

DOI: 10.7652/xjtuxb201508006

一种全双工物理层安全通信波束成形的低功耗方法

叶夏^{1,2}, 朱丰超^{2,3}, 高飞飞²

(1. 温州医科大学计算机与信息管理系统, 325035, 浙江温州; 2. 清华大学自动化系, 100084, 北京;
3. 第二炮兵工程大学 403 教研室, 710025, 西安)

摘要: 在保证物理层安全的前提下,为解决传统迫零成形算法在全双工通信功耗过高的问题,提出了一种适用于全双工通信的信息波束和噪声波束联合成形的低功耗方法。首先,在高斯信道模型下对全双工基站的传输信号进行信息波束成形,实现基站与接收端的信息传输;然后,在全双工基站发射天线中添加人工噪声,并将噪声波束成形保证全双工基站的接收信息和发送信息不被偷听者窃听;最后,经过凸优化求解,将 NP 难的信息和噪声波束联合成形问题转化为可高效求解的凸优化问题,最终得到最优的信息和噪声波束成形向量。仿真结果表明,在上下行安全速率均为 3 b/(s·Hz) 时,该方法可以有效降低全双工基站的功耗,与经典的迫零波束成形算法相比,均值功耗降低约 18%。

关键词: 物理层安全;全双工通信;波束成形;凸优化

中图分类号: TN929.5 **文献标志码:** A **文章编号:** 0253-987X(2015)08-0031-07

A Beam Forming Method for Secure Communications of Full Duplex Physical Layer

YE Xia^{1,2}, ZHU Fengchao^{2,3}, GAO Feifei²

(1. Department of Computer Science & Information Management, Wenzhou Medical University, Wenzhou, Zhejiang 325035, China; 2. Department of Automation, Tsinghua University, Beijing 100084, China;
3. Staff Room 403, The Second Artillery Engineering University, Xi'an 710025, China)

Abstract: A joint beamforming method of information and noise is proposed to reduce the power consumption of conventional zero-forcing beamforming method for full duplex secure communication systems. An information beamforming vector is designed for down-link communication of a full-duplex base-station (FD-BS) in a Gaussian channel model, and a noise beamforming vector is designed to jam the eavesdropper and to protect the information of both uplink and downlink for FD-BS. Then the joint beamforming problem, that is NP hard, is converted to a convex optimization problem which can be efficiently solved, and the optimal information beamforming vector and noise beamforming vector are derived from the optimal solutions. Simulation results show that when both the uplink and the downlink secret rates are set to 3 b/(s·Hz), the proposed algorithm effectively reduces the power consumption of FD-BS. A comparison with the conventional zero-forcing beamforming method show that the power saved by the proposed algorithm is 18%.

Keywords: physical layer security; full duplex communications; beamforming; convex optimization

收稿日期: 2015-01-13。 作者简介: 叶夏(1979—),男,讲师;高飞飞(通信作者),男,副教授,博士生导师。 基金项目: 国家自然科学基金资助项目(61201187);浙江省教育厅科研基金资助项目(Y201121579);浙江省教育厅国内访问学者专业发展课题资助项目(FX2014052)。

网络出版时间: 2015-05-15 网络出版地址: <http://www.cnki.net/kcms/detail/61.1069.T.20150515.1747.005.html>

由于无线信道的开放性,无线通信易受攻击和窃听。随着无线网络在信息领域应用规模的不断扩大,越来越多的入侵者试图通过物理层截获关键信息。因此,确保无线信息的安全,是无线通信技术在军事、金融、医疗、信息系统领域等各方面广泛应用的关键问题^[1]。随着计算机技术的飞速发展,传统通过数据加密、解密来保证信息安全的方法已不能完全胜任。由于物理层安全通信主要是利用信道的自身特性来实现信息的安全传输^[2],因而物理层安全方法可以与其他安全通信方法(例如直接序列扩频技术^[3])很好地兼容。近年来,多种物理层安全通信技术得到了快速的发展,其中文献[4]提出了一种利用噪声来提高安全速率的方法,与雷达通信中的干扰源^[5-6]不同,该方法中的噪声干扰是由发射端自身设计并发送的。物理层安全技术具有重要的现实意义和研究价值,但是,以文献[1-6]为例的物理层安全通信的研究都是基于传统的半双工通信模型,频谱效率仅为全双工模型的50%,并且由于全双工系统的信息安全涉及上下行信息的安全,传统半双工系统中的物理层安全技术在全双工系统中的应用并不能有效实现。

全双工无线通信目前为我国5G通信系统充分挖掘无线频谱资源的一个重要方向。近年来,随着器件技术和信号处理技术的发展,全双工无线通信设备中的自干扰消除技术有了深入的理论研究和系统实验。文献[7]方法结合物理隔离与时频域重构等技术,大幅度提高了自干扰消除效果,其剩余自干扰被压制在很低的噪声水平上;文献[8]和文献[9]的最新研究结果表明,斯坦福大学研究团队设计的全双工通信系统(单天线或者多天线)可以完全消除自干扰。但是,文献[7-9]中均未涉及系统的安全问题的讨论,存在信息安全方面的不足。

目前对全双工系统的安全机制的研究并不全面,文献[10-11]中在全双工自干扰能被完全消除的假设下,分别提出了一种利用全双工终端来提高通信系统接收信息的物理层安全方法,然而二者均只考虑全双工基站的信息接收方向的安全策略,而没有考虑全双工基站的信息发送的安全,这给信号窃听者提供了机会。因此,文献[10-11]中的物理层安全通信方法有待进一步提高。另外,虽然传统的迫零波束成形算法可以较容易地应用于全双工物理层安全通信系统中,但是该方法没有充分利用信号的空间自由度,因而存在功耗过高的缺点。

