基于人工噪声的多用户 MIMO 系统加密算法

赵家杰* 彭建华 黄开枝 吉 江
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：当多用户 MIMO 系统中的用户数多于或等于发射端天线数时，现有的基于人工噪声的物理层加密算法会导致合法用户无法正常接收。为提高此时的多用户 MIMO 系统的安全性，该文提出一种新的基于人工噪声的多用户 MIMO 系统加密算法。首先，发送端对多个合法用户进行联合处理，建立多用户联合信道状态矩阵；然后，将联合信道状态矩阵进行奇异值分解，并根据最小的奇异值进行预编码，以消除人工噪声对合法用户的影响；最后，提出一种优化功率分配的方案。仿真结果表明，该算法将多用户 MIMO 系统的保密容量平均增加了 0.1 bit/(s·Hz)，从而提高多用户 MIMO 系统的安全性。

关键词：多用户 MIMO 系统；联合信道状态矩阵；保密容量；人工噪声；物理层安全
中图分类号：TN929.53 **文献标识码**： A **文章编号**：1009-5896(2012)08-1939-05
DOI: 10.3724/SP.J.1146.2011.01068

A Multi-user MIMO System Encryption Algorithm Based on Artificial Noise

Zhao Jia-jie Peng Jian-hua Huang Kai-zhi Ji Jiang
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: The existing physical layer encryption algorithm, which is based on artificial noise, could affect legitimate receivers negatively when the number of users is no less than sending antennas in the multiuser MIMO system. In order to improve the multiuser MIMO system security under this scenario, this paper proposes a new multiuser MIMO system physical layer encryption algorithm based on joint channel state matrix. Firstly, multiple users are processed together, thus a multiuser joint channel state matrix is established. After Singular Value Decomposition (SVD) of the joint channel state matrix, the minimum singular value is obtained and can be utilized for pre-coding, so as to eliminate the interference of artificial noise to legitimate receivers. Further, the paper also presented an approach to optimize the power allocation. The simulation results show that the proposed algorithm can increase the secrecy capacity by 0.1 bit/(s·Hz) averagely, and improve the multiuser MIMO system security.

Key words: Multiuser MIMO system; Joint channel state matrix; Secrecy capacity; Artificial noise; Physical layer security

1 引言

多入多出(MIMO)技术已经成为下一代无线通信系统的关键技术之一，并且在 IEEE 802.11/16 和 3GPP LTE 标准中都采用了该技术。但是，由于电磁信号传播的广播特性和无线信道的开放性，无线通信系统传递的通信内容极易被窃听，因此如何保障多用户 MIMO 系统的通信安全变得日益重要。

由于针对多用户 MIMO 系统不存在零空间(系统中的合法用户数多于或等于发射端的天线数)的场景，利用人工噪声来进行物理层加密会对合法用户引入额外的噪声。因此，现有利用人工噪声实现多用户 MIMO 系统的物理层加密都是针对系统存在零空间的情况展开研究的。文献[1,2]通过向第三方用户发送人工噪声的方法来提高授权用户的安全性：发送端使用多天线将主瓣对准期望用户，在其它波束中发送人工噪声，从而抑制潜在窃听用户的接收。文献[3]研究了当窃听方位置未知的时候，利用波束赋形与人工噪声结合的方法来提高保障通信安全。文献[4]从空域和频域结合的角度出发，通过引入冗余发射人工噪声来干扰窃听方，从而保障合法用户的通信安全。文献[5,6]研究了在多用户下行情况下，采用人工噪声干扰窃听用户的加密方案。其中文献[5]分别针对 MIMO 广播信道和 MIMO 多点传输研究了线性波束赋形结合人工噪声的安全效果，并研究了在保证期望用户信干噪比不变情况下

2011-10-17 收到，2012-04-20 改回
国家自然科学基金(61171108)资助课题
*通信作者：赵家杰 zhaojiajie@gmail.com

的噪声功率分配方案。文献[7–9]从信息论的角度推导并证明了高斯 MIMO 和 MISO 窃听信道存在多个合法用户和多个窃听用户时的保密容量范围。文献[10]具体研究了如何分配噪声功率，从而实现最大化保密容量。文献[11]研究了当发射端天线数量有限时，为了使系统存在零空间，如何从下行多用户中选取 k 个用户来确保系统的安全性。上述研究应用场景受限，限制了系统用户容量。

