

基于随机天线阵的物理层安全通信系统峰均功率比问题研究

洪涛^{*①} 宋茂忠^② 王保云^③

^①(南京邮电大学通信与信息工程学院 南京 210003)

^②(南京航空航天大学电子信息工程学院 南京 210016)

^③(南京邮电大学自动化学院 南京 210003)

摘要: 采用多天线发射方式保障通信信息的安全传输是物理层安全通信研究领域常采用的手段之一,但这种方式会导致发射信号高峰均功率比的缺点,从而影响合法用户的通信性能。该文从多天线发射的加权系数出发,定义了基于多天线发射方式的物理层安全通信信号峰均功率比(PAPR)概念,并且针对随机天线阵物理层安全通信系统提出一种基于部分传输序列的物理层安全通信信号 PAPR 抑制算法。仿真结果表明该文提出的 PAPR 抑制算法能在不降低发射信号安全性能的前提下有效地降低发射信号的 PAPR 值。

关键词: 无线通信; 物理层安全; 峰均功率比; 部分传输序列

中图分类号: TN92

文献标识码: A

文章编号: 1009-5896(2015)01-0188-05

DOI: 10.11999/JEIT140089

Research on Peak-to-average Power Ratio Problem for the Physical Layer Security Communication System Using Random Antenna Array

Hong Tao^① Song Mao-zhong^② Wang Bao-yun^③

^①(College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

^②(College of Electronic and Engineering, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China)

^③(College of Automation, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Using multiple transmit antennas to guarantee the information security is one of the common methods in the field of physical layer security communication. However, this method leads to the transmit signal with the drawback of high Peak-to-Average Power Ratio (PAPR), which degrades the communication performance for the desired receiver. In this paper, the PAPR conception for security communication signal based on the weighted antenna array is defined from the point view of weighted value. The degradation performance of the desired receiver is also analyzed. In addition, a PAPR reduction algorithm is proposed for the physical layer security communication system using a random antenna array. Simulation results show that the proposed algorithm reduces the PAPR value for the security communication signal under the condition that the security performance does not reduce.

Key words: Wireless communication; Physical layer security; Peak-to-Average Power Ratio (PAPR); Partial transmit sequence

1 引言

随着无线通信技术在民用军事等方面的广泛应用,通信信息在传输过程中的安全性问题越来越受到人们的关注。无线信道的开放性使得窃听方能够接收到与合法用户相同的无线通信信号,传统的上

层加密解决方案逐渐受限于窃听方计算能力的日益增强和 Ad-hoc 等无中心网络密钥管理和分配等因素。如何在物理层利用无线通信系统自身的特点来解决通信信息的安全传输成为信息安全研究领域新的热点。物理层安全通信涉及多个交叉研究方向,包括信息论^[1]、编码技术^[2]、多输入多输出(MIMO)系统^[3,4]、调制技术^[5]、信号处理技术^[6]等,研究目的是在物理层实现通信信息安全传输给合法用户而不泄露给恶意的非法用户。

MIMO 天线系统应用于无线通信系统中,一般都是用来提高无线通信系统的信道容量。近年来,

2014-01-15 收到, 2014-05-30 改回

国家自然科学基金(61302102, 61271232), 江苏省属高校自然科学基金面上项目(13KJB510023), 国家博士后自然科学基金(2013M531390)和南京邮电大学人才引进项目(NY212020)资助课题

*通信作者: 洪涛 hongt@njupt.edu.cn

研究者们开始将 MIMO 系统应用于物理层安全通信研究领域中, 利用多天线收发系统提供的空间冗余度, 牺牲无线通信系统信道容量的提升而去换取发射信号安全性能的提升。文献[7]提出了一种基于随机天线阵列的物理层安全传输方法, 通过对发射天线随机加权的方法, 使得发射机与窃听者之间的无线信道快速变化, 窃听者使用的盲估计算法无法得到收敛的解, 确保无线通信信息在物理层的安全传输; 文献[8]在此基础上改进了随机天线阵权系数的设计算法, 提高了期望用户的功率利用率; 文献[9]将随机天线阵与扩频技术相结合提出了一种具有一定抗干扰能力的物理层安全通信信号; 文献[10]将随机天线阵思想拓展到 OFDM 通信系统中, 提出了一种基于分布式差分编码的协同 OFDM 物理层安全通信系统, 采用多个中继点协同的思想解决通信信息在物理层的安全传输。这类研究文献核心思想都是采用对于多个发射天线随机加权的方法, 使得窃听者与基站之间的信道快速随机变化而多天线发射信号与合法用户之间的等效信道保持恒定, 利用基站发射端多天线发射提供的空间冗余度确保窃听接收机无法跟踪基站发射信号的等效信道信息, 增加发射信号的安全性能。