针对以上问题,本文提出了一种信息波束成形

和噪声波束成形的联合优化方法。该方法与传统的迫零波束成形方法相比充分利用了全双工基站的天线自由度,在整个信道空间对波束成形向量进行优化,因而可充分降低全双工基站的功耗。另一方面,本文方法克服了文献[10-11]中方法的缺点,即可实现全双工基站上下行信息安全速率的优化,可同时保证全双工基站上、下行通信的信息安全。

1 总体模型

在高斯信道模型假设下,本文研究的全双工通信系统包括一个全双工基站(full-duplex base station),一个信息发送端(transmitter),一个信息接收端(receiver),以及一个窃听端(eavesdropper)。全双工基站具有 M 根接收天线和 N 根发射天线,其余终端均只有单个天线。发射端到窃听端和全双工基站的信道分别为 $g_e \in \mathbb{C}^{1 \times 1}$ 和 $h_t \in \mathbb{C}^{M \times 1}$;全双工基站到接收端和窃听端的信道分别为 $h_r \in \mathbb{C}^{N \times 1}$ 和 $h_e \in \mathbb{C}^{N \times 1}$;全双工基站自干扰信道为 $H_b \in \mathbb{C}^{N \times M}$ 。假设全双工基站的自干扰被完全消除^[7-11],可以得到 $H_b = \mathbf{0}$ 。全双工通信模型如图1所示。

全双工基站利用发送同频随机噪声的方式^[5]来确保全双工通信系统的物理层安全。假设 q_b 为全双工基站待发送的信息符号,服从 $\text{CN}(0,1)$ 随机分布, q_e 为全双工基站待发送的噪声符号,服从 $\text{CN}(0,1)$ 随机分布,则全双工基站的基带发射信号可以表示为

$$\mathbf{x}_b = s q_b + w q_e \quad (1)$$

式中: $s \in \mathbb{C}^{N \times 1}$ 为信息波束成形向量; $w \in \mathbb{C}^{N \times 1}$ 为噪声波束成形向量,两者均为需要设计的参数。

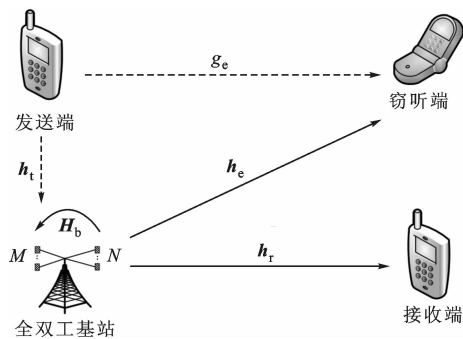


图1 全双工通信模型

假设 $q_t \sim \text{CN}(0,1)$ 为发射端待发送符号, P_t 为发射端的发射功率,则全双工基站接收到的信号为

$$\mathbf{y}_b = \mathbf{h}_t P_t^{1/2} q_t + \mathbf{z}_b \quad (2)$$

式中: $\mathbf{z}_b \sim \text{CN}(\mathbf{0}, \mathbf{I})$ 为全双工基站接收天线噪声。接收端和窃听端接收到的信号分别为

$$\mathbf{y}_r = \mathbf{h}_r^H \mathbf{x}_b + \mathbf{z}_r \quad (3)$$

$$y_e = g_e P_t^{1/2} q_t + \mathbf{h}_e^H \mathbf{x}_b + z_e \quad (4)$$

式中: $z_r \sim \text{CN}(0, 1)$ 和 $z_e \sim \text{CN}(0, 1)$ 分别为接收端和窃听端的接收天线噪声。

由物理层安全理论^[4]可知,为了保证全双工基站上下行信息的安全,必须使得上下行信息的安全速率大于0。发射端到全双工基站的安全速率 R_b 和全双工基站到接收端的安全速率 R_r 分别定义为^[4]

$$R_b = C_b - C_{b,e}; \quad R_r = C_r - C_{r,e} \quad (5)$$

式中

$$C_b = \log(1 + P_t \|\mathbf{h}_t\|^2) \quad (6)$$

$$C_{b,e} = \log\left(1 + \frac{P_t \|\mathbf{g}_e\|^2}{1 + \mathbf{s}^H \mathbf{H}_e \mathbf{s} + \mathbf{w}^H \mathbf{H}_e \mathbf{w}}\right) \quad (7)$$

$$C_r = \log\left(1 + \frac{\mathbf{s}^H \mathbf{H}_r \mathbf{s}}{1 + \mathbf{w}^H \mathbf{H}_r \mathbf{w}}\right) \quad (8)$$

$$C_{r,e} = \log\left(1 + \frac{\mathbf{s}^H \mathbf{H}_e \mathbf{s}}{1 + P_t \|\mathbf{g}_e\|^2 + \mathbf{w}^H \mathbf{H}_e \mathbf{w}}\right) \quad (9)$$

式中: $\mathbf{H}_r = \mathbf{h}_r \mathbf{h}_r^H$; $\mathbf{H}_e = \mathbf{h}_e \mathbf{h}_e^H$ 。

安全速率 R_b 和 R_r 的意义在于:当 $R_b > 1$ 且 $R_r > 0$ 时,全双工基站的上下行通信链路可以安全地收发信息,并保证窃听端无法破译全双工基站的收发信息,从而实现了全双工基站的物理层安全通信。在实际全双工系统设计时需要尽量提高 R_b 和 R_r ,即提高全双工基站的上下行通信的吞吐量,同时为了节省全双工基站的耗费,需要尽量降低全双工基站的发射功率。为了实现上述目标,设计优化问题为

$$\begin{aligned} & \min_{\mathbf{s}, \mathbf{w}} (\|\mathbf{s}\|^2 + \|\mathbf{w}\|^2) \\ & \text{s. t. } C_b - C_{b,e} \geq \gamma_t; \quad C_r - C_{r,e} \geq \gamma_r \end{aligned} \quad (10)$$