本文针对多用户 MIMO 系统不存在零空间的场景，将人工噪声消除问题转化为预编码设计问题，提出了一种基于人工噪声的多用户 MIMO 系统加密算法。首先，发送端对多个合法接收用户进行联合处理，建立多用户联合信道状态矩阵和补矩阵；然后，分别对联合信道状态矩阵和补矩阵进行奇异值分解，并根据最小的奇异值进行预编码，以消除人工噪声对合法用户的影响和多用户干扰；最后，提出了一种优化功率分配的方案。本文建立联合信道状态矩阵充分考虑了多用户系统可能存在的问题，通过预编码既抑制了人工噪声对合法用户的影响又消除了多用户间的干扰，迫使人工噪声在对合法用户影响最小的子信道上传输，而大部分人工噪声落在窃听方。仿真结果表明，系统的保密容量平均提高了 0.1 bit/(s·Hz)，有效保障了多用户 MIMO 系统的安全性。

2 多用户 MIMO 系统加密模型

多用户 MIMO 系统的加密模型如图 1 所示。假设发送端拥有 N_T 根发射天线， K 个合法用户的接收天线均为 N_R 根。有 1 个窃听用户，其接收天线数为 N_E 根。

第 k 个合法用户和窃听用户接收到的信号分别为

$$y_k = \boldsymbol{H}_k\boldsymbol{t}_k b_k + \boldsymbol{H}_k\sum_{j\neq k}^{K}\boldsymbol{t}_j b_j + \boldsymbol{H}_k\boldsymbol{p}z + n_k \tag{1}$$

$$y_e = \boldsymbol{H}_e\sum_{j=1}^{K}\boldsymbol{t}_j z_j + \boldsymbol{H}_e\boldsymbol{p}z + n_e \tag{2}$$

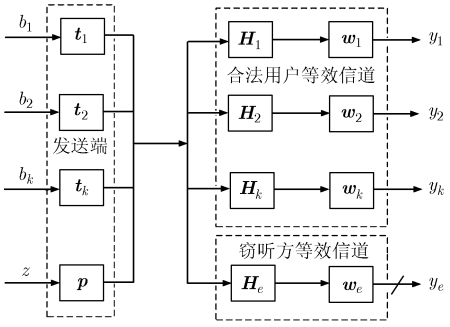

图 1 多用户 MIMO 系统物理层加密模型

其中 b_k 为第 k 个合法用户发送的信号，$\boldsymbol{H}_k$ 为第 k 个合法用户的信道状态矩阵，$\boldsymbol{H}_e$ 为窃听用户的信道状态矩阵，$\boldsymbol{t}_k$ 和 $\boldsymbol{p}$ 分别为消除多用户干扰和人工噪声对合法用户影响的预编码且均为 $N_T\times 1$ 维， z 为人工噪声，n_k 和 n_e 分别为合法用户与窃听用户的加性高斯白噪声。

第 k 个合法用户与窃听用户对信号的估计分别为

$$\tilde{y}_k = \boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k b_k + \boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\sum_{j\neq k}^{K}\boldsymbol{t}_j b_j + \boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}z + \boldsymbol{w}_k^{\mathrm{H}}n_k \tag{3}$$

$$\tilde{y}_e = \boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\sum_{j=1}^{K}\boldsymbol{t}_j\boldsymbol{b}_j + \boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{p}z + \boldsymbol{w}_e^{\mathrm{H}}n_e \tag{4}$$

其中 $\boldsymbol{w}_k$ 和 $\boldsymbol{w}_e$ 分别为第 k 个合法用户与窃听方的波束赋形加权且均为 $N_R\times 1$ 维向量， $\boldsymbol{w}_k^{\mathrm{H}}$ 和 $\boldsymbol{w}_e^{\mathrm{H}}$ 为 $\boldsymbol{w}_k$ 和 $\boldsymbol{w}_e$ 共轭转置。

