doi:10.3969/j.issn.1001-893x.2015.07.003
引用格式:刘春国,李立忠. MIMO 系统的物理层安全性[J]. 电讯技术,2015,55(7):725-729. [LIU Chunguo, LI Lizhong. Physical Layer Security Performance of MIMO System[J]. Telecommunication Engineering, 2015, 55(7):725-729.]

MIMO 系统的物理层安全性*

刘春国**,李立忠

(盲信号处理重点实验室,成都 610041)

摘 要:针对闭环多输入多输出(MIMO)预编码,分析了符号随机加密特性以及系统的安全容量,针对信道和预编码矩阵估计存在误差的情况,分析给出了窃听者接收信干噪比的上界。仿真分析表明,在同样信噪比下,安全容量随着收发天线数增加而增大,即使窃听者信噪比略好仍然具有无法窃听的安全容量。存在估计误差时,窃听者接收信干噪比降低,且预编码矩阵估计误差对其影响更严重。

关键词:MIMO 系统;预编码矩阵估计误差;信道容量;安全容量
中图分类号:TN918 **文献标志码**:A **文章编号**:1001-893X(2015)07-0725-05

Physical Layer Security Performance of MIMO System

LIU Chunguo, LI Lizhong

(National Key Laboratory of Science and Technology on Blind Signal Processing, Chengdu 610041, China)

Abstract: For closed-loop multiple-input multiple-output (MIMO) precoding, the random symbol encryption and the secrecy capacity are analyzed. For receiver with channel and precoding matrix estimation error, an upper bound of eavesdropper signal-interference-noise ratio (SINR) is derived. Simulation results show that the secrecy capacity increases with the increase of the numbers of transmitting and receiving antennas, the eavesdropper couldn't intercepte the information even if it has higher signal-to-noise ratio (SNR). The estimation error will lead to the decrease of eavesdropper SINR, and the influence of the precoding matrix estimation error is even worse.

Key words: MIMO system; precoding matrix estimation error; channel capacity; secrecy capacity

1 引 言

自从 1996 年贝尔实验室的 Foschini 提出利用多天线收发的 BLAST(Bell Labs Layered Space-Time)通信架构用以传输高速数据以来,多输入多输出(Multiple-Input Multiple-Output, MIMO)通信系统就以其极高的数据传输速率、频谱利用率和可靠的信息传输引起众多学者的关注。

MIMO 技术在地面无线传输领域得到了广泛应用,并拓展到物理层安全传输方面[1]。近年来,很多研究致力于利用信号在空间、时间以及多个用户之间的特性来实现物理层信号传播的安全性。由于 MIMO 技术引入了信号传播的空间特性,而窃听信道与通信信道在空间上存在差异,信号传播所经历的衰落不同,有学者利用该特性来研究 MIMO 系统安全传输[2],并将其应用于安全通信设计。2006 年,文献[3]给出了慢衰落信道下安全容量的基本特征,表明在存在衰落的情况下,即使窃听者比合法接收者有更好的平均信噪比,系统仍然能够获得信息论上的安全。文献[4]研究分析了衰落信道下的安全容量,并考虑了广播信道的场景,指出在这些场景下利用信道的衰落特性,可以实现安全的物理层传输。同时,开始有文献研究多天线窃听信道的安

* 收稿日期:2014-12-25;修回日期:2015-06-02 Received date: 2014-12-25; Revised date: 2015-06-02
** 通讯作者:schg_liu@126.com **Corresponding author**: schg_liu@126.com

全容量。文献[5-6]分析了多天线发送和窃听场景下的安全传输特性,在信道传输矩阵确定且各个终端已知的情况下,利用广义特征值方法分析了安全容量的特点和安全传输时的折衷考虑。文献[7]考虑了 MIMO 广播场景,当发送端和合作接收方以一定速率传输信息时,可以获得完全的保密,该文给出了这个多天线 MIMO 广播信道场景下的完全安全容量。在理论研究的基础上,也有一部分研究者提出了实现保密传输的具体方法,例如文献[2]提出通过随机化 MIMO 传输的方法来实现安全的思想,文献[8]提出使用波束成形的方法在多用户 MIMO 窃获信道中实现物理层安全的方案。

相关文献的研究表明,MIMO 系统物理层传输具有安全性,但是未进行深入探讨。本文针对利用已知传输信道特性进行 MIMO 预编码的情况,分析了物理层传输具有的安全特性,并进行了仿真。