式中: γ_t 、 γ_r 分别为发射端和接收端的信干噪比阈值。全双工基站可以根据实际通信的需要选择不同的 γ_t 和 γ_r 来满足其上下行信息的传输需求,而 $\mathbf{s}$ 和 $\mathbf{w}$ 则是需要求解的波束成形向量。相较于传统的迫零波束成形方法,本文的物理层安全设计方法没有对 $\mathbf{s}$ 和 $\mathbf{w}$ 的选取进行额外限制,即 $\mathbf{s}$ 和 $\mathbf{w}$ 在满足安全速率阈值条件下可在整个信号空间自由选择,因而本文方法可充分利用全双工基站的自由度,从而以最低的功耗达到信息安全的目的。波束成形向量 $\mathbf{s}$ 和 $\mathbf{w}$ 的自由度的增加也使得优化设计式(10)变得更加复杂,并且式(10)是一个全新的优化问题,传统的优化方法对本文式(10)不再适用,因而需要对优化式(10)进行深入的分析,进而得到最优的波束成形向量 $\mathbf{s}$ 和 $\mathbf{w}$ 。

2 问题求解

在上文的解决方法中,设计优化问题式(10)是

一个复杂的非凸问题^[12],其主要难点在于式(10)的限制条件为非凸函数,这使得该方法缺乏实现基础,因而下文需要证明将问题式(10)等价转化为非凸问题求解的同时,依然能够保持 $\text{rank}(\mathbf{S}^*) = 1$ 和 $\text{rank}(\mathbf{W}^*) = 1$ 的前提条件。

2.1 问题等价转化

为将问题式(10)转化为凸问题,本文首先引入辅助变量 $R(0 \leq R \leq \gamma_r)$, R 是一个安全速度常数,通过不同的 R 可将问题式(10)等价转化为

$$\begin{aligned} & \min_{0 \leq R \leq \gamma_r} \min_{\mathbf{s}, \mathbf{w}} (\|\mathbf{s}\|^2 + \|\mathbf{w}\|^2) \\ & \text{s. t. } C_b - C_{b,e} \geq \gamma_t; \quad C_r \geq R; \quad C_{r,e} \leq \gamma_r - R \end{aligned} \quad (11)$$

然后可以通过对 R 进行一维搜索的方式来求解式(11)。一维搜索法具有计算速度快的优点,其复杂度是被各种物理层安全算法普遍接受的。假设 R 已知,每一次搜索中需要求解的子问题为

$$\min_{\mathbf{S} \geq 0, \mathbf{W} \geq 0} \text{tr}(\mathbf{S}) + \text{tr}(\mathbf{W}) \quad (12)$$

$$\text{s. t. } \text{tr}(\mathbf{H}_e \mathbf{S}) + \text{tr}(\mathbf{H}_e \mathbf{W}) \geq \xi \quad (13)$$

$$\text{tr}(\mathbf{H}_r \mathbf{S}) - (2^R - 1) \text{tr}(\mathbf{H}_r \mathbf{W}) \geq 2^R - 1 \quad (14)$$

$$\text{tr}(\mathbf{H}_e \mathbf{S}) - (2^{\gamma_r - R} - 1) \text{tr}(\mathbf{H}_e \mathbf{W}) \leq \xi_1 \quad (15)$$

$$\text{rank}(\mathbf{S}) = 1; \quad \text{rank}(\mathbf{W}) = 1 \quad (16)$$

式中: $\mathbf{S} = \mathbf{s} \mathbf{s}^H$; $\mathbf{W} = \mathbf{w} \mathbf{w}^H$;

$$\xi = \frac{2^{\gamma_t} P_t \|\mathbf{g}_e\|^2 + 2^{\gamma_t} - P_t \|\mathbf{h}_t\|^2 - 1}{1 + P_t \|\mathbf{h}_t\|^2 - 2^{\gamma_t}} \quad (17)$$

$$\xi_1 = (2^{\gamma_r - R} - 1)(1 + P_t \|\mathbf{g}_e\|^2) \quad (18)$$

上述子问题(式(12)~(16))的目标函数(式(12))和限制条件(式(13)~(15))均满足凸函数的条件,然而限制条件式(16)为非凸函数。限制条件式(16)的作用是保证得到 $\mathbf{S}$ 和 $\mathbf{W}$ 后,可以通过奇异值分解获得波束成形向量 $\mathbf{s}$ 和 $\mathbf{w}$ 。求解含有限制条件式(16)的非凸优化问题,可采用半定松弛(semi-definite relaxation, SDR)技术^[13]将问题进行转化。SDR 技术实际上是通过忽视限制条件式(16)的影响,直接求解式(12)~式(15)中的问题。利用 SDR 技术可以将非凸的问题转化为凸优化问题,然而得到的解并不是原问题的最优解,但本文问题具有特殊性,式(12)~式(15)中的最优解经证明仍满足式(16)的限制,即式(12)~式(15)中的问题的最优解等效于原问题式(11)的最优解。

2.2 SDR 的最优性分析

根据凸优化理论^[11],凸优化问题的最优解和其对应的对偶问题的最优解是相同的。因此要分析 SDR 的最优性通常需要分析原问题的对偶问题。通过分析

对偶问题的最优解的形式,可以判断原问题的最优解是否满足类似式(16)的限制。若满足,则表明SDR是可以得到原问题的最优解的。因此,要得到原问题的最优解,进行SDR的最优性分析是一种行之有效的办法。