3 基于人工噪声的多用户 MIMO 系统加密算法

当系统存在多个合法用户时，利用人工噪声进行加密必须满足两点要求：(1)防止多用户之间的互干扰；(2)人工噪声对合法用户的影响最小。根据这两点要求，加密算法的主要思想是设计预编码 $\boldsymbol{p}$ 和 $\boldsymbol{t}_k$， 使信号经过合法用户信道后能滤掉大量的人工噪声和多用户间的干扰，而窃听方受到人工噪声的干扰无法正确解调。从式(3)，式(4)可以看出合法用户受到小部分人工噪声的干扰 $\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}z$ 和信道中存在的自然加性噪声 $\boldsymbol{w}_k^{\mathrm{H}}n_k$ 的影响，窃听方受到用户间的干扰 $\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\sum_{j\neq k}^{K}\boldsymbol{t}_j b_j$， 大部分人工噪声 $\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{p}z$ 以及信道中的自然加性噪声 $\boldsymbol{w}_e^{\mathrm{H}}n_e$ 的影响。从上述分析可以看出，预编码 $\boldsymbol{t}_k$ 和 $\boldsymbol{p}$ 的设计直接关系到能否消除人工噪声对合法用户的影响和多用户干扰，然而 $\boldsymbol{t}_k$ 和 $\boldsymbol{p}$ 是通过构造补矩阵和联合信道状态矩阵并分别对其进行奇异值分解才得到的预编码。因此，算法可以分为基于补矩阵奇异值分解的预编码和基于联合信道状态矩阵奇异值分解的预编码两大模块。

3.1 基于补矩阵奇异值分解的预编码

采用改进的迫零波束赋形方法[5]，首先在接收端进行波束赋形其加权向量为 $\boldsymbol{w}_l$， 然后定义补矩阵 $\widetilde{\boldsymbol{H}}_l = [\tilde{\boldsymbol{h}}_1,\cdots,\tilde{\boldsymbol{h}}_{l-1},\tilde{\boldsymbol{h}}_{l+1},\cdots,\tilde{\boldsymbol{h}}_K]^{\mathrm{T}}$ ， 且 $\tilde{\boldsymbol{h}}_l = (\boldsymbol{w}_l^{\mathrm{H}}\boldsymbol{H}_l)^{\mathrm{T}}$ 是 $N_T\times 1$ 的向量，可以得知 $\widetilde{\boldsymbol{H}}_l$ 为 $(K-1)\times N_T$ 维，最后对其进行奇异值分解得 $\widetilde{\boldsymbol{H}}_l = \widetilde{\boldsymbol{U}}_l\widetilde{\boldsymbol{D}}_l\widetilde{\boldsymbol{V}}_l^{\mathrm{H}}$ 。当 $K\le N_T$ 时， $\widetilde{\boldsymbol{H}}_l$ 的行小于列，奇异值分解存在零空间，右奇异向量可以继续分解为 $\widetilde{\boldsymbol{V}}_l = [\widetilde{\boldsymbol{V}}_l^{(s)}\widetilde{\boldsymbol{V}}_l^{(0)}]^{\mathrm{H}}$， $\widetilde{\boldsymbol{V}}_l^{(s)}$ 为非零奇异值对应的右奇异向量， $\widetilde{\boldsymbol{V}}_l^{(0)}$ 为补矩

阵的零空间。因此，可得基于 $\widetilde{\boldsymbol{H}}_l$ 奇异值分解的预编码 $\boldsymbol{t}_k=\widetilde{\boldsymbol{V}}_l^{(0)}$。

3.2 基于联合信道状态矩阵奇异值分解的预编码

要使人工噪声同时满足对 K 个合法用户的影响最小，定义联合信道状态矩阵为 $\boldsymbol{H}_k=[\tilde{\boldsymbol{h}}_1,\cdots,\tilde{\boldsymbol{h}}_K]^{\mathrm{T}}$，其中 $\tilde{\boldsymbol{h}}_l=(\boldsymbol{w}_l^{\mathrm{H}}\boldsymbol{H}_l)^{\mathrm{T}}$ 是 $N_T\times 1$ 的向量，$\boldsymbol{H}_k$ 为 $K\times N_T$ 维，进行奇异值分解得 $\boldsymbol{H}_k=\widetilde{\boldsymbol{U}}_k\widetilde{\boldsymbol{D}}_k\widetilde{\boldsymbol{V}}_k^{\mathrm{H}}$。

