部分信道特征下的物理层安全编码方法*

王亚东, 黄开枝, 吉 江, 钟 州
(国家数字交换系统工程技术研究中心, 郑州 450002)

摘 要: 针对部分信道特征(授权信道特征存在估计误差且窃听信道特征未知)下的物理层安全传输问题,结合人工噪声和安全编码,提出了一种实用的物理层安全编码方法。多天线发射机采用波束成型传输信号时添加与授权信道特征正交的人工噪声,利用交织 LDPC 码缩小安全距离,在授权信道 SNR 约束下求最小私密中断概率,实现功率优化分配,尽可能使窃听信道保持低 SNR 高 BER,授权信道保持高 SNR 低 BER,从而实现物理层安全传输。仿真结果表明,在授权信道 SNR 约束下,本方法可以实现较低的私密中断概率。

关键词: 人工噪声; 波束成型; 交织 LDPC; 私密中断概率
中图分类号: TN918.3 **文献标志码**: A **文章编号**: 1001-3695(2012)09-3452-04
doi:10.3969/j.issn.1001-3695.2012.09.067

Scheme of physical layer secrecy coding under partial channel characteristics

WANG Ya-dong, HUANG Kai-zhi, JI Jiang, ZHONG Zhou
(*National Digital Switching System Engineering & Technological Research Center, Zhengzhou* 450002, *China*)

Abstract: This paper proposed a scheme of physical layer secrecy coding under partial channel characteristics aiming at physical layer secure transmission problem. The multi-antenna transmitter exploited beam-former to send signal with artificial noise which was orthogonal with authorized channel characteristics. It used interleaving LDPC to reduce the security gap between authorized channel and eavesdropping channel. Then found the minimum secrecy outage probability with authorized channel SNR constraint, and archived the optimal power allocation for physical layer secure transmission. So the authorized channel could keep low BER with high SNR, while the eavesdropping channel could only have high BER with low SNR. Simulation results show that, the proposed method can realize lower secrecy outage probability with authorized channel SNR constraint.

Key words: artificial noise; beam-former; interleaving LDPC; secrecy outage probability

0 引言

电磁波的空间传播特性使得无线信道具有易窃听、易受干扰的特性,因此无线通信的安全传输问题成为人们关注的焦点。现有解决方案是通过高层加密协议来实现,但其实现复杂、代价高,同时还要解决密钥的分发和管理问题;而物理层安全传输因其传输技术共知、实现简单,不存在私密共享等优点,近年来成为研究的热点。

Shannon 在文献[1]中证明只有通信双方共享的密钥熵不小于信源熵,才能实现无条件安全通信,但这种一次一密的加密机制只是将信息安全共享问题转换为密钥安全共享问题;同时,Shannon 假设接收方接收的密文信息相同,但因为信道的随机性,这在实际中很难保证。文献[2,3]中的工作证明,只要窃听者的信道比授权信道差,就存在正的私密信道容量,可以通过信道编码实现私密信道容量(称可以实现私密信道容量的信道编码为安全编码),而实际中 Eve 的信道很可能比 Bob 好,这时私密信道容量为零,安全编码也就不存在了。文献[4,5]进一步推导了多天线窃听信道的私密信道容量,但没有设计相应的安全编码。以上研究[2-5]将私密信道容量作为安全测度,其计算需要知道窃听者的信道特征或其分布信息,对只听不发的被动窃听者来说,这是不可能知道的。文献[6]使用误比特率(bit-error-rate,BER)作为安全测度,提出了一种最小化安全距离的打孔 LDPC 码,私密信息隐藏于打孔位中,Eve 因为信道条件差无法估计打孔位而保持高 BER;文献[7]则使用交织编码进一步缩小了安全距离。安全距离是指满足安全编码可靠性和安全性要求对应的信噪比(signal-to-noise-ratio,SNR)门限之差,打孔 LDPC 码和交织编码减小了安全距离,降低了对窃听信道的要求,为实用的安全编码设计提供了一条可行的思路;文献[8]提出了一种添加人工噪声使窃听信道 SNR 降低的方法,给出了满足信道条件假设[2]的一种可行思路。文献[9]以私密信道容量为优化目标,分析了人工噪声和信号的功率分配问题,得到了私密信道容量为正时的 SNR 门限,证明了私密信道容量随授权信道 SNR 降低而降低,随窃听信道 SNR 升高而降低。以上研究[8,9]多是在发射天线数很大的情况下给出的结论,不具有实用性。文献[10]结合人工噪声提出了一种服务质量(quality of service,QoS)约束下的波束成形安全传输方法,通过联合优化发射权重和人工噪声的空间分布,给出了窃听信道保持低 SNR 和授权信道保持高 SNR 的具体实现方案。文献[11]在保证授权信道一定发送速率的前提下最大化人工噪声的功率分配;文献[12]则在保证授权