2 MIMO 系统窃听模型

图 1 所示为窃听者对正常通信进行窃听的示意图。

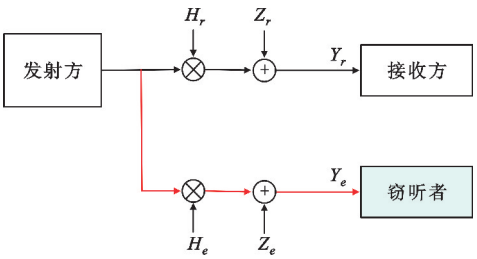


图 1 窃听信道示意图

Fig. 1 Wire-tap channel model

假设发射机、接收方和窃听者接收机分别配置了 N_T、N_R 和 N_e 根天线,且 $N_T<N_R$,则合法接收机和窃听装置的接收信号可以分别表示为

$$\boldsymbol{Y}_r=\boldsymbol{H}_r\boldsymbol{X}+\boldsymbol{Z}_r, \tag{1}$$

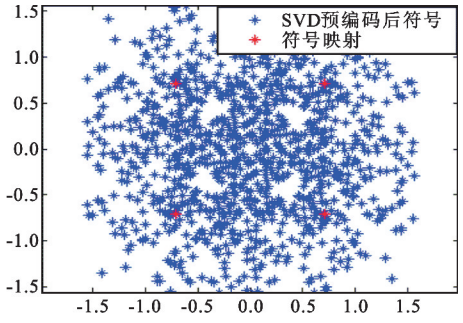
$$\boldsymbol{Y}_e=\boldsymbol{H}_e\boldsymbol{X}+\boldsymbol{Z}_e。 \tag{2}$$

式中,$\boldsymbol{X}\in\mathbb{C}^{N_T\times 1}$ 为发送信号矢量;$\boldsymbol{Z}_r\in\mathbb{C}^{N_R\times 1}$ 和 $\boldsymbol{Z}_e\in\mathbb{C}^{N_e\times 1}$ 分别为接收机和窃听者处的加性高斯白噪声(AWGN)矢量,其每个元素独立同分布,服从 $CN(0,1)$;矩阵 $\boldsymbol{H}_r\in\mathbb{C}^{N_R\times N_T}$ 和 $\boldsymbol{H}_e\in\mathbb{C}^{N_e\times N_T}$ 分别表示合法接收机和窃听者的信道,假设两者相互独立,均服从准静态平坦瑞利衰落,均为零均值单位方差的复高斯变量,且在整个传输过程中是固定的;发送信号满足平均总功率约束 $\mathrm{Tr}(E\{\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}}\})\leqslant P$。

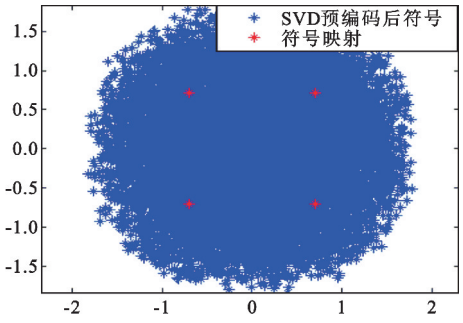
3 MIMO 系统的物理层安全性

3.1 闭环 MIMO 预编码的符号随机加密特性

对于窃听者来说,预编码变换使得发送符号幅度缩放、相位旋转,扰乱了原始的发送信息符号,直观表现为发送符号被加密了。以奇异值分解(Singular Value Decomposition,SVD)预编码为例,当正常通信双方能够实时获取传输信道状态信息,采用 SVD 预编码,4 天线复用时 QPSK 映射符号星座点变化如图 2 所示。



(a)确定性信道



(b)Rayleigh 多径信道

图 2 不同信道条件下预编码的星座图

Fig. 2 Precoded constellations with different channel conditions

由图 2 可见,QPSK 的 4 个星座点变成了很多无规律的点。对于确定性信道,4 天线空间复用时预编码后的星座空间变为 $4\times4^4=1024$。而在 Rayleigh 多径信道条件下,预编码矩阵随着瞬时变化的信道矩阵生成,相当于一种随机的符号加密,星座点将变得毫无规律,由于 Rayleigh 分布的随机变量的实部和虚部服从高斯分布,预编码后星座分布在一个圆形区域。这种情况下,时变信道中的闭环 MIMO 预编码矩阵随信道变化,能达到近似一次一密的符号随机加密效果,由于窃听者难以获取合法通信双方的信道状态信息,也就无从推断预编码矩阵的相关