当 $K<N_T$ 时，$\boldsymbol{H}_k$ 的行小于列，奇异值分解存在零空间，右奇异向量可以继续分解为 $\widetilde{\boldsymbol{V}}_k=[\widetilde{\boldsymbol{V}}_k^{(s)}\widetilde{\boldsymbol{V}}_k^{(0)}]^{\mathrm{H}}$，$\widetilde{\boldsymbol{V}}_k^{(0)}$ 为 $\boldsymbol{H}_k$ 的零空间，可得基于 $\boldsymbol{H}_k$ 奇异值分解的预编码 $\boldsymbol{p}=\widetilde{\boldsymbol{V}}_k^{(0)}$，此时通过预编码人工噪声对合法用户的干扰为零。当 $K\geq N_T$ 时，右奇异向量可以继续分解为 $\widetilde{\boldsymbol{V}}_k=[\widetilde{\boldsymbol{V}}_k^{(s)}]^{\mathrm{H}}$，此时 $\boldsymbol{H}_k$ 分解不存在零空间，即多用户 MIMO 系统不存在零空间。为了使人工噪声落在对合法用户影响最小的子信道传输，以达到减少对合法用户影响的效果，选取 $\widetilde{\boldsymbol{V}}_k^{(s)}$ 中对应奇异值最小的向量为预编码 $\boldsymbol{p}$。其具体计算步骤如下：

(1)对 $\boldsymbol{h}_k$ 进行奇异值分解，并选择最大奇异值对应的左奇异向量为 $\boldsymbol{w}_k$；

(2)构造补矩阵 $\widetilde{\boldsymbol{H}}_l=[\tilde{\boldsymbol{h}}_1,\cdots,\tilde{\boldsymbol{h}}_{l-1},\tilde{\boldsymbol{h}}_{l+1},\cdots,\tilde{\boldsymbol{h}}_K]^{\mathrm{T}}$，并对其进行奇异值分解得到预编码 $\boldsymbol{t}_k$，用于消除多用户干扰；

(3)构造联合信道状态矩阵 $\boldsymbol{H}_k=[\tilde{\boldsymbol{h}}_1,\cdots,\tilde{\boldsymbol{h}}_K]^{\mathrm{T}}$，并对其进行奇异值分解得到预编码 $\boldsymbol{p}$，用于消除人工噪声对合法用户的影响。

4 性能分析

4.1 安全性能分析

根据文献[4]关于保密容量的定义，可以推出不存在零空间下的多用户 MIMO 系统第 k 个用户的保密容量为

$$C_{\mathrm{sec}}\geq\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2\sigma_u^2}{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}\right|^2\sigma_z^2+\sigma_n^2}\right)-\log_2\left(1+\frac{\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_k\right|^2\sigma_u^2}{\sum\limits_{j\neq k}^{K}\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_j\right|^2\sigma_u^2+\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{p}\right|^2\sigma_z^2+\sigma_e^2}\right)\tag{5}$$

其中 $\sigma_u^2,\sigma_z^2,\sigma_n^2,\sigma_e^2$ 分别表示第 k 个用户分配的信号功率、人工噪声功率、合法用户信道的噪声功率，以及窃听用户信道的噪声功率。当且仅当干扰项与人工噪声均服从高斯分布时，等式成立，即可以得到高斯信道下的多用户 MIMO 系统的第 k 个用户的保密容量为

$$C_{\mathrm{sec}}=\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2\sigma_u^2}{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}\right|^2\sigma_z^2+\sigma_n^2}\right)-\log_2\left(1+\frac{\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_k\right|^2\sigma_u^2}{\sum\limits_{j\neq k}^{K}\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_j\right|^2\sigma_u^2+\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{p}\right|^2\sigma_z^2+\sigma_e^2}\right)\tag{6}$$

从式(6)可以看出在总功率受限的条件下，一部分功率用来发射人工噪声，这个信号功率与噪声功率的分配问题直接影响到保密容量。假设用户之间的功率是均匀分配的，且有用功率分配系数为 φ，则第 k 个用户的功率为 $p_k=\varphi P/K$，第 k 个用户噪声分配的功率为 $p_n=(1-\varphi)P/K$，第 k 个用户的信道容量为

$$C_{Ak}=\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2\varphi P}{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}\right|^2(1-\varphi)P+K\sigma_n^2}\right)\tag{7}$$