收稿日期: 2012-02-16; **修回日期**: 2012-04-13 **基金项目**: 国家自然科学基金资助项目(61171108)

作者简介: 王亚东(1984-),男,陕西米脂人,硕士研究生,主要研究方向为无线与移动通信安全(yadowang@gmail.com);黄开枝(1973-),女,副教授,博士,主要研究方向为无线与移动通信;吉江(1983-),男,山西忻州人,博士研究生,主要研究方向为物理层安全.

信道一定信干噪比的前提下最小化窃听信道的信干噪比。上述研究[10~12]只是给出了满足授权信道一定 QoS 的人工噪声波束成型传输方法,并没有讨论具体的安全编码构造。文献[13]将私密中断概率作为安全测度,并给出了两种安全传输策略;文献[14]则在保证一定私密中断概率的前提下最大化人工噪声的功率分配,但其讨论限于已知完全授权信道特征和部分窃听信道特征。

针对以上问题,本文提出了一种基于人工噪声的物理层安全编码方法。

1　系统模型

假设系统模型的分析场景为 MISO(multiple-input-single-output)系统,包含授权用户 Alice、Bob 和只听不发的窃听者 Eve。Alice 与 Bob 间的信道称授权信道,Eve 与 Alice 间的信道称窃听信道;Alice 有 N_A 根天线,Bob 和 Eve 均为单天线,有 M 个 Eve,其中 $N_A, M \geqslant 2$。窃听者分为联合和不联合两种情况,联合相当于 Eve 有 M 根天线,不联合则为单天线 Eve。

实用的物理层安全编码没有出现,很大程度上是因为信道条件假设难以满足。因此本文提出了一种部分信道特征下的物理层安全编码模型,用于实现满足信道条件假设的物理层安全编码,具体如图 1 所示。

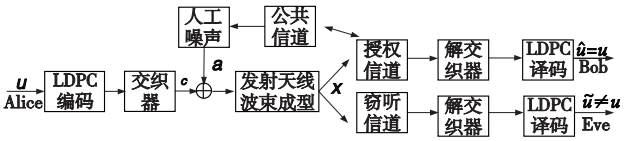

图1　部分信道特征下的物理层安全编码模型

在采用波束成型传输的 MISO 系统中,通过预先设计的交织 LDPC 码降低对窃听信道的 SNR 要求,结合人工噪声和波束成型进行发射功率的优化分配,保证窃听信道低 SNR,授权信道高 SNR,满足安全编码的信道条件假设,从而实现物理层安全传输。如图 1 所示,Alice 通过公共信道向 Bob 发送训练序列用于信道估计,Bob 估计授权信道特征并通过公共信道反馈给 Alice;Alice 选择交织 LDPC 码将私密信息矢量 $\boldsymbol{u}$ 信道编码映射成为码矢量 $\boldsymbol{c}$,结合由授权信道特征零空间产生的人工噪声 $\boldsymbol{a}$,通过发射波束成型映射为信号矢量 $\boldsymbol{x}$ 进行传输;Bob 通过符号检测将译码信息送给解交织译码还原私密信息 $\hat{u}$,Eve 因为 SNR 低而无法译码还原私密信息 $\tilde{u}$。

MISO 系统中授权信道和窃听信道的接收信号分别为

$$y_B(t) = \boldsymbol{h}^{\mathrm{H}}\boldsymbol{x}(t) + n(t) \tag{1}$$

$$y_{E,i}(t) = \boldsymbol{g}_i^{\mathrm{H}}\boldsymbol{x}(t) + v_i(t) \quad i = 1, \cdots, M \tag{2}$$

