送天线数为 $N_a = 3$ 或 $N_a = 2$,文献[12]方案中 $N_a = 1$. 两方案通过天线索引和幅相调制部分携带的信息量都相同,系统的频谱效率都是 4 bit/symbol. 从图 6(a)可看出本文方案和文献[12]方案中 Eve 的误比特率基本一致. 但对 Bob 而言,本文方案的误比特率要远低于文献[12]的方案. 从图 6(b)可看到本文方案保密互信息高于文献[12],也就意味着系统具有更好的保密传输能力,且激活天线数越多保密互信息越大. 本文方案中,每次传输时激活的天线数越多,Bob 的误码性能越好,因为激活天线数越多也就意味着发射分集更大,接收端性能更好. 但相应的射频部分的复杂度也会增加,所以在实际选择时,需要考虑到性能和复杂度的均衡.



(a) 误比特率



(b) 保密互信息

图 6 本文方案与文献[12]方案误码性能和保密互信息对比

Fig.6 Comparison of bit error rates and security mutual information between the schemes of this paper and Ref.[12]

5 结　论

本文给出了在多发射天线系统中利用 GSM 调制技术的物理层安全传输方案，系统通过发射天线索引和传统幅相调制符号传递信息. 发送端利用其与合法接收者间的信道特性对发送信号进行预处理，使合法接收者接收到的来自各激活天线信号的相位对齐，获得发送分集的效果，增加信噪比. 同时预处理过程还使各激活天线组合的合成信号相位等间隔分布，进一步提高合法接收者的接收性能，降低误码率. 而窃听者接收到的来自各激活天线的信号相位仍为随机分布，无分集和相位等间隔分布的效果. 为了防止窃听者获得幅相调制符号携带的信息，方案中还引入了指向窃听者的人工噪声. 理论分析和仿真结果表明，合法接收者的误码性能远优于窃听者，能获得可观的系统保密容量. 本文中假设发射端能获得信道准确的 CSI，在 CSI 存在误差的情况下，发送信号预处理向量和人工噪声的指向准确性都会有所下降，使系统的保密传输性能有所下降. 研究在 CSI 有误差情况下具有良好鲁棒性的信号预处理和人工噪声方案将是下一步的研究问题.

参考文献

[1] ZHANG Junwei, GURSOY M C. Relay beamforming strategies for physical-layer security[C]// Proceeding of 44th Annual Conference on Information Sciences and Systems. Piscataway: IEEE Press, 2010: 1-6. DOI: 10.1109/CISS.2010.5464970.

[2] LIU Yupeng, LI Jiangyuan, PETROPULU A P. Destination assisted cooperative jamming for wireless physical-layer security[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(4): 682-694. DOI: 10.1109/TIFS.2013.2248730.

[3] ZOU Yulong, WANG Xianbin, SHEN Weiming. Optimal relay selection for physical layer security in cooperative wireless networks [J]. IEEE Journal on Selected Areas in Communications, 2013, 31(10)10: 2099-2111. DOI: 10.1109/JSAC.2013.131011.

[4] HUI Hui, SWINDLEHURST L A, LI Guobing, et al. Secure relay and jammer selection for physical layer security[J]. IEEE Signal Processing Letters, 2015, 22(8): 1147-1151. DOI: 10.1109/LSP.2014.2387860.

[5] MESLEH R Y, HAAS H, SINANOVIC S, et al. Spatial modulation [J]. IEEE Transactions on Vehicular Technology, 2008, 57(4): 2228-2241. DOI: 10.1109/TVT.2007.912136.

[6] FU Jinlin, HOU Chunping, XIANG Wei, et al. Generalised spatial modulation with multiple active transmit antennas[C]// Proceeding of IEEE GLOBECOM Workshops. Piscataway: IEEE Press, 2010: 839-844. DOI: 10.1109/GLOCOMW.2010.5700442.

[7] TAKEUCHI K. Spatial modulation achieves information-theoretically optimal energy efficiency[J]. IEEE Wireless Communications Letters, 2015, 19(7): 1133-1136. DOI: 10.1109/LCOMM.2015.2433271.

[8] XIAO Yue, YANG Zongei, DAN Lilin, et al. Low-complexity signal detection for generalized spatial modulation[J]. IEEE Communications Letters, 2014, 18(3): 403-406. DOI: 10.1109/LCOMM.2013.123113.132586.

[9] CAL-BRAZ J A, SAMPAIO-NETO R. Low-complexity sphere decoding detector for generalized spatial modulation systems [J]. IEEE Communications Letters, 2014, 18(6): 949-952. DOI: 10.1109/LCOMM.2014.2320936.

[10] LIU Wenlong, WANG Nan, JIN Minglu, et al. Denoising detection for the generalized spatial modulation system using sparse property [J]. IEEE Communications Letters, 2014, 18(1): 22-25. DOI: 10.1109/LCOMM.2013.111413.131722.

[11] BASNAYAKAD A, HAAS H. Spatial modulation for massive MIMO [C]// Proceeding of IEEE International Conference on Communications Piscataway: IEEE Press, 2015: 1945-1950. DOI: 10.1109/ICC.2015.7248610.

[12] GUAN Xinrong, CAI Yueming, YANG Weiwei. On the secrecy mutual information of spatial modulation with finite alphabet[C]// Proceeding of International Conference on Wireless Communications and Signal Processing. Piscataway: IEEE Press, 2012: 1-4. DOI: 10.1109/WCSP.2012.6542961.

[13] WU Feilong, YANG Lieliang, WANG Wenjie, et al. Secret precoding-aided spatial modulation[J]. IEEE Wireless Communications Letters, 2015, 19(9): 1544-1547. DOI: 10.1109/LCOMM.2015.2453313.

[14] DONG Lun, HAN Zhu, PETROPULU A P, et al. Improving wireless physical layer security via cooperating relays [J]. IEEE Transactions on Signal Processing, 2010, 58(3): 1875-1888. DOI: 10.1109/TSP.2009.2038412.

[15] JEGANATHAN J, GHRAYEB A, SZCZECINSKI L. Spatial modulation: optimal detection and performance analysis[J]. IEEE Communications Letters, 2008, 12(8): 545-547. DOI: 10.1109/LCOMM.2008.080739.

（编辑　王小唯，苗秀芝）