窃听方的信道容量为

$$C_{Ae}=\log_2\left(1+\frac{\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_k\right|^2\varphi P}{\sum\limits_{j\neq k}^{K}\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_j\right|^2\varphi P+\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{p}\right|^2(1-\varphi)P+K\sigma_e^2}\right)\tag{8}$$

设 $A=\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2$，$B=\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}\right|^2$，$C=K\delta_n^2$，$D=\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_k\right|^2$，$E=\sum\limits_{j\neq k}^{K}\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{t}_j\right|^2$，$F=\left|\boldsymbol{w}_e^{\mathrm{H}}\boldsymbol{H}_e\boldsymbol{p}\right|^2$，$G=K\delta_e^2$，则有

$$C_{Ak}=\log_2\left(1+\frac{A\varphi P}{B(1-\varphi)P+C}\right)\tag{9}$$

$$C_{Ae}=\log_2\left(1+\frac{D\varphi P}{E\varphi P+F(1-\varphi)P+G}\right)\tag{10}$$

对保密容量公式 $C_{\mathrm{sec}}=C_{Ak}-C_{Ae}$ 进行求导，并令其等于零得到 φ 的一元二次等式为

$$(z_1a_1b_1-z_2a_2b_2)\varphi^2+(z_1a_1h_1+z_1b_1h_1-z_2a_2h_2-z_2b_2h_2)\varphi+z_1h_1^2-z_2h_2^2=0\tag{11}$$

其中 $a_1=E-F+D,a_2=A-B,b_1=E-F,b_2=-B,h_1=F+G,h_2=B+C,z_1=Ah_2,z_2=dh_1$，通过以上公式可以讨论判断得到 φ 的取值使第 k 个用户的保密容量最大。

4.2 系统性能分析

由式(7)可得不加人工噪声即 $\varphi=1$ 时，第 k 个用户的信道容量为

$$C_{Ak}=\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2 P}{K\sigma_n^2}\right) \tag{12}$$

那么不加人工噪声时系统的和容量为

$$C=\sum_{k=1}^{K}\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2 P}{K\sigma_n^2}\right) \tag{13}$$

同理可得加人工噪声后系统的和容量为

$$C_z=\sum_{k=1}^{K}\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2 \varphi P}{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}\right|^2(1-\varphi)P+K\sigma_n^2}\right) \tag{14}$$

于是可得通过人工噪声加密后系统损失的和容量为

$$\begin{aligned}\Delta C=C-C_z=&\sum_{k=1}^{K}\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2 P}{K\sigma_n^2}\right)\\&-\sum_{k=1}^{K}\log_2\left(1+\frac{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k\right|^2 \varphi P}{\left|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}\right|^2(1-\varphi)P+K\sigma_n^2}\right)\end{aligned} \tag{15}$$

由式(15)系统损失的和容量与接收端波束赋形向量 $\boldsymbol{w}_k$ 以及消除多用户干扰的预编码 $\boldsymbol{t}_k$，减少人工噪声影响的预编码 $\boldsymbol{p}$，有效功率分配系数 φ 密切相关，在上节的分析均给出了预编码的设计原则，即让有用信号在主信道发送即使 $|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{t}_k|^2$ 最大，让人工噪声在次信道上发送即 $|\boldsymbol{w}_k^{\mathrm{H}}\boldsymbol{H}_k\boldsymbol{p}|^2$ 最小，这样人工噪声对合法用户影响最小，系统损失的和容量也最小。

5 仿真与分析

5.1 保密容量

首先，本文依据文献[6]的方法对系统存在零空间下的加密进行了保密容量与和容量的仿真。假设发送方与接收方的天线数均为 4，合法用户数为 3，合法用户信道状态已知且归一化，总功率恒为 500 mW。系统中第 k 个用户的保密容量与和容量的仿真如图 3 和图 4 所示。

图 2 横坐标为用户信道噪声功率与窃听方信道噪声功率的比值，纵坐标为保密容量。在未加人工噪声之前，由于多用户间的干扰对第三方的影响使其部分保密容量大于零；加人工噪声后，保密容量整体提高，致使 $40\le\sigma_n^2/\sigma_e^2\le100$ 部分保密容量均大于零，从而实现安全通信。图 3 表示由于发射功率受限，所以加密后对和容量有一定的损失，且噪声功率分配越多损失越大。