在式(12)~式(16)中,忽略限制条件式(16),可以将子问题转化为一组半定规划(semi-definite programming, SDP)问题(即式(12)~式(15)中的问题)。SDP问题为凸优化问题,该问题关于优化变量 $\mathbf{S}$ 和 $\mathbf{W}$ 的Karush-Kuhn-Tucker(KKT)条件^[11]为

$$\mathbf{\Sigma}_S^* = \mathbf{I} - \alpha^* \mathbf{H}_e - \beta^* \mathbf{H}_r + \lambda^* \mathbf{H}_e \quad (19)$$

$$\mathbf{\Sigma}_W^* = \mathbf{I} - \alpha^* \mathbf{H}_e + \beta^* (2^R - 1) \mathbf{H}_r - \lambda^* (2^{\gamma_r - R} - 1) \mathbf{H}_e \quad (20)$$

$$\mathbf{\Sigma}_S^* \mathbf{S}^* = \mathbf{0}, \quad \mathbf{\Sigma}_W^* \mathbf{W}^* = \mathbf{0} \quad (21)$$

式中: $\alpha^* \geq 0, \beta^* \geq 0, \lambda^* \geq 0$ 为最优的拉格朗日系数。

此时,如果可以证明KKT条件中的 $\mathbf{S}^*$ 和 $\mathbf{W}^*$ 满足 $\text{rank}(\mathbf{S}^*)=1, \text{rank}(\mathbf{W}^*)=1$,那就可以直接求解半定松弛后的子问题式(12)~式(16)(凸优化问题),然后可以通过奇异值分解很容易地获得最优的 $\mathbf{s}^*$ 和 $\mathbf{w}^*$ 。为了证明半定松弛的最优性,下面证明经过半定松弛的子问题式(12)~式(16)的最优解满足 $\text{rank}(\mathbf{S}^*)=1, \text{rank}(\mathbf{W}^*)=1$ 。

在式(19)中,因为 $R \geq 0, \beta^* \geq 0, \mathbf{H}_r = \mathbf{h}_r \mathbf{h}_r^H \geq \mathbf{0}$,所以 $\mathbf{I} + \beta^* (2^R - 1) \mathbf{H}_r$ 是满秩的,即 $\text{rank}(\mathbf{I} + \beta^* (2^R - 1) \mathbf{H}_r) = N$ 。同时,在式(9)中,又因为 $\mathbf{H}_e = \mathbf{h}_e \mathbf{h}_e^H$,所以可得到 $\text{rank}(\alpha^* \mathbf{H}_e + \lambda^* (2^{\gamma_r - R} - 1) \mathbf{H}_e) \leq 1$ 。综合以上讨论,在式(20)中,可以得到 $\text{rank}(\mathbf{\Sigma}_W^*) \geq N - 1$ 。又因为式(21)中有 $\mathbf{\Sigma}_W^* \mathbf{W}^* = \mathbf{0}$ 成立,所以 $\text{rank}(\mathbf{\Sigma}_W^*) + \text{rank}(\mathbf{W}^*) \leq N$ 成立。由此,可以得到结论 $\text{rank}(\mathbf{W}^*) \leq 1$ 。

与上面的讨论类似,由式(19)首先可以得到 $\text{rank}(\alpha^* \mathbf{H}_e + \beta^* \mathbf{H}_r) \leq 2$,进而可以得到 $\text{rank}(\mathbf{\Sigma}_S^*) \geq N - 2$ 。式(20)中由于 $\mathbf{\Sigma}_S^* \mathbf{S}^* = \mathbf{0}$,所以 $\text{rank}(\mathbf{\Sigma}_S^*) + \text{rank}(\mathbf{S}^*) \leq N$ 成立。因此可以得到结论: $\text{rank}(\mathbf{S}^*) \leq 2$ 。

下面讨论 $\text{rank}(\mathbf{S}^*)=2$ 的情况。证明思路为根据原问题的KKT条件分析最优解的形式,然后构造一组等价的最优解满足式(16)的限制。

(1)首先讨论在 $\text{rank}(\mathbf{S}^*)=2$ 时最优解的形式。在式(16)中可以得到

$$\text{rank}(\mathbf{I} + \lambda^* \mathbf{H}_e - \alpha^* \mathbf{H}_e) = N - 1 \quad (22)$$

$$\text{rank}(\mathbf{I} + \lambda^* \mathbf{H}_e - \beta^* \mathbf{H}_r) = N - 1 \quad (23)$$

并且 $\alpha^* > 0, \beta^* > 0$ 成立。在此前提下, $\text{rank}(\mathbf{S}^*) =$

2可以成立。下面将证明此时方法仍能够保持结果的最优化。

令 $\pi_1 \in \mathbb{C}^{N \times 1}$ 为 $\mathbf{I} + \lambda^* \mathbf{H}_e - \alpha^* \mathbf{H}_e$ 的零空间的基, π_1 平行于 $\mathbf{h}_e$ 。将 $\mathbf{\Sigma}_S^*$ 左乘 π_1^H 并且右乘 π_1 ,得到

$$\pi_1^H \mathbf{\Sigma}_S^* \pi_1 = -\pi_1^H \mathbf{H}_r \pi_1 \quad (24)$$

由于 $\mathbf{\Sigma}_S^* \geq \mathbf{0}, \mathbf{H}_r \geq \mathbf{0}$,在式(24)中,可以得到 $\pi_1^H \mathbf{\Sigma}_S^* \pi_1 \geq 0, -\pi_1^H \mathbf{H}_r \pi_1 \leq 0$ 。所以,式(24)中可推出

$$\pi_1^H \mathbf{\Sigma}_S^* \pi_1 = \pi_1^H \mathbf{H}_r \pi_1 = 0 \quad (25)$$