信息,窃听者难以恢复原始发送符号。

3.2　预编码对 MIMO 系统的安全容量影响分析

当发送端想要向合法用户发送一个安全信息,同时不希望窃听者获取这个信息时,有研究表明,如果发送端和合法用户以一定速率来进行通信的话,就可以实现完全安全,这个速率被称为安全容量,此时理论上能够找到一种方法实现完全安全的通信,使得窃听者能够获取的信息量就为零。

MIMO 系统的安全容量定义为[3]

$$R_s=[I(\boldsymbol{Y}_r;\boldsymbol{X})-I(\boldsymbol{Y}_e;\boldsymbol{X})]^+。\tag{3}$$

式中,$[x]^+=\max\{0,x\}$,$I(\boldsymbol{Y}_e;\boldsymbol{X})$ 表示窃听者所获得的信源信息,$I(\boldsymbol{Y}_r;\boldsymbol{X})$ 表示合法收发端之间的互信息。

对于窃听系统来说,在窃听接收机确定的条件下,能够获取的最大信息量为 $I(\boldsymbol{Y}_e;\boldsymbol{X})$。若通信双方传输的信息速率 $I(\boldsymbol{Y}_r;\boldsymbol{X})$ 超过 $I(\boldsymbol{Y}_e;\boldsymbol{X})$,窃听者就不能无误接收发送端传输的通信信息,由此可以得到一个安全通信的充分条件:$I(\boldsymbol{Y}_r;\boldsymbol{X})\geqslant I(\boldsymbol{Y}_e;\boldsymbol{X})$,即 $R_s>0$。当 $R_s>0$ 时,正常通信双方传输的信息量超过窃听者可以达到的信息量,因此窃听者无法获得全部通信信息,该系统能够实现安全通信。

文献[9]已分析了 MIMO 系统的信道容量,可以表示为

$$C=\max I(\boldsymbol{X};\boldsymbol{Y})=\max_{\boldsymbol{R}_{XX},\mathrm{tr}(\boldsymbol{R}_{XX})=P}\mathrm{lb}\ \det\left[\boldsymbol{I}_{N_R}+\frac{\rho}{N_T}\boldsymbol{H}\boldsymbol{R}_{\boldsymbol{XX}}\boldsymbol{H}^{\mathrm{H}}\right]。\tag{4}$$

式中,ρ 为接收信噪比,$\det[\cdot]$ 为矩阵行列式,$\boldsymbol{R}_{\boldsymbol{XX}}=E(\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}})$。

若发送方已知信道矩阵 $\boldsymbol{H}_r$,对其进行 SVD 分解得

$$\boldsymbol{H}_r=\boldsymbol{U}_r\boldsymbol{\Lambda}_r\boldsymbol{V}_r^{\mathrm{H}}。\tag{5}$$

发送方利用已知信道特性采用特征值模式传输,进行 MIMO 预编码:

$$\widetilde{\boldsymbol{X}}=\boldsymbol{V}_r\boldsymbol{D}^{1/2}\boldsymbol{X}。\tag{6}$$

式中,$\boldsymbol{D}$ 是对角矩阵,其对角元素为 $D_{ii}=\max\left(0,u-\frac{\sigma_w^2}{\lambda_i}\right)$,$\sum_{i=1}^{N_T}\max\left(0,u-\frac{\sigma_w^2}{\lambda_i}\right)=P$,$\lambda_i$ 是式(5)中 $\boldsymbol{\Lambda}$ 的第 i 个对角元素,$\boldsymbol{\Lambda}_r=\mathrm{diag}\left(\sqrt{\lambda_1},\sqrt{\lambda_2},\cdots,\sqrt{\lambda_{N_T}}\right)$,此时 $\boldsymbol{R}_{\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{X}}}=E(\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{X}}^{\mathrm{H}})=\boldsymbol{V}_r\boldsymbol{D}\boldsymbol{V}_r^{\mathrm{H}}$。