然后，保持其它仿真条件不变将合法用户数增加到 4 个，此时系统不存在零空间，依照本文算法得到的第 k 个用户保密容量与和容量的仿真如图 4 和图 5 所示。

图 4 可以看出在系统不存在零空间的情况下，通过人工噪声仍然可以提高系统的保密容量。但是，由于系统不存在零空间，其保密容量比有零空间下的系统保密容量有下降。并且，当有用功率分配系数为 0.8 且 $70\le\sigma_n^2/\sigma_e^2\le100$ 时，系统不能实现安全通信。随着合法用户的信道条件变差，有用功率分配系数为 0.6 或 0.4 的保密容量逐步高于有用功率分配系数为 0.8 的保密容量。这表明在一定条件下，通过发射更多的人工噪声来扰乱窃听方，可以有效提高保密容量，从而实现安全通信。

图 5 表明当系统不存在零空间的情况下，人工噪声对合法用户有部分影响，所以通过人工噪声进行加密加剧了对和容量的损失，有用功率分配系数为 0.8 和 0.4 的和容量损失量为未加密前和容量的 1/4 和 1/2。虽然和容量损失较大，但由于用户数的增多，其加密后的和容量高于系统存在零空间下的和容量。综上所述，本文算法的实质是通过损失一定的和容量来提高保密容量。

5.2 功率分配

假设总功率恒为 500 mW，系统中第 k 用户保密容量随有用信号功率分配系数变化的仿真如图 6 所示。当 $\sigma_n^2/\sigma_e^2=20$，仿真得到的已知条件为