即 π_1 为 $\mathbf{\Sigma}_S^*$ 的零空间的一个基,且 $\mathbf{h}_r^H \pi_1 = 0$ 。

令 $\pi_2 \in \mathbb{C}^{N \times 1}$ 为 $\mathbf{\Sigma}_S^*$ 的零空间的另一个基,且满足 $\pi_1^H \pi_2 = 0, \mathbf{h}_e^H \pi_2 = 0$,并且,由于式(10)中 $\mathbf{\Sigma}_S^* \mathbf{S}^* = \mathbf{0}, \mathbf{S}^*$ 可以表达为

$$\mathbf{S}^* = T_1 \pi_1 \pi_1^H + T_2 \pi_2 \pi_2^H + T_3 \pi_1 \pi_2^H + \bar{T}_3 \pi_2 \pi_1^H \quad (26)$$

式中: $T_1, T_2, T_3, \bar{T}_3$ 为系数。

将 $\mathbf{\Sigma}_W^*$ 左乘 π_1^H 并且右乘 π_1 ,可以得到

$$\pi_1^H \mathbf{\Sigma}_W^* \pi_1 = \pi_1^H (\mathbf{\Sigma}_S^* + \beta^* 2^R \mathbf{H}_r - \lambda^* 2^{\gamma_r - R} \mathbf{H}_e) \pi_1 = -\pi_1^H \lambda^* 2^{\gamma_r - R} \mathbf{H}_e \pi_1 \quad (27)$$

与式(23)的推导类似,可以得到

$$\pi_1^H \mathbf{\Sigma}_W^* \pi_1 = -\pi_1^H \lambda^* 2^{\gamma_r - R} \mathbf{H}_e \pi_1 = 0 \quad (28)$$

即 π_1 为 $\mathbf{\Sigma}_W^*$ 的零空间的基,并且由于式(21)中 $\mathbf{\Sigma}_W^* \mathbf{W}^* = \mathbf{0}, \mathbf{W}^*$ 可以表达为

$$\mathbf{W}^* = T_4 \pi_1 \pi_1^H \quad (29)$$

式中: T_4 为系数。将式(26)~式(29)代入式(12)~式(15),并且利用性质 $\mathbf{h}_r^H \pi_1 = 0$ 以及 $\mathbf{h}_e^H \pi_2 = 0$,可以得到:式(26)中因子 $T_3 \pi_1 \pi_2^H + \bar{T}_3 \pi_2 \pi_1^H$ 不影响限制条件式(13)~式(15),但是会使得目标函数式(12)增大。因此,为了获得最小的目标函数,在最优条件下, $T_3 \pi_1 \pi_2^H + \bar{T}_3 \pi_2 \pi_1^H = \mathbf{0}$ 成立。所以,式(26)需要重新写为

$$\mathbf{S}^* = T_1 \pi_1 \pi_1^H + \bar{T}_2 \pi_2 \pi_2^H \quad (30)$$

通过以上对SDR问题的KKT条件的分析得出,设计的信息传输矩阵表达式(30)依然不满足式(16)的限制。

(2)在 $\text{rank}(\mathbf{S}^*)=2$ 时构造一组等价的最优解。假设存在一组解 $\bar{\mathbf{S}}^*$ 和 $\bar{\mathbf{W}}^*$,满足

$$\bar{\mathbf{S}}^* = T_2 \pi_2 \pi_2^H; \quad \bar{\mathbf{W}}^* = (T_1 + T_4) \pi_1 \pi_1^H \quad (31)$$

并满足 $\text{rank}(\bar{\mathbf{S}}^*)=1$ 和 $\text{rank}(\bar{\mathbf{W}}^*)=1$ 。将式(30)代入式(12)~式(15),利用性质 $\mathbf{h}_r^H \pi_1 = 0$ 以及 $\mathbf{h}_e^H \pi_2 = 0$,可以得到: $\bar{\mathbf{S}}^*$ 和 $\bar{\mathbf{W}}^*$ 不影响式(12)~式(15)的目标函数值,但可以提高子问题的限制条件式(15)的自由度。

综上,在最优条件下, $\bar{\mathbf{S}}^*, \bar{\mathbf{W}}^*$ 更优于 $\mathbf{S}^*, \mathbf{W}^*$ 。因此, $\bar{\mathbf{S}}^*, \bar{\mathbf{W}}^*$ 为式(11)子问题的最优解,并且满足

$\text{rank}(\mathbf{S}^*)=1$ 和 $\text{rank}(\mathbf{W}^*)=1$ 。

本节通过 SDR 问题的 KKT 条件分析了最优解的形式。通过构造满足式(14)约束的最优解证明了 SDR 的最优性,即利用半定松弛技术可以得到式(12)~式(16)最优解的结果。

2.3 问题最优解分析

通过前面的分析可知:本文需要求解的优化问题可以通过一维搜索算法获得,而每一次搜索求解的问题等价于凸优化问题。对于凸优化问题可以通过 Matlab 中的凸优化工具箱快速求解。

3 迫零波束成形

迫零波束成形算法^[14]为一种经典的低复杂度算法,其基本思想是限制波束成形的空间自由度,从而降低波束成形参数的设计难度^[15-16]。也正是因为迫零波束成形算法没有充分利用信号的空间分布特性,所以该算法需要消耗更多的能量。