文献[11]基于 MIMO 系统提出了一种人工噪声辅助的物理层安全通信系统, 利用多天线提供的空间冗余度, 在合法用户的正交信道上人为地加上干扰信号破坏窃听信道, 保证通信信息的安全传输; 在此基础上, 文献[12]设计了一种基于波束形成的人工噪声辅助物理层安全通信系统, 利用加权发射形成空间正交的和差波束, 和波束用来传输通信信息而差波束用来破坏窃听信道; 文献[13]研究了人工噪声辅助的物理层安全通信系统中通信信息发射功率和人工噪声最优分配算法; 文献[3,4]从信息论的角度给出了基于 MIMO 系统的物理层安全通信系统的安全信道容量。文献[14]中证明了随机天线阵物理层安全通信系统和人工噪声辅助的物理层安全通信系统具有统一的数学模型和共同的物理实质, 即在合法用户的合法信道上传输通信信息, 而在其正交信道上发送干扰信号影响窃听者的窃听性能。因此, 上述的研究文献都可以归于基于 MIMO 系统的物理层安全通信系统。

上述采用多天线发射方式的物理层安全通信系统的研究主要集中在如何设计不同的加权算法防止窃听方对于通信信息的窃听, 而忽略了发射信号本身由于加权算法存在严重的峰均功率比问题, 当发射信号的峰值功率超过功率放大器的线性范围时, 会导致带内信号失真, 从而使得合法用户的通信性

能下降。本文从发射天线加权系数出发, 定义了这一类物理层安全通信系统发射信号峰均功率比的概念。并且针对基于随机天线阵的物理层安全通信系统, 在不影响发射信号防窃听性能的前提下, 提出了一种基于部分传输序列的峰均功率比抑制算法。为这一类采用多天线发射方式实现的物理层安全通信系统实际应用奠定理论基础。

2 峰均功率比问题的提出

图 1 中给出了基于多天线加权发射方式的物理层安全传输系统模型^[7-9]。Alice 作为发射机可以配置多天线的发射系统。Bob 作为移动终端, 只能配置简单的单天线接收系统。Eve 作为窃听者, 可以配置多天线的接收系统窃听通信信息。文献[11]中证明当发射天线数目大于窃听接收机的接收天线数目时, 仍然可以保证通信信息在物理层的安全传输。这就要求发射机天线数目随着窃听接收机天线数目的增加而增加, 但随着发射机天线数目的增加会导致发射信号严重的峰均功率比问题, 这也是本文的研究目的之所在, 在后面的叙述中会详细论述。权系数设置有两类主要算法: 一种是人工噪声辅助的方式; 一种是随机天线阵加权的方式。并且文献[14]中证明了这两种加权方式具有统一的数学模型, 在物理实质上是相同的。因此, 本文以文献[7-9]中随机天线阵的方式来说明这种多天线加权发射方式的物理层安全通信信号具有高峰均功率比的缺点。

不失一般性, 假设 Alice 发射天线数为 N , Bob 采用单天线接收, Eve 接收天线数为 J 。则 Alice 与 Bob 之间的信道可以表示为如式(1)的 $N \times 1$ 维向量:

$$\mathbf{H}_{AB} = \mathbf{H}_{BA} = [h_{AB,1}, h_{AB,2}, \dots, h_{AB,N}]^T \quad (1)$$

发射天线对应的加权系数表示为

$$\mathbf{w} = [w_1, w_2, \dots, w_N]^T \quad (2)$$

Alice 与 Eve 之间的信道可以表示为 $\mathbf{H}_{AE}$ 。将调制信号符号 $b(m)$ 分配到 N 个发射天线上加权发射, 则第 n 根天线发射信号表示为

$$S(m, n) = \sqrt{\frac{P}{N}} b(m) \frac{w(n)}{\|\mathbf{w}\|}, \quad n = 1, 2, \dots, N \quad (3)$$