由于合作接收方能准确估计出通信信道特性,由式(4)可得其接收信道容量为

$$C_n=\mathrm{lb}\ \det\left(\boldsymbol{I}_{N_R}+\frac{\rho}{N_T}\boldsymbol{D}\cdot\boldsymbol{\Lambda}_r^2\right),\tag{7}$$

此时窃听信道容量为

$$C_e=\mathrm{lb}\ \det\left(\boldsymbol{I}_{N_e}+\frac{\rho}{N_T}\boldsymbol{H}_e\boldsymbol{R}_{\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{X}}}\boldsymbol{H}_e^{\mathrm{H}}\right)。\tag{8}$$

由于窃听者信道与正常接收信道不同(即 $\boldsymbol{H}_e\neq\boldsymbol{H}_r$),无法通过自身计算获得发射预编码矩阵,此时系统的安全容量为

$$R_s=[C_n-C_e]^+=\left[\mathrm{lb}\ \det\left(\boldsymbol{I}_{N_R}+\frac{\rho}{N_T}\boldsymbol{D}_k\cdot\boldsymbol{\Lambda}_k^2\right)-\mathrm{lb}\ \det\left(\boldsymbol{I}_{N_e}+\frac{\rho}{N_T}\boldsymbol{H}_e\boldsymbol{R}_{\widetilde{\boldsymbol{X}}\widetilde{\boldsymbol{X}}}\boldsymbol{H}_e^{\mathrm{H}}\right)\right]^+。\tag{9}$$

式中,$[x]^+=\max\{0,x\}$。

由于预编码针对传输信道矩阵 $\boldsymbol{H}_r$ 优化设计,而窃听信道存在差异,与预编码矩阵不匹配,因此在接收时无法达到最优的效果。在接收信噪比相近时,安全容量 $R_s>0$,这时窃听者能够获取的互信息小于正常通信传输的互信息。

3.3　估计误差对窃听者接收信干噪比的影响

当窃听者在信道估计和预编码矩阵估计方面存在误差时,窃听者接收到信号的信噪比会降低。考虑发送端发射 N_T 个数据流,预编码矩阵为 $\boldsymbol{V}\in\mathbb{C}^{N_T\times N_T}$,窃听者接收信号为

$$\boldsymbol{Y}_e=\boldsymbol{H}_e\boldsymbol{V}\boldsymbol{X}+\boldsymbol{Z}_e。\tag{10}$$

式中,$\boldsymbol{H}_e\in\mathbb{C}^{N_e\times N_T}$ 为窃听者信道矩阵,其中每个元素都服从独立 $CN(0,1)$ 分布。

若窃听者能对信道矩阵 $\boldsymbol{H}_e$ 及预编码矩阵进行相应的估计,则窃听者对数据流 k 的接收信号可表示为

$$\begin{aligned}\boldsymbol{Y}_e&=\boldsymbol{H}_e\boldsymbol{V}\boldsymbol{X}+\boldsymbol{Z}_e=\\&\boldsymbol{H}_e[\boldsymbol{v}_1,\cdots\boldsymbol{v}_{N_T}]\begin{bmatrix}x_1\\\vdots\\x_{N_T}\end{bmatrix}+\boldsymbol{Z}_e=\\&\boldsymbol{H}_e\boldsymbol{v}_kx_k+\underbrace{\left(\sum_{i=1,i\neq k}^{N_T}\boldsymbol{H}_e\boldsymbol{v}_ix_i+\boldsymbol{Z}_e\right)}_{\text{Interference+Noise}}。\end{aligned}\tag{11}$$

假设窃听者的信道估计值为 $\hat{\boldsymbol{H}}_e=\boldsymbol{H}_e+\Delta_h$,预编码矢量的估计值为 $\hat{\boldsymbol{v}}_k=\boldsymbol{v}_k+\Delta_v$,其中 Δ_h 中的元素服从 $CN(0,\sigma_h^2)$ 分布,Δ_v 中的元素服从 $CN(0,\sigma_v^2)$ 分布,当窃听者采用 MMSE(Minimum Mean Square Error)检测接收机[10]时有

$$\hat{x}_k=(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)^{\mathrm{H}}\left(\begin{array}{l}(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)^{\mathrm{H}}+\\E\left[\left(\sum_{i=1,i\neq k}^{N_T}\boldsymbol{H}_e\boldsymbol{v}_ix_i+\boldsymbol{Z}_e\right)\left(\sum_{i=1,i\neq k}^{N_T}\boldsymbol{H}_e\boldsymbol{v}_ix_i+\boldsymbol{Z}_e\right)^{\mathrm{H}}\right]\end{array}\right)^{-1}\cdot$$