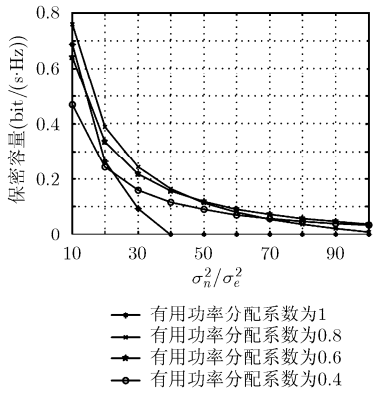

图 2 保密容量

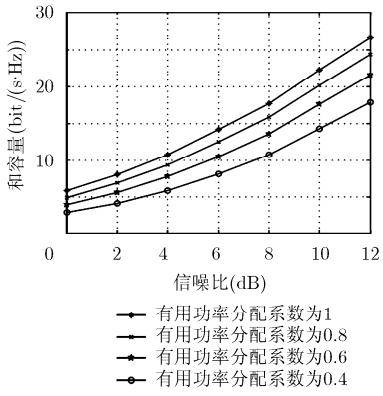

图 3 和容量

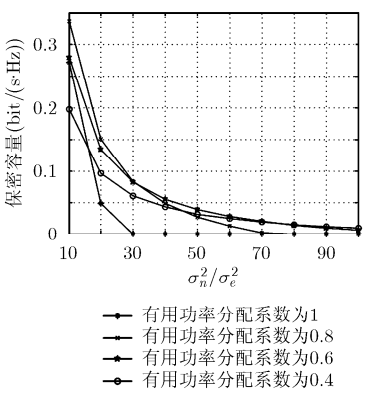

图 4 保密容量

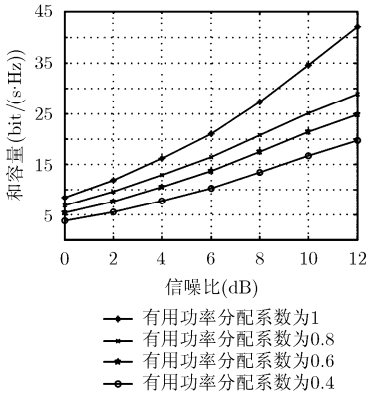

图 5 和容量

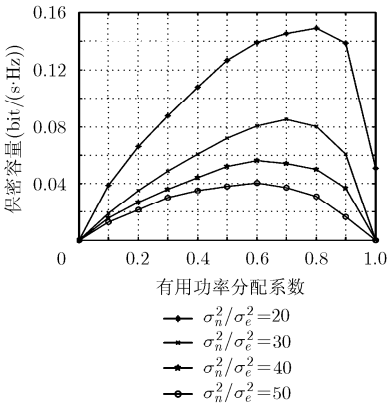

图 6 保密容量与有用功率分配系数的关系

$A=0.0775,\ B=0.0067,\ C=80,\ D=9.786\times10^{-4},$
$E=1.0048,\ F=0.0012,\ G=4$

代入式(10)并解方程可以得出使保密容量最大(即安全传输下的最大传输速率)的功率分配系数为 φ，同理当 σ_n^2/σ_e^2 变动时，只变动 C 即可。

图 6 表明在不存在零空间的多用户 MIMO 系统中，人工噪声的发射功率过小尤其是小于总功率的 0.1 情况下，保密容量急速下降，条件更差的情况下就不能实现安全传输。随着合法用户信道条件变差，最佳分配系数也逐步左移，即在窃听方信道明显优于合法用户的时候，分配的人工噪声功率也越来越多。

6　结束语

本文针对多用户 MIMO 系统不存在零空间的场景，提出了一种基于人工噪声的多用户 MIMO 系统加密算法。该算法通过预编码来抑制人工噪声对合法用户的影响。为此，建立联合信道状态矩阵；然后对联合信道状态矩阵进行奇异值分解，并根据最小奇异值来进行预编码；最后，提出了一种优化功率分配的方案。仿真分析表明，当多用户 MIMO 系统不存在零空间时，引入人工噪声进行物理层加密，在牺牲一定和容量的条件下有效提高保密容量；当合法用户信道条件变差时，为使保密容量最大，分配的人工噪声功率也越来越多。

参 考 文 献

[1] Negi R and Goel S. Secure communications using artificial noise[C]. IEEE Vehicle Technology Conference(VTC), Dallas, TX, September 2005: 1906–1910.

[2] Goel S and Negi R. Guaranteeing secrecy using artificial noise[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189.

[3] Ghogho M and Swami A. Physical layer secrecy of MIMO communications in the presence of a poisson random field of eavesdroppers[C]. IEEE ICC Workshop on Physical Layer Security, Kyoto, Japan, June 2011: 1–5.

[4] Ghogho M and Zurita1 N R. Physical layer security of MIMO frequency selective channels by beamforming and noise generation[C]. European Signal Processing Conference, Barcelona, Spain, Augest 2011: 829–833.

[5] Mukherjee A and Swindlehurst A L. Utility of beamforming strategies for secrecy in multiuser MIMO wiretap channels[C]. Proceedings of the Forty-Seventh Allerton Conference, Monticello, Oct. 2009: 1134–1141.

[6] Liao W, Chang T, and Ma W. Joint transmit beamforming and artificial noise design for QoS discrimination in wireless downlink[C]. Proceedings of the IEEE International Conference on Acoustics, Speech, and Signal Processing, Dallas, Mar. 2010: 2562–2565.

[7] Ekrem E and Ulukus S. The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel[J]. *IEEE Transactions on Information Theory*, 2011, 57(4): 2083–2114.

[8] Khisti A and Wornell G W. Secure transmission with multiple antennas Part II: the MIMOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2010, 56(11): 5515–5532.

[9] Khisti A and Wornell G W. Secure transmission with multiple antennas I: the MISOME wiretap channel[J]. *IEEE Transactions on Information Theory*, 2010, 56(7): 3088–3104.

[10] Zhou X and Mckay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[C]. International Conference Signal Processing and Communication Systems, Omaha, NE, Oct. 2010: 3831–3842.

[11] Mukherjee A and Swindlehurst A L. User selection in multiuser MIMO systems with secrecy considerations[C]. Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, 2009: 1479–1482.

赵家杰：　男，1986 年生，硕士生，研究方向为移动通信关键技术及无线网络安全.

彭建华：　男，1966 年生，教授，硕士生导师，研究方向为第 4 代移动通信关键技术及无线网络安全.

黄开枝：　女，1973 年生，副教授，研究方向为第 4 代移动通信关键技术及异构无线网络安全.

吉　江：　男，1983 年生，博士生，研究方向为移动通信关键技术及无线网络安全.