本文采用的迫零波束成形算法的主要思路是让信息波束垂直于非法偷听者的信道,并让噪声波束垂直于合法接收端的信道。令式(10)中的 $\mathbf{s}$ 垂直于 $\mathbf{h}_e$, $\mathbf{w}$ 垂直于 $\mathbf{h}_r$, 即

$$\mathbf{h}_e^H \mathbf{s} = 0; \mathbf{h}_r^H \mathbf{w} = 0 \quad (32)$$

首先对 $\mathbf{H}_e$ 进行奇异值分解,可以得到 $\mathbf{H}_e$ 的零空间矩阵 $\mathbf{U}_e \in \mathbb{C}^{N \times (N-1)}$ 。同时,考虑到 $\mathbf{s}$ 向量的方向应该尽量与 $\mathbf{h}_r$ 一致,可以得到 $\mathbf{s}$ 的方向向量为

$$\mathbf{s}' = \mathbf{U}_e \mathbf{U}_e^H \mathbf{h}_r / \|\mathbf{U}_e^H \mathbf{h}_r\| \quad (33)$$

其次,对 $\mathbf{H}_r$ 进行奇异值分解,可以得到 $\mathbf{H}_r$ 的零空间矩阵 $\mathbf{U}_r \in \mathbb{C}^{N \times (N-1)}$ 。同时,考虑到 $\mathbf{w}$ 向量的方向应该尽量与 $\mathbf{h}_e$ 一致,可以得到 $\mathbf{w}$ 的方向向量为

$$\mathbf{w}' = \mathbf{U}_r \mathbf{U}_r^H \mathbf{h}_e / \|\mathbf{U}_r^H \mathbf{h}_e\| \quad (34)$$

假设 FD-BS 用于信息波束成形和噪声波束成形的能量分别为 P_s 和 P_w ,将式(33)和式(34)代入式(10)中,并利用式(32)可以得到迫零波束成形向量分别为

$$\mathbf{s}^* = P_s^{1/2} \mathbf{U}_e \mathbf{U}_e^H \mathbf{h}_r / \|\mathbf{U}_e^H \mathbf{h}_r\| \quad (35)$$

$$\mathbf{w}^* = P_w^{1/2} \mathbf{U}_r \mathbf{U}_r^H \mathbf{h}_e / \|\mathbf{U}_r^H \mathbf{h}_e\| \quad (36)$$

式中

$$P_s = \frac{2^{\gamma_r} - 1}{\|\mathbf{U}_e^H \mathbf{h}_r\|^2} \quad (37)$$

$$P_w = \frac{2^{\gamma_r} P_t \|\mathbf{g}_e\|^2 + 2^{\gamma_r} - P_t \|\mathbf{h}_t\|^2 - 1}{(1 + P_t \|\mathbf{h}_t\|^2 - 2^{\gamma_r}) \|\mathbf{U}_r^H \mathbf{h}_e\|^2} \quad (38)$$

由以上公式可以得出:迫零波束成形算法可以得到问题的闭值解,因而当信道参数已知时,通过简单计算就可以得到迫零波束成形算法的具体参数。

4 仿真实验

为了检验信息波束成形和噪声波束成形的联合优化方法与迫零波束成形算法的功耗差异,本节内容设置了3组仿真实验。设置全双工基站的发射天线数和接收天线数分别为 $M=N=4$ 。所有信道均经过 10 000 次蒙特卡洛仿真获得。同时为了确保原问题存在可行解(请参考式(10)的限制条件),在选取 γ_t 时满足 $\gamma_t \leq \text{lb}(1 + P_t \|\mathbf{h}_t\|^2)$ 。

首先对比在不同发射端发射功耗情况下本文算法的性能,其中最小的安全速率阈值条件分别设置为 $\gamma_t = \gamma_r = 3 \text{ b}/(\text{s} \cdot \text{Hz})$ 。图2给出不同发射端发射功率下,2种算法的基站功耗比较。可以看到,随着 P_t 的增加,本文所提出的最优波束成形和迫零波束成形算法所需功耗均变化不大。这是因为考虑的是问题(10)存在可行解的情况,即所选择的 γ_t 满足 $\gamma_t \leq \text{lb}(1 + P_t \|\mathbf{h}_t\|^2)$ 。最优波束成形所需功耗在 2.55 dB 左右,而迫零波束成形算法所需功耗在 3 dB 左右。迫零波束成形算法的功耗高于最优解 0.45 dB,即本文方法可降低约 18% 的功耗值。

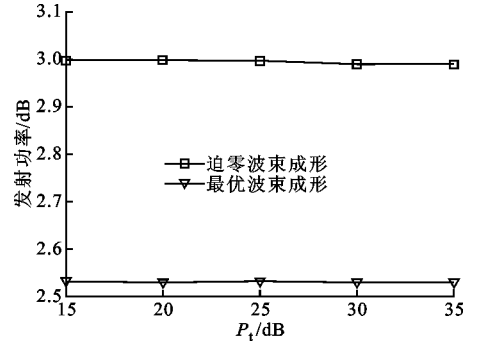


图2 2种算法的全双工基站功率比较

其次,对比在不同安全速率阈值条件下本文算法的性能,其中设置 $P_t = 25 \text{ dB}$ 。同时,为了保证全双工基站上下行安全速率的均衡,设置 $\gamma_t = \gamma_r$ 。在图3中,可以看出迫零波束成形算法和最优波束成形算法的功耗均随着阈值的增加而增大。这主要是因为随着 γ_r 的增加,全双工基站需要更大的功率来满足下行安全速率的限制条件。可以看到,迫零波束成形算法和最优波束成形算法的功耗差异趋于一个常数 0.45 dB。当阈值较大时,全双工基站所需功耗也较大,迫零波束成形与最优波束成形的功耗差异可以忽略不计。此时,迫零波束成形算法可以获得较好的效果。