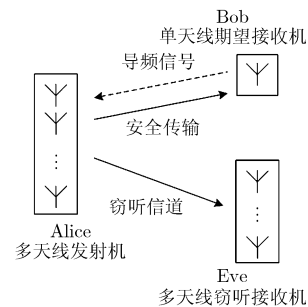


图 1 基于多天线加权发射方式的物理层安全通信系统模型

其中, P 为 N 根发射天线发射总功率, $n = 1, 2, \dots, N$ 表示第 n 个发射天线, $m = 1, 2, \dots, M$ 表示第 m 个调制符号。为了防止窃听接收机对于通信信息的窃听, 权系数的设计算法如下所示:

(1) 随机选择一个发射天线对应的权系数

$w_i, i = 1, 2, \dots, N$ (选取发射天线 $|h_i| > \alpha$);

(2) 随机产生 $N - 1$ 个权系数, 服从均值为 0 方差为 1 的复高斯随机分布;

(3) 根据式(4)计算第 i 个权系数 w_i :

$$\mathbf{w}^T \mathbf{H}_{AB} = \|\mathbf{H}_{AB}\| \quad (4)$$

其中 $\|\mathbf{H}_{AB}\| = (\mathbf{H}_{AB}^H \mathbf{H}_{AB})^{1/2}$;

(4) 整个天线系统的发射权系数归一化为处理

1, 加权系数 $\mathbf{w}(n) = \frac{\mathbf{w}(n)}{\|\mathbf{w}\|}$, $n = 1, 2, \dots, N$ 。

在上述的发射算法下, 期望接收机和窃听接收机的接收信号分别表示如下:

$$x_{\text{Bob}}(m) = b(m) \frac{\sqrt{P}}{\|\mathbf{w}\|} \|\mathbf{H}_{AB}\| + v_{\text{Bob}}(m) \quad (5)$$

$$x_{\text{Eve}}(m) = b(m) \frac{\sqrt{P}}{\|\mathbf{w}\|} \mathbf{w}^T \mathbf{H}_{AE} + v_{\text{Eve}}(m) \quad (6)$$

其中, $v_{\text{Bob}}(m)$ 和 $v_{\text{Eve}}(m)$ 分别为 Bob 和 Eve 的加性高斯白噪声。因此, 对于 Bob 可以通过式(7)直接解调出发射的调制符号 $b(m)$ 的估计值:

$$\hat{b}(m) = \arg \min_{b(m)} \left| b(m) \frac{\sqrt{P}}{\|\mathbf{w}\|} \|\mathbf{H}_{AB}\| - x_{\text{Bob}}(m) \right|^2 \quad (7)$$

由于发射天线的维度大于窃听天线的维度 ($N > J$), Eve 无法采用盲估计算法有效地跟踪发射信号的变化, 从而无法解调出通信信息。这要求系统发射天线数需要随着窃听天线数的增加而增加, 这就导致发射信号高峰均功率比的缺点。本文从发射天线的加权系数值出发定义发射信号的峰均功率比如式(8)所示。

$$\text{PAPR} = \frac{\max_{1 \leq n \leq N} |\mathbf{w}(n)|^2}{\mathbb{E}[\|\mathbf{w}(n)\|^2]} \quad (8)$$

根据式(4)计算第 i 个权系数 w_i 是线性运算, 其余 $N - 1$ 个权系数是随机产生的, 可能导致第 i 个权系数 w_i 具有高的峰值, 并且权系数的峰值随着发射天线数的增加逐渐恶化, 这点类似于 OFDM 信号 IFFT 运算产生高的峰均功率比值。图 2 给出了不同发射天线数的条件下, 发射信号峰均功率比的互补累计分布函数曲线图。由图 2 可以看出随着发射天线数的增加发射信号峰均功率比逐渐恶化, 当发射天线为 32 根时, 发射信号峰均功率比值超过 10 dB 的可能性为 50%。相比于子载波数为 1024 的 OFDM 信号(峰均功率比值超过 10 dB 的可能性为 10%), 这种基于多天线加权方式发射的物理层安全通信信号具有更严重的峰均功率比问题。