其中:$\boldsymbol{h}$ 为授权信道特征矢量;$\boldsymbol{g}_i$ 为第 i 个窃听信道特征矢量,$\boldsymbol{h}$ 和 $\boldsymbol{g}_i$ 中元素均为独立同分布的复高斯随机变量;$\boldsymbol{x}(t)$ 为发射信号矢量;$n(t)$、$v_i(t)$ 为独立同分布的均值为 0、方差分别为 σ_n^2 和 $\sigma_{v,i}^2$ 的复高斯噪声。

采用结合人工噪声的发射波束成型,则有

$$\boldsymbol{x}(t) = \boldsymbol{w}s(t) + \boldsymbol{z}(t) \tag{3}$$

其中:$s(t)$ 为发射信号,不失一般性,假设 $E[\,|s(t)|^2\,] = 1$,$E[\,\cdot\,]$ 表示求数学期望;$\boldsymbol{w}$ 是波束成型矢量;$\boldsymbol{z}(t)$ 为人工噪声矢量。假设 $\boldsymbol{z}(t) \sim CN(0, \boldsymbol{\Sigma})$,其中 $\boldsymbol{\Sigma} \geqslant 0$,即 $\boldsymbol{z}(t)$ 为复高斯人工噪声矢量,其协方差为半正定矩阵。已有的人工噪声都是全向辐射的,即 $\boldsymbol{\Sigma} = \beta \boldsymbol{P}_{\hat{h}}^{\perp}$,其中 $\boldsymbol{P}_{\hat{h}}^{\perp} = \boldsymbol{I}_{N_A} - \hat{\boldsymbol{h}}\hat{\boldsymbol{h}}^{\mathrm{H}} / \|\hat{\boldsymbol{h}}\|^2$,即 $\boldsymbol{P}_{\hat{h}}^{\perp}$ 是 $\hat{\boldsymbol{h}}$ 的正交投影矩阵,$\hat{\boldsymbol{h}}$ 是 $\boldsymbol{h}$ 的估计值,β 表示人工噪声的功率分配因子,$\beta \geqslant 0$。授权信道特征是否存在估计误差,窃听信道特征是否未知,直接决定着人工噪声和发射权重的功率分配,影响最终传输方案的安全性。本文主要分析授权信道特征存在估计误差和窃听信道特征未知的情况,即部分信道特征。

1.1　安全测度

私密信道容量是安全编码理论上的安全测度,但其计算需要知道窃听信道特征,对被动窃听者来说,这几乎是不可能的,因此私密信道容量很难作为一种实用的安全测度。安全编码从物理意义上必须满足两个指标:a)可靠性指标:$P_e^B \leqslant P_{e,\max}^B$,其中 P_e^B 表示授权信道的 BER,$P_{e,\max}^B$ 表示授权信道可容忍的最大 BER,即授权信道必须保持低 BER;b)安全性指标:$P_e^E \geqslant P_{e,\min}^E$,其中 P_e^E 表示窃听信道的 BER,$P_{e,\min}^E$ 表示窃听信道必须满足的最小 BER,即窃听信道必须保持高 BER,因此 BER 是一种直观的衡量安全编码安全性的安全测度。BER 直接对应着 SNR,定义安全距离为 $SG = \mathrm{SNR}_{B,\min} - \mathrm{SNR}_{E,\max}$,其中 $\mathrm{SNR}_{B,\min}$ 是授权信道对应 $P_{e,\max}^B$ 的可靠性 SNR 门限,$\mathrm{SNR}_{E,\max}$ 是窃听信道对应 $P_{e,\min}^E$ 的安全性 SNR 门限,SNR 取 dB 作单位。从定义可以看出,安全距离是衡量一定物理层安全水平(BER)下信道差异的安全测度。

实际中,授权信道很可能会工作在 $\mathrm{SNR}_{B,\min}$ 以下,此时 Alice 会选择停止传输,私密信息传输中断。因此,定义私密中断概率为

$$P_{SO} = P(\mathrm{SNR}_E > \mathrm{SNR}_{E,\max} \,|\, \mathrm{SNR}_B \geqslant \mathrm{SNR}_{B,\min}) \tag{4}$$