最后,给出在不同安全速率阈值的情况下式

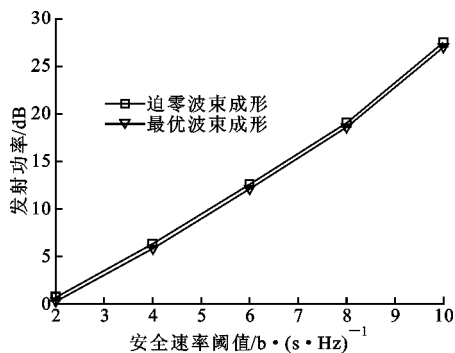


图3 不同安全速率阈值条件下2种算法的全双工基站功率比较

(10)存在可行解的概率,其中,设置 $P_t = 25$ dB, $\gamma_t = \gamma_r = 3$ b/(s · Hz)。由于全双工基站接收到的信号强度取决于发射端的发射能量,因此当全双工基站接收信息的安全速率阈值 γ_t 过大就会导致原设计问题不可解。讨论原问题的可行解随 γ_t 的变化,可以为安全速率阈值 γ_t 的选取提供参考。可行解存在概率随安全速率阈值的变化如图4所示。从图4中可以看出,当 $\gamma_t = \gamma_r \leq 8$ b/(s · Hz)时,式(10)存在可行解的概率趋近于1,而当 $\gamma_t = \gamma_r > 8$ b/(s · Hz)时,式(10)存在可行解的概率随着阈值的增大而减小,此时,在某些信道增益下,无论全双工基站消耗多大的能量都不可能满足接收端的安全接收速率的要求(请参看式(10))。尤其是当 $8 < \gamma_t = \gamma_r < 12$ b/(s · Hz)时,式(10)存在可行解的概率迅速降低。当 $\gamma_t = \gamma_r > 12$ b/(s · Hz)时,可以看出式(10)存在可行解的概率逐渐趋近于0。因此,最合适的安全速率阈值 γ_t 的范围应该为 $0 \leq \gamma_t \leq 8$ b/(s · Hz)。

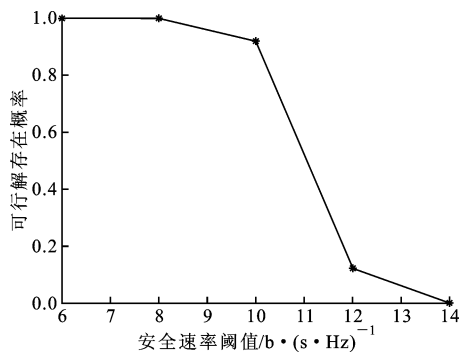


图4 可行解存在概率随 γ_t 的变化

5 结论

本文在保证全双工通信上下行信息窃听安全的基础上,提出了一种信息波束成形和噪声波束成形的联合优化算法。首先在全双工基站发射天线设计

信息波束成形向量和噪声波束成形向量以提高上下行通信的安全速率;其次对全双工基站的功耗进行了优化。该方法与传统的迫零波束成形算法相比可以为全双工基站节省更多的功耗。仿真结果表明,在全双工基站上下行安全速率均为 3 b/(s · Hz)时,两种算法的功耗差值为 0.45 dB。

参考文献:

- [1] 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 Pengcheng, YIN Qinye, WANG Wenjie. A security method of physical layer transmission using random antenna arrays in wireless communication [J]. Journal of Xi'an Jiaotong University, 2010, 44(6): 62-66.
- [2] WYNER A D. The wire-tap channel [J]. Bell System Technical Journal, 1975, 54: 1355-1387.
- [3] 尚佳栋,王祖林,周丽娜,等. 采用随机共振增强的混合扩频信号调频参数估计[J]. 西安交通大学学报, 2014, 48(10): 42-48.
SHANG Jiadong, WANG Zulin, ZHOU Lina, et al. An estimation method of frequency hopping parameters for hybrid spread spectrum signals using stochastic resonance enhanced strategy [J]. Journal of Xi'an Jiaotong University, 2014, 48(10): 42-48.
- [4] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.
- [5] 杨晓超,刘宏伟,王勇,等. 利用多输入多输出雷达低秩杂波的降维空时自适应算法[J]. 西安交通大学学报, 2012, 46(8): 76-81.
YANG Xiaochao, LIU Hongwei, WANG Yong, et al. A new reduced dimensional space-time adaptive processing algorithm exploiting low-rank clutter for multiple-input multiple-output radar [J]. Journal of Xi'an Jiaotong University, 2012, 46(8): 76-81.
- [6] 石娟,邓科,殷勤业. 一种适合任意流型的相干信号波达方向估计算法[J]. 西安交通大学学报, 2009, 43(6): 72-75, 98.
SHI Juan, DENG Ke, YIN Qinye. A method for estimating the direction of arrival of coherent signals on arbitrary antenna array in multi-path scenarios [J]. Journal of Xi'an Jiaotong University, 2009, 43(6): 72-75, 98.
- [7] RIIHONEN T, WERNNER S, WICHMAN R. Mitigation of loopback self-interference in full-duplex MI-