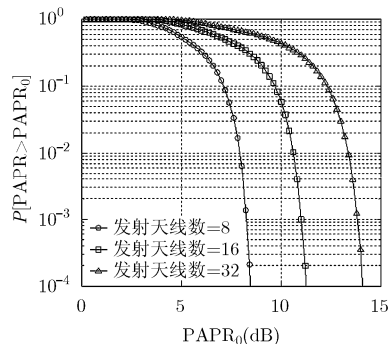


图 2 不同发射天线数对应的峰均功率比互补累计分布函数曲线图

3 基于部分传输序列的峰均功率比降低算法

本节提出一种基于部分传输序列的峰均功率比抑制算法。首先, 将权系数 $\mathbf{w}(n)$, $n = 1, 2, \dots, N$ 分为 U 个不相交的权系数块 $\mathbf{w}^{(u)}$, $u = 1, 2, \dots, U$, 本文中权系数块称为部分传输序列, 部分传输序列对应的发射天线信道信息表示为 $\mathbf{H}_{AB}^{(u)}$, 并且满足 $\mathbf{w} = \sum_{u=1}^U \mathbf{w}^{(u)}$; 然后, 引入相位旋转因子 $p^{(u)} = e^{j\phi^{(u)}}$, $\phi^{(u)} \in [0, 2\pi)$, $p^{(u)}$ 只改变权系数矢量的相位值而不改变系数矢量的幅值, 因此并不影响算法对于 Eve 的干扰性能。为了简化相位因子的搜索复杂度, 相位因子取有限的集合 $\phi^{(u)} \in \{0, \pi/2, \pi, 3\pi/2\}$; 最后, 改变不同分块对应的旋转相位 $\phi^{(u)}$, 采用式(9)得到不同的第 i 个权系数 w_i 的解集合。

$$\{w_i\} = \frac{\|\mathbf{H}_{AB}\|}{h_i} - \frac{1}{h_i} \sum_{u=1}^U e^{j\phi^{(u)}} [\mathbf{w}^{(u)}]^T \mathbf{H}_{AB}^{(u)} \quad (9)$$

式(9)对应 4^U 个权系数 $\mathbf{w}$ 集合, 在解集合中搜寻最优峰均功率比的相位因子组合, 如式(10)所示:

$$\{\tilde{p}^{(1)}, \tilde{p}^{(2)}, \dots, \tilde{p}^{(U)}\} = \arg \min_{\{\tilde{p}^{(1)}, \tilde{p}^{(2)}, \dots, \tilde{p}^{(U)}\}} \left(\frac{\max_{1 \leq n \leq N} |\mathbf{w}(n)|^2}{\mathbb{E}[\|\mathbf{w}(n)\|^2]} \right) \quad (10)$$

为了减少式(10)的搜索复杂度, 本文提出了如下的迭代算法:

(1) 权系数 $\mathbf{w}(n)$, $n = 1, 2, \dots, i-1, i+1, \dots, N$ 分为 U 个不相交的权系数块 $\mathbf{w}^{(u)}$, $u = 1, 2, \dots, U$;

(2) 设置 $p^{(u)} = 1$, $u = 1, 2, \dots, U$, 采用式(8)和式(9)计算 PAPR, 并将这个值设为 PAPR_min。

(3) 设置 $u = 2$;

(4) 在 $p^{(u)} = -1, j, -j$ 的条件下, 分别计算 PAPR;

(5) 如果 $\text{PAPR} > \text{PAPR_min}$, 那么 $p^{(u)} = 1$; 否则, 更新 $\text{PAPR_min} = \text{PAPR}$;

(6) 如果 $u < U$, 那么 $u = u + 1$, 然后回到步骤(4); 否则, 得到最优的相位旋转因子 $\tilde{p}$ 。

通过上述的算法, 相位旋转因子搜索算法复杂度降低为 $3(U-1)$ 。相比于 4^U , 整个算法的复杂度由指数递增降低为线性递增。

4 仿真性能及其分析

仿真条件设置如下: (1)发射天线数分别设置为 $N=8, 16$, 对应不同的发射天线采用不同的分块数 U ; (2)发射天线对应的信道为相互独立的平坦衰落信号, 发射功率 P 归一化为 1;