其中:SNR_B 和 SNR_E 分别表示授权信道和窃听信道的 SNR,这与文献[13]从私密速率出发定义的私密中断概率是不同的。从定义可知,私密中断概率是衡量安全传输方法对授权信道特征影响程度的安全测度,私密中断概率越大,对授权信道的影响越大,安全传输方法的实用性越差。

1.2　安全编码构造

假设 Alice 将 $k \times 1$ 维的二进制信息矢量 $\boldsymbol{u}$ 信道编码映射为 $n \times 1$ 维的二进制码矢量 $\boldsymbol{c}$ 进行传输,即码率 $R = k/n$。定义私密率 $R_s = s/n$,其中 s 表示码矢量 $\boldsymbol{c}$ 中私密信息所占位数。具体在安全编码的构造中,安全编码应该包含两部分信息,即要传输的私密信息和置乱窃听信道的随机信息[2,3]。因此,一般有 $s \leqslant k$,$R_s \leqslant R$。已有的两种用于最小化安全距离的安全编码策略,即打孔[6]和交织[7],其实质是使 BER 曲线在门限处变陡,实现低于门限 SNR 下高 BER。本文主要考虑波束成型 MISO 系统中有限码长下如何利用交织减小安全距离。模型采用 LDPC 码的主要原因有:a)在低 SNR(门限之上)下具有低 BER;b)在对称信道下其性能分析可以采用 GA(Gaussian approximation,高斯近似)或 DE(density evolution,密度进化)实现。下面是安全编码的一些预备知识。

LDPC 码按校验矩阵的行重和列重是否相同可分为规则 LDPC 码和非规则 LDPC 码两类。相同称规则 LDPC 码,不同则称非规则 LDPC 码。一般来说,非规则 LDPC 要好于规则 LDPC 码[15]。LDPC 可用 Tanner 图表示,对应 Tanner 图的度分布对为 $(\lambda(x), \rho(x))$。其中 $\lambda(x) = \sum_{i=2}^{d_v} \lambda_i x^{i-1}$ 表示变量节点的度分布,$\rho(x) = \sum_{j=2}^{d_c} \rho_j x^{j-1}$ 表示校验节点的度分布,λ_i 和 ρ_j 分别表示 Tanner 图中变量节点或校验节点出边在总边数中的占比,d_v 和 d_c 分别表示最大变量节点度数和最大校验节点度数。相应的码率可表示为

$$R = 1 - \int_0^1 \rho(x)\,\mathrm{d}x / \int_0^1 \lambda(x)\,\mathrm{d}x = 1 - m/n \tag{5}$$

其中：m 表示校验节点数(校验矩阵行数)，n 表示变量节点数(校验矩阵列数)。

交织是指用交织矩阵 S 对信息矢量 u 进行重排，信道编码中一般用于将突发错误离散成随机错误，具体到编码映射中为 $c = uSG$。其中，$G_{k\times n}$ 是系统编码生成矩阵，即 $G_{k\times n} = [I_k \mid C_{k\times(n-k)}]$，$S_{k\times k}$ 是非奇异的交织矩阵。码字可以表示为 $c = [uS \mid uSC] = [c_l \mid c_r]$，其中 c_l 包含 c 的前 k 位，c_r 包含 c 的后 $n-k$ 位。授权信道和窃听信道均存在误码，但授权信道 SNR 足够大，可以实现解交织后的信息还原，即 $u_B = u = c_l S^{-1}$；窃听信道 SNR 太小，存在译码错误矢量 e，则解交织后的还原信息为 $u_E = u + e_l S^{-1}$，其中 e_l 是 $e = [e_l \mid e_r]$ 的左半部分。由此可知，交织可以使译码错误扩散。

文献[7]指出交织编码可以比打孔 LDPC 码得到更小的安全距离，但并没有给出一种通用的交织矩阵构造方法，因此本文从实用的角度出发，提出了简单实用的交织矩阵构造方法。