- MO relays [J]. IEEE Transactions on Signal Processing, 2011, 59(12): 5983-5993.
- [8] BHARADIA D, MCMILIN E, KATTI S. Full duplex radios [C]//Proceedings of the ACM Special Interest Group on Data Communication. New York, USA: ACM, 2013: 375-386.
- [9] BHARADIA D, KATTI S. Full duplex MIMO radios [C]//Proceedings of the 11th Systems Administration Conference on Networked Systems Design and Implementation. New York, USA: ACM, 2014: 359-372.
- [10] LI W, GHOGHO M, CHEN B, et al. Secure communication via sending artificial noise by the receiver: outage secrecy capacity/region analysis [J]. IEEE Communications Letters, 2012, 16(10): 1628-1631.
- [11] ZHOU Y, XIANG Z Z, ZHU Y, et al. Application of full-duplex wireless technique into secure MIMO communication: achievable secrecy rate based optimization [J]. IEEE Signal Processing Letters, 2014, 21(7): 804-808.
- [12] BOYD S, VANDENBERGHE L. Convex optimization [M]. Cambridge, UK: Cambridge University Press, 2004: 265-271.
- [13] LUO Z Q, MA W K, SO A M C, et al. Semidefinite relaxation of quadratic optimization problems [J]. IEEE Transactions on Signal Processing Magazine, 2010, 27(3): 20-34.
- [14] GUTHY C, UTSCHICK W. Low-complexity linear zero-forcing for the MIMO broadcast channel [J]. IEEE Journal of Selected Topics in Signal Processing, 2009, 3(6): 1106-1117.
- [15] 李玉花, 齐春. 利用位置字典对的人脸图像超分辨率方法 [J]. 西安交通大学学报, 2012, 46(6): 7-11.
LI Yuhua, QI Chun. A super-resolution method for face images using position-dictionary pairs [J]. Journal of Xi'an Jiaotong University, 2012, 46(6): 7-11.
- [16] 黄华, 程徽, 刘玓玓. 判断运动复杂度的快速运动估计算法 [J]. 西安交通大学学报, 2009, 43(10): 81-84, 93.
HUANG Hua, CHENG Hui, LIU Dingding. A fast motion estimation algorithm for motion complexity decision [J]. Journal of Xi'an Jiaotong University, 2009, 43(10): 81-84, 93.
- 017]
- 吴飞龙, 王文杰, 刘超文, 等. 接收空间调制信道容量计算及其鲁棒性设计. 2015, 49(2): 49-54. [doi: 10. 7652/xjtuxb201502009]
- 边根庆, 高松, 邵必林. 面向分散式存储的云存储安全架构. 2011, 45(4): 41-45. [doi: 10. 7652/xjtuxb201104008]
- 刘伎昭, 王泉. 车载自组网中联盟博弈的虚假数据检测策略. 2015, 49(2): 69-73. [doi: 10. 7652/xjtuxb201502012]
- 陈诚, 王磊, 李晓峰. 采用星座旋转的高速率空时分组码空间调制算法. 2014, 48(12): 113-119. [doi: 10. 7652/xjtuxb201412018]
- 张光华, 连峰, 韩崇昭, 等. 高斯混合扩展目标多伯努利滤波器. 2014, 48(10): 9-14. [doi: 10. /xjtuxb201410002]
- 高翔, 祝跃飞, 刘胜利. 应用三角模糊矩阵博弈的网络安全评估研究. 2013, 47(8): 49-53. [doi: 10. 7652/xjtuxb201308009]
- 胡鹤, 胡昌振, 姚淑萍. 应用部分马尔科夫博弈的网络安全主动响应决策模型. 2011, 45(4): 18-24. [doi: 10. 7652/xjtuxb201104004]
- 高锐, 李赞, 司江勃, 等. 一种双重序贯检测的协作频谱感知方法. 2014, 48(4): 102-108. [doi: 10. 7652/xjtuxb201404018]
- 周游, 郑娜娥, 胡捍英. 上行正交频分多址接入系统快速盲频偏估计算法. 2013, 47(12): 77-83. [doi: 10. 7652/xjtuxb201312014]
- 王超, 邓科, 庄丽莉, 等. 协作认知网络中鲁棒的分布式波束形成. 2013, 47(12): 84-89. [doi: 10. 7652/xjtuxb201312015]
- 李晓峰, 王磊, 张晓阳. 获得天线选择分集的空移键控调制算法. 2013, 47(8): 98-103. [doi: 10. 7652/xjtuxb201308017]
- 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. 2010, 44(6): 62-66. [doi: 10. 7652/xjtuxb201006012]
- 李建东, 郑杰, 刘勤, 等. 异构协作网络中采用令牌漏桶的多接入业务分配算法. 2014, 48(8): 7-11. [doi: 10. 7652/xjtuxb201408002]
- 李晓艳, 张海林, 郭超平, 等. 一种异步的认知无线网络跳频算法. 2012, 46(12): 30-35. [doi: 10. 7652/xjtuxb201212006]
- 宋婧, 丛犁, 葛建华, 等. 双层网络中一种协作博弈的动态资源分配方法. 2012, 46(10): 89-94. [doi: 10. 7652/xjtuxb201210016]
- 王磊, 陈志刚. 快衰落信道中的分布式差分空时编码传输方案. 2012, 46(4): 77-82. [doi: 10. 7652/xjtuxb201204013]
- 杨咏, 胡予濮, 张乐友, 等. 标准模型下可证明安全的分级身份签名方案. 2011, 45(2): 27-33. [doi: 10. 7652/xjtuxb201102006]
- 张文健, 田茂, 何浩, 等. 分层网络下行中断概率的闭式表达. 2011, 45(12): 59-63. [doi: 10. 7652/xjtuxb201112011]

(编辑 刘杨)

[本刊相关文献链接]

俱莹, 殷勤业, 陈媛, 等. 发射聚焦式的多天线跳空安全通信技术. 2015, 49(6): 22-26. [doi: 10. 7652/xjtuxb201506004]

钟艺玲, 穆鹏程. 单发多收无线窃听信道中的自适应保密速率传输方案. 2015, 49(4): 104-109. [doi: 10. /xjtuxb201504