图 3 给出了发射天线数 $N=8$, 分组数 $U=2, 4, 8$ 和发射天线数 $N=16$, 分组数 $U=4, 8, 16$ 时原算法和本文算法 PAPR 的互补累计函数曲线图。由图 3 可以看出: (1)对比子图 3(a)和图 3(b)本文算法相比较原算法在 $N=8, 16$ 和 $U=8, 16$ 的条件下分别提高了 2.00 dB 和 4.00 dB, 说明本文算法性能随着发射天线数的增加而提高; (2)当 $N=8$ 和 $U=2, 4, 8$ 时, 算法性能分别提高了 0.20 dB, 1.10 dB 和 2.00 dB, PAPR 抑制性能随着 U 的增加提高明显;

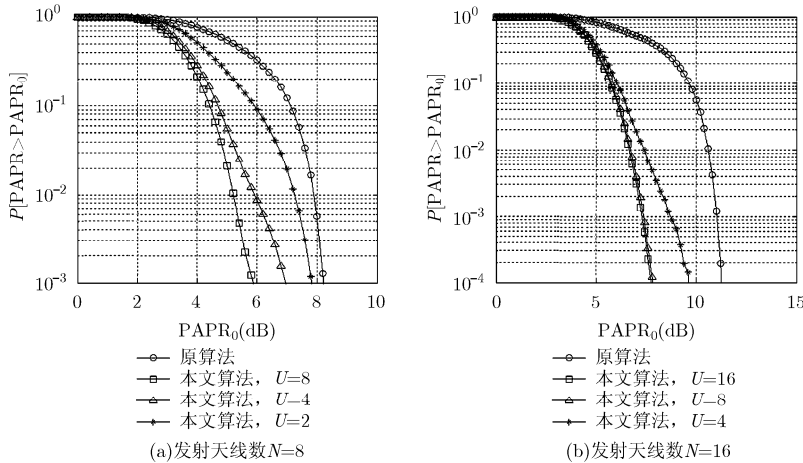


图 3 不同发射天线和分组数条件下峰均功率比互补累计分布函数曲线图

而 $N=16$ 和 $U=4, 8, 16$ 时, 算法性能分别提高了 2.00 dB, 3.95 dB 和 4.00 dB, 可以看出当分块数达到 8 时, 继续增加分块数对于 PAPR 抑制算法的性能提升很小, 说明本文算法并不需要过多的分组就能达到很好的性能。

图 4 给出了在发射天线数 $N=16$, 分组数 $U=16$ 和不同 PAPR 门限值条件下原算法和本文算法 Bob 误码性能的对比如。由图 4 可以看出: (1)原算法期望接收机 Bob 的误码性能随着 PAPR 门限的降低迅速恶化; 而对于本文算法影响很小, 误码性能曲线几乎重合。说明原算法中 PAPR 值较高的有用通信信息被门限值限幅削去, 而本文算法的 PAPR 值较小, 未被门限值限幅, 保留了有用的通信信息; (2)原算法和本文算法对于窃听接收机 Eve 的干扰性能相同, 窃听接收机都无法从接收信号中解调出有用的通信信息。说明本文算法抑制了发射信号的 PAPR 值的同时并没有影响基于随机天线阵的物理层安全通信系统的安全性能。

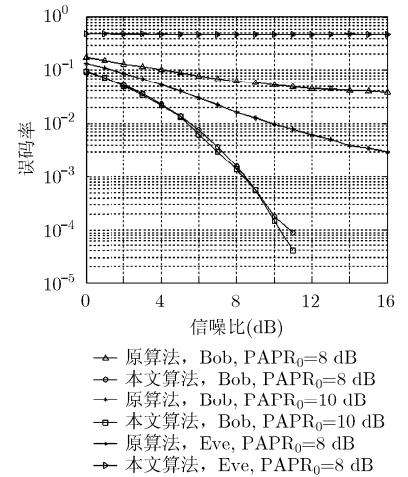


图 4 不同 PAPR 门限值条件下原算法和本文算法误码性能的对比如

5 结论

本文针对基于多天线加权发射的物理层安全通信系统发射信号高峰均功率比的缺点, 提出了一种基于部分传输序列的物理层安全通信信号峰均功率比抑制算法, 仿真结果表明本文算法在不影响整个物理层安全系统安全性能的条件下能够有效地抑制发射信号的峰均功率比值, 从而改善期望接收机的通信性能。本文的核心内容是阐述这种多天线加权发射的物理层安全通信系统类似于 OFDM 无线通信系统具有发射信号高峰均功率比的缺点, 需要一定的算法抑制发射信号的峰均功率比值。文中针对