一般来说，交织矩阵越密集，译码错误的扩散就越明显，交织矩阵密度接近 0.5 时，就可以近似实现完美交织，即一个比特的译码错误就可以导致解交织后码字有一半误码[7]。下面是二进制密集交织矩阵的具体构造步骤：

a)首先由编码信息矢量 u 确定单位阵 $I_{k\times k}$，逐列(行)按指定交织密度 SD 在 $I_{k\times k}$ 中随机填“1”得到 S_0，其中 $SD \in [0.2, 0.5]$；

b)对 S_0 进行 k 次随机行列置换得到 S，同时检验 S 的行重和列重是否大于 1，若没有则重新进行适当的行列置换，得到行重和列重均大于 1 的交织矩阵 S，且 S 可逆。

由 PEG 方法[15]构造母码，得到校验矩阵 H，矩阵求逆得到生成矩阵 $G = H^{-1}$，利用 $c = uSG$ 进行编码，然后利用高斯近似分析交织 LDPC 码的 BER 性能。

1.3 部分信道特征下的人工噪声波束成型

采用人工噪声波束成型传输时，如果是部分信道特征，即 $\hat{h} = h + \Delta h$，窃听信道特征未知。因为 $\hat{h}$ 存在估计误差 Δh，肯定会有一定的人工噪声进入授权信道，影响授权信道的 SNR；窃听信道特征未知，与 $\hat{h}$ 正交的人工噪声最好采用全向发射。此时，人工噪声矢量 $z(t)$ 的协方差为 $\Sigma' = \beta P_{\hat{h}}^{\perp} = \beta(I_{N_A} - \hat{h}\hat{h}^{\mathrm{H}} / \|\hat{h}\|^2)$，Bob 的 SNR 可表示为

$$\mathrm{SNR}_B(w,\Sigma') = E[|h^{\mathrm{H}} w s(t)|^2] / (E[|h^{\mathrm{H}} z'(t)|^2] + \sigma_n^2) = w^{\mathrm{H}} R_h w / (Tr(\Sigma' R_h) + \sigma_n^2) \tag{6}$$

其中：$Tr(\cdot)$ 表示求矩阵的迹。假设 h 与 Δh 相互独立，且 Δh 中元素为独立同分布的零均值方差为 $\sigma_{\Delta,i}$ 的复高斯随机变量，则 Bob 的 SNR 可进一步简化为

$$\mathrm{SNR}_B(w,\Sigma') = \frac{w^H R_h w}{Tr(\Sigma R_h) + Tr(\mathrm{Diag}(\sigma_{\Delta,1},\cdots,\sigma_{\Delta,N_A}) R_h) + \sigma_n^2} \tag{7}$$

其中：$\mathrm{Diag}(\cdot)$ 表示除对角线元素外其他元素均为 0，$\sigma_{v,1}$ 表示对应的噪声方差。同理可知单天线 Eve 的 SNR 为

$$\mathrm{SNR}_E(w,\Sigma') = E[|g^{\mathrm{H}} w s(t)|^2] / (E[|g^{\mathrm{H}} z'(t)|^2] + \sigma_v^2) = w^{\mathrm{H}} R_s w / (Tr(\Sigma' R_g) + \sigma_v^2) \tag{8}$$

由此，可知在发射功率 P 一定的情况下，即 $\|w\|^2 + Tr(\Sigma') \leqslant P$，从安全性和可靠性折中的角度出发，问题归结为授权信道 SNR 约束下求最小私密中断概率 P_{SO}：

$$\begin{aligned} \min\ & P_{SO} = P(\mathrm{SNR}_E > \mathrm{SNR}_{E,\max} \mid \mathrm{SNR}_B \geqslant \mathrm{SNR}_{B,\min}) \\ \text{s.t.}\ & \|w\|^2 + Tr(\Sigma') \leqslant P \\ & \mathrm{SNR}_B \geqslant \mathrm{SNR}_{B,\min} \end{aligned} \tag{9}$$

在约束条件 $\mathrm{SNR}_B \geqslant \mathrm{SNR}_{B,\min}$ 满足的前提下，问题可变为

$$\begin{aligned} \min\ & P(\mathrm{SNR}_E > \gamma_E) \\ \text{s.t.}\ & \|w\|^w + Tr(\Sigma') \leqslant P \\ & \mathrm{SNR}_B \geqslant \mathrm{SNR}_{B,\min} = \gamma_B \end{aligned} \tag{10}$$

由文献[9]的分析知 $\hat{h}$ 存在估计误差时，要分配给人工噪声更多的功率才能保证一定的私密速率。因为窃听信道特征的分布信息未知，问题只能通过数值分析进行求解。