$$(\boldsymbol{H}_e\boldsymbol{v}_kx_k+\sum_{i=1,i\neq k}^{N_T}\boldsymbol{H}_e\boldsymbol{v}_ix_i+\boldsymbol{Z}_e)=$$

$$(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)^{\mathrm{H}}((\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)^{\mathrm{H}}+\sum_{i=1,i\neq k}^{N_T}(\boldsymbol{H}_e\boldsymbol{v}_i)(\boldsymbol{H}_e\boldsymbol{v}_i)^{\mathrm{H}}+\sigma_e^2\boldsymbol{I}_{N_e})^{-1}\cdot$$
$$(\boldsymbol{H}_e\boldsymbol{v}_kx_k+\sum_{i=1,i\neq k}^{N_T}\boldsymbol{H}_e\boldsymbol{v}_ix_i+\boldsymbol{Z}_e)。\tag{12}$$

假设接收机在最佳情况下,窃听者各数据流之间不存在相互干扰,即

$$\sum_{i=1,i\neq k}^{N_T}\boldsymbol{H}_e\boldsymbol{v}_ix_i=0,\tag{13}$$

此时,对第 k 个数据流的最佳检测结果为

$$\begin{aligned}\hat{x}_{k\_\mathrm{best}}&=(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)^{\mathrm{H}}((\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)(\hat{\boldsymbol{H}}_e\hat{\boldsymbol{v}}_k)^{\mathrm{H}}+\sigma_e^2\boldsymbol{I}_{N_e})^{-1}(\boldsymbol{H}_e\boldsymbol{v}_kx_k+\boldsymbol{Z}_e)=\\&((\boldsymbol{H}_e+\Delta_h)(\boldsymbol{v}_k+\Delta_v))^{\mathrm{H}}\cdot\\&((\boldsymbol{H}_e+\Delta_h)(\boldsymbol{v}_k+\Delta_v)(\boldsymbol{v}_k+\Delta_v)^{\mathrm{H}}(\boldsymbol{H}_e+\Delta_h)^{\mathrm{H}}+\sigma_e^2\boldsymbol{I}_{N_e})^{-1}\cdot\\&(\boldsymbol{H}_e\boldsymbol{v}_kx_k+\boldsymbol{Z}_e)=\\&\boldsymbol{\alpha}\boldsymbol{H}_e\boldsymbol{v}_kx_k+\boldsymbol{\alpha}\boldsymbol{Z}_e。\end{aligned}\tag{14}$$

式中,

$$\boldsymbol{\alpha}=((\boldsymbol{H}_e+\Delta_h)(\boldsymbol{v}_k+\Delta_v))^{\mathrm{H}}\cdot$$
$$((\boldsymbol{H}_e+\Delta_h)(\boldsymbol{v}_k+\Delta_v)(\boldsymbol{v}_k+\Delta_v)^{\mathrm{H}}(\boldsymbol{H}_e+\Delta_h)^{\mathrm{H}}+\sigma_e^2\boldsymbol{I}_{N_e})^{-1}。$$

则第 k 个数据流的信干噪比(Signal-Interference-Noise Ratio,SINR)上界为

$$\mathrm{SINR}_{\mathrm{upper}}=\frac{(\boldsymbol{\alpha}\boldsymbol{H}_e\boldsymbol{v}_k)(\boldsymbol{\alpha}\boldsymbol{H}_e\boldsymbol{v}_k)^{\mathrm{H}}}{\sigma_e^2\boldsymbol{\alpha}\boldsymbol{\alpha}^{\mathrm{H}}}。\tag{15}$$

4 仿真实验及分析

式(9)的目标函数难以得到闭合解,为了评估 MIMO 系统的安全容量,分析系统的安全性能,我们对 MIMO 系统的信道容量进行仿真,分析信道容量、安全容量在不同信噪比下的特性,以指导安全通信系统的设计。