基于随机天线阵的物理层安全通信系统, 初步提出了一种基于部分传输序列的峰均功率比抑制算法, 峰均功率比抑制性能更优的算法还需要进一步地讨论。

参考文献

- [1] Poor H V. Information and inference in the wireless physical layer[J]. *IEEE Wireless Communications*, 2012, 19(1): 40-47.
- [2] Harrison W K, Almeida J, Bloch M R, et al. Coding for secrecy: an overview of error-control coding techniques for physical-layer security[J]. *IEEE Signal Processing Magazine*, 2013, 30(5): 41-50.

- [3] 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.
- [4] 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.
- [5] Babakhani A, Rutledge D B, and Hajimiri A. Near-field direct antenna modulation[J]. *IEEE Microwave Magazine*, 2009, 10(1): 36–46.
- [6] Hong Y W P, Lan Pang-chang, and Kuo C C J. Enhancing physical-layer secrecy in multiantenna wireless systems: an overview of signal processing approaches[J]. *IEEE Signal Processing Magazine*, 2013, 30(5): 29–40.
- [7] Li Xiao-hua, Hwu J, and Ratazzi E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. *Journal of Communications*, 2007, 2(3): 24–32.
- [8] 穆鹏程, 殷勤业, 王文杰. 无线通信中使用随机天线阵列的物理层安全传输方法[J]. 西安交通大学学报, 2010, 44(6): 62–66.
Mu Peng-cheng, Yin Qin-ye, and Wang Wen-jie. A security method of physical layer transmission using random antenna arrays in wireless communication[J]. *Journal of Xi'an Jiao Tong University*, 2010, 44(6): 62–66.
- [9] 洪涛, 宋茂忠, 刘渝. 切换天线发射的低截获率通信信号物理层安全传输[J]. 应用科学学报, 2011, 29(4): 368–373.
Hong Tao, Song Mao-zhong, and Liu Yu. Signal transmitted from switched antenna array with low interception probability for physical layer security[J]. *Journal of Applied Sciences-Electronics and Information Engineering*, 2011, 29(4): 368–373.
- [10] Li Zheng and Xia Xiang-gen. A distributed differentially encoded OFDM scheme for asynchronous cooperative systems with low probability of interception[J]. *IEEE Transactions on Wireless Communications*, 2009, 8(7): 3372–3379.
- [11] Goel S and Negi R. Guaranteeing secrecy using artificial noise [J]. *IEEE Transactions on Wireless Communications*, 2008, 7(6): 2180–2189.
- [12] Liao Wei-cheng, Chang Tsung-hui, Ma Wing-kin, *et al.* QoS-based transmit beamforming in the presence of eavesdroppers: an optimized artificial-noise-aided approach [J]. *IEEE Transactions on Signal Processing*, 2011, 59(3): 1202–1216.
- [13] Zhou Xiang-yun and McKay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. *IEEE Transactions on Vehicular Technology*, 2008, 59(8): 2180–2189.
- [14] 吴飞龙, 王文杰, 王慧明, 等. 基于空域加扰的保密无线通信统一数学模型及其窃密方法[J]. 中国科学: 信息科学, 2012, 42(4): 483–492.
Wu Fei-long, Wang Wen-jie, Wang Hui-ming, *et al.* A unified mathematical model spatial scrambling based secure wireless communication and its wiretap method[J]. *SCIENCE CHINA Information Sciences*, 2012, 42(4): 483–492.

洪涛: 男, 1982年生, 讲师, 主要研究方向为多天线收发系统、物理层安全通信。

宋茂忠: 男, 1962年生, 教授, 博士生导师, 研究方向为调制信号设计与接收、多天线通信跟踪定位综合化技术、卫星导航。

王保云: 男, 1967年生, 教授, 博士生导师, 研究方向为信息论、物理层安全通信。