当窃听者联合(Eve 有 M 根天线)时，假设 Eve 采用最大信噪比接收波束成型，则 Eve 的接收波束成型矢量 r[13] 为

$$r = (E\Sigma' E^{\mathrm{H}} + D^2)^{-1} E w \tag{11}$$

对应 Eve 的 SNR[13] 为

$$\mathrm{SNR}_E(w,\Sigma') = \frac{r^{\mathrm{H}} T(ww^{\mathrm{H}}) r}{r^{\mathrm{H}}(T(\Sigma') + D^2) r} \tag{12}$$

此时问题变为

$$\begin{aligned} \min\ & P(\mathrm{SNR}_E > \gamma_E) \\ \text{s.t.}\ & \|w\|^2 + Tr(\Sigma') \leqslant P \\ & \mathrm{SNR}_B \geqslant \mathrm{SNR}_{B,\min} = \gamma_B \end{aligned} \tag{13}$$

同样因为窃听信道的分布特征信息未知，问题只能通过数值分析进行求解。

2 仿真分析

仿真中使用 PEG 算法产生了两个非规则 LDPC 码，第一个码：$n = 3940$，$k = 1576$，用于打孔 LDPC 码实现，打孔比为 0.4，即1576 个变量节点打孔；第二个码：$n = 2364$，$k = 1576$，用于交织 LDPC 码实现，交织密度 $SD = 0.2$。采用为 BPSK 调制，仿真条件如下：

a)使用 10 000 组测试数据，每组包含 1 576 bit 数据。

b)信道特征在每组测试数据期内保持不变，不同测试分组间保持独立。

c)所涉随机信道相互独立，每个信道的实部和虚部也相互独立，且都服从均值为 0、方差为 0.5 的正态分布，因此所涉信道增益均为 1。

d)所涉信道噪声的实部与虚部相互独立，且都服从均值为 0、方差为 0.5 的正态分布，因此噪声的功率为 1。

图 2 给出的是编码对应的误比特率，LDPC 母码比打孔 LDPC 码和交织 LDPC 码具有更低的 BER，可见交织和打孔使得 LDPC 码在低 SNR 下具有较高的 BER。图 3 仿真比较了不同编码的安全距离，给定 $P_{e,\max}^B = 10^{-5}$，$P_{e,\min}^E = 0.4$，LDPC 母码需要 SG 达到 7 dB 以上，打孔 LDPC 码则要达到 2.2 dB，交织 LDPC 码则只需 1.4 dB，可见交织 LDPC 码具有最小的安全距离，当然这只是对短码长情况下，码长变大时的情况还需要进一步研究。

部分信道特征下求最小私密中断概率，其实质是一种尽力而为的安全传输策略，即保证授权信道一定接收质量的同时最大化对窃听信道的干扰。仿真中使用交织 LDPC 编码，$P_{e,\min}^E = 0.4$，对应 SNR 门限为 $\gamma_e = 1.2$ dB，$N_A = 4$，$M = 3$。简单起见，假设 Δh 的实部和虚部相互独立且都服从均值为 0、方差为 0.5

的正态分布,且 Δh 与 h 相互独立。

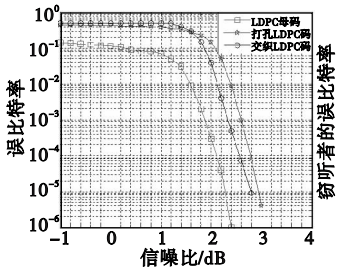

图2　安全编码误比特率

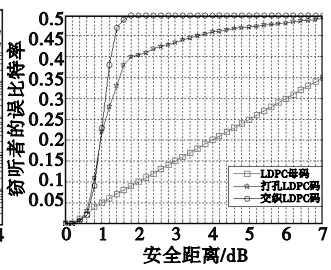

图3　安全距离性能曲线

图 4、5 给出了 γ_b 从 3 ~ 5 dB 以 1 dB 递增变化以及 P 从 5 ~ 25 dB 以 2.5 dB 递增变化时私密中断概率的变化情况,其中图 4 给出的是单窃听者的情况,图 5 给出的是窃听者联合的情况。