在高斯白噪声信道下进行 Monte Carlo 仿真分析,仿真中信道响应 $\boldsymbol{H}_r$、$\boldsymbol{H}_e$ 随机产生且 $E\{\boldsymbol{H}_e\}=E\{\boldsymbol{H}_r\}$。图 3 所示为 $N_T=8$、$N_R=8$ 时,1000 次 Monte Carlo 试验得到的系统在信道响应未知、信道响应已知、窃听信道条件下的信道容量和安全容量曲线。

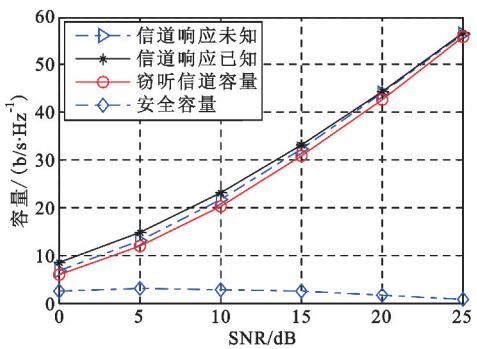


图 3 $N_T=8$、$N_R=8$ 时各种信道条件下的信道容量

Fig. 3 The channel capacity of various channel conditions when $N_T=8$, $N_R=8$

由图 3 可见,在同样的接收信噪比条件下,窃听信道所能够达到的信道容量是最低的,甚至低于信道响应未知条件下的信道容量,表明窃听信道与接收信道不匹配会给窃听者带来负面影响,使其无法正常接收。而随着接收信噪比增强,信道差异带来的影响逐渐减小,安全容量也随之变小。

不同收发天线时的安全容量如图 4 所示。由图可见,在同样信噪比条件下,随着收发天线数增加,信道安全容量增大,表明天线数越多,窃听信道差异的影响越大,窃听者越难以获得信息。

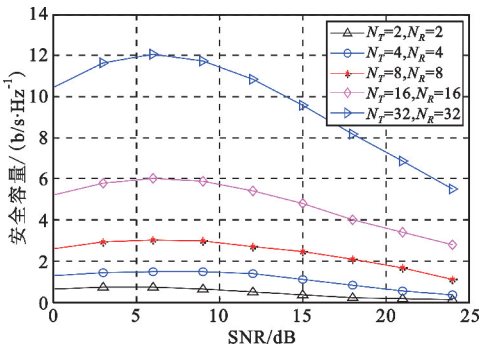


图 4 不同收发天线条件下的安全容量

Fig. 4 Secrecy capacity of different transmitting and receiving antennas

当窃听信道条件较好,接收信噪比高于正常通信双方接收信噪比时的安全容量如图 5 所示,图中 ΔSNR 为窃听者的信噪比增量。图中可见,即使在窃听者信噪比条件较优时,在一定信噪比条件下仍然可以实现安全通信。但是随着接收信噪比增强,信道差异带来的影响减小,安全容量将逐渐减小至 0,窃听者将可以获得正常通信双方的信息。

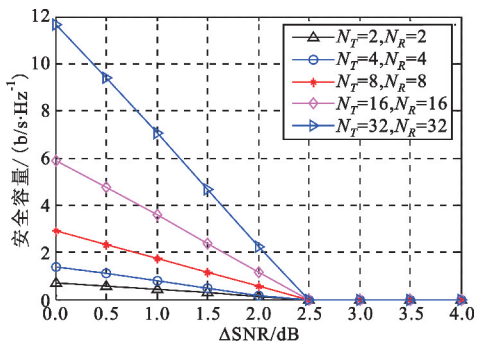


图 5 信噪比为 3 dB 时安全容量随窃听者信噪比增量的变化曲线

Fig. 5 Secrecy capacity versus ΔSNR when SNR = 3 dB

假设 $N_T=4$,图 6 是在不同估计误差条件下随着接收噪声功率 σ_e^2 变化的仿真曲线。

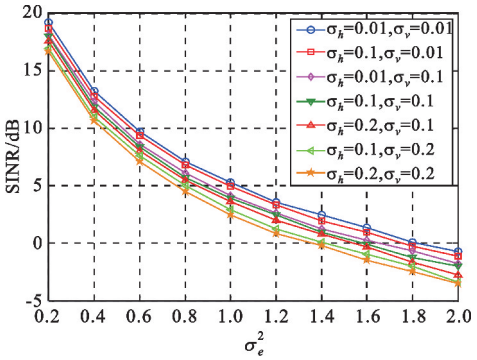


图 6　不同估计误差条件下的窃听者 SINR 上界

Fig. 6 The upper bound of SINR for different estimation error

由图 6 可知,随着信道估计误差和预编码矩阵估计误差的增加,相应的 SINR 上界在不断恶化,而且预编码矩阵的估计误差对其影响更大。

5　结束语

本文讨论了在已知传输信道特性,利用预编码来实现安全传输时的符号加密特性以及 MIMO 系统的安全容量特点。分析及仿真结果表明,由于窃听信道与正常通信信道存在差异,使得窃听信道容量低于正常接收信道容量,因此在一定信噪比条件下安全容量大于 0,此时窃听者将不能完全获得通信信息,信息传输是安全的。当收发天线数越多时,窃听信道差异带来的影响越大,此时安全容量越高,即使窃听者比合法接收者有更好的平均信噪比,系统仍然能够获得安全通信能力。

MIMO 系统的物理层安全性通常从三个方面来考虑,一是利用已知的传输信道特性进行 MIMO 预编码来实现安全传输,二是使用波束成形的方法实现物理层安全传输,三是使用协作方式结合物理层网络编码来或者发射人工噪声来实现物理层安全传输,本文主要针对第一种思想进行探讨,下一步还需要从其他方面进一步分析。

参考文献:

[1] 胡爱群,李古月. 无线通信物理层安全方法综述[J]. 数据采集与处理,2014,29(3):341-350.
HU Aiqun, LI Guyue. Physical Layer Security in Wireless Communication: Survey[J]. Journal of Data Acquisition and Processing, 2014, 29(3): 341-350. (in Chinese)

[2] LI X H, Ratazzi E P. MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks[C]//Proceedings of 2005 IEEE Military Communication Conference. Atlantic, NJ: IEEE, 2005: 1-7.

[3] Barros J, Rodrigues M R D. Secrecy capacity of wireless channels[C]//Proceedings of IEEE International Symposium on Information Theory. Seattle: IEEE, 2006: 356-360.

[4] Liang Y, Poor H V, Shamai S. Secure communication over fading channels[J]. IEEE Transactions on Information Theory, 2008, 54(6): 2470-2492.

[5] Khisti A, Wornell G W. Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel[J]. IEEE Transactions on Information Theory, 2010, 56(7): 3088-3104.

[6] Khisti A, Wornell G W. Secure TransmissionWith Multiple Antennas - Part II: The MIMOME Wiretap Channel[J]. IEEE Transactions on Information Theory, 2010, 56(11): 5515-5532.

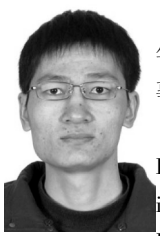
[7] Oggier F, Hassibi B. The Secrecy Capacity of the MIMO Wiretap Channel[J]. IEEE Transactions on Information Theory, 2011, 57(8): 4961-4972.

[8] Mukherjee A, Swindlehurst A L. Utility of Beamforming Strategies for Secrecy in Multiuser MIMO Wiretap Channels[C]//Proceedings of 47th Annual Allerton Conference on Communication, Control, and Computing. Illinois, USA: Allerton, 2009: 1134-1141.

[9] Foschini G J, Gans M J. On the limits of wireless communications in a fading environment when using multiple antennas[J]. Wireless Personal Communications, 1998, 6(3): 315-335.

[10] Park H, Lee Y S, Kim N. Performance Analysis of MIMO System with Linear MMSE Receiver[J]. IEEE Transactions on Wireless Communications, 2008, 7(11): 4474-4478.

作者简介:



刘春国(1982—),男,云南丽江人,2007 年获工学硕士学位,现为博士研究生,主要从事无线通信系统、信号处理方面的研究工作;

LIU Chunguo was born in Lijiang, Yunnan Province, in 1982. He received the M. S. degree in 2007. He is currently working toward the Ph. D. degree. His research concerns wireless communication system and signal processing.

Email: schg_liu@126.com

李立忠(1967—),男,四川成都人,2000 年于电子科技大学获博士学位,现为高级工程师,主要从事通信系统、信号处理方面的研究工作。

LI Lizhong was born in Chengdu, Sichuan Province, in 1967. He received the Ph. D. degree from University of Electronic Science and Technology of China in 2000. He is now a senior engineer. His research concerns communication system and signal processing.