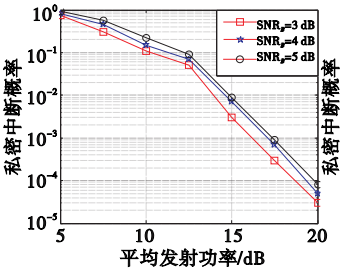

图4　单窃听者私密中断概率

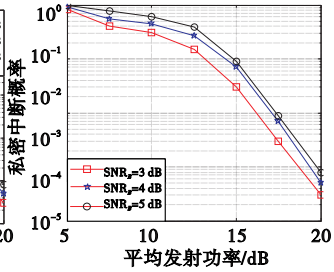

图5　窃听者联合私密中断概率

由图 4 可知,当授权信道信噪比门限 γ_b 提高时,相应的私密中断概率也提高,这是因为平均发射功率分配给人工噪声的比重降低的结果。当 γ_b 一定时,随平均发射功率的增加私密中断概率开始减小。如图 5 所示,当窃听者联合时,相同的 γ_b 下私密中断概率有了明显的提高,这时需要增加平均发射功率才能降低私密中断概率。

3　结束语

本文主要针对部分信道特征下的物理层安全传输问题,提出了一种实用的物理层安全编码方法。在采用波束成型传输的 MISO 系统中,多天线发射机通过信道反馈得到授权信道特征,波束成型发射时添加与授权信道特征完全正交的人工噪声;通过交织 LDPC 码进一步缩小安全距离,在授权信道 SNR 约束下求最小私密中断概率,实现人工噪声和发射权重的功率优化分配,使窃听信道尽可能保持低 SNR 高 BER,授权信道保持高 SNR 低 BER,满足安全编码的信道条件假设,实现物理层安全传输。仿真结果表明,在授权信道 SNR 约束下,本方法可以实现较低的私密中断概率。

参考文献:

[1] SHANNON C. Communication theory of secrecy systems[J]. Bell Systems Technical Journal,1949,29(1):656-715.

[2] WYNER A D. The wire-tap channel[J]. Bell Systems Technical Journal,1975,54(8):1355-1387.

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

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

[5] LI Jiang-yuan, PETROPULU A P. On ergodic secrecy rate for gaussian miso wiretap channels[J]. IEEE Trans on Wireless Communications,2011,10(4):1176-1187.

[6] KLINC D, HA J, MCLAUGHLIN S, *et al*. LDPC codes for physical layer security [C]//Proc of the 28th IEEE Global Telecommunications Conference. Piscataway,NJ:IEEE Press,2009:1-6.

[7] BALDI M, BIANCHI M, CHIARALUCE F. Non-systematic codes for physical layer security[C]//Proc of IEEE Information Theory Workshop. 2010:1-5.

[8] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Trans on Wireless Communications, 2008, 7(6):2180-2189.

[9] ZHOU Xiang-yun, MCKAY M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Trans on Vehicular Technology,2010,59(8):3831-3842.

[10] LIAO Wei-cheng, CHANG T H, MA W K,*et al*. QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach [J]. IEEE Trans on Signal Processing, 2011,59(3):1202-1216.

[11] MUKHERJEE A, SWINDLEHURST A L. Fixed-rate power allocation strategies for enhanced secrecy in MIMO wiretap channels[J]. IEEE SPAWC,2009,21(24):344-348.

[12] SWINDLEHURST A L. Fixed SINR solutions for the MIMO wiretap channel[C]//Proc of IEEE ICASSP. Washington DC:IEEE Computer Society,2009:2437-2440.

[13] ZHOU Xiang-yun, MCKAY M R, MAHAM B, *et al*. Rethinking the secrecy outage formulation: a secure transmission design perspective [J]. IEEE Communication Letters,2011,15(3):302-304.

[14] LI Qiang, MA W K, SO A M. Safe convex approximation to outage-based miso secrecy rate optimization under imperfect CSI and with artificial noise[C]//Proc of the 45th Annual Asilomar Conference on Signals, Systems, and Computers. 2011:207-211.

[15] HU Xiao-yu, ELEFTHERIOU E, ARNOLD D M. Regular and irregular progressive edge-growth tanner graphs[J]. IEEE Trans on Information Theory,2005,51(1):386-398.