DOI：10.7652/xjtuxb201504017

单发多收无线窃听信道中的自适应保密速率传输方案

钟艺玲[1]，穆鹏程[2]
（1. 西安交通大学智能网络与网络安全教育部重点实验室，710049，西安；
2. 西安交通大学电子与信息工程学院，710049，西安）

摘要：针对无线通信中基于保密中断的物理层安全问题，提出了一种单发多收（SIMO）窃听信道下使用保密中断概率约束的自适应保密速率方案。利用信道估计与信道的衰落特性分别获得发射端到合法接收端信道（主信道）的信道状态信息（CSI）与发射端到窃听者信道（窃听信道）的统计CSI。在发射端已知主信道CSI而未知窃听信道CSI的情况下，根据主信道CSI和窃听信道CSI的概率密度函数对保密传输速率进行自适应调整，并根据保密中断的定义确定发射门限，然后在满足保密中断概率约束的条件下实现保密吞吐量的最大化。在准静态瑞利衰减信道条件下进行了仿真验证，结果表明：与以往的SISO系统方法相比，在保密中断概率低于0.1、合法接收端天线数不少于窃听端时，系统的保密吞吐量可提高1倍以上；即使合法接收端的天线数少于窃听端，只要合法接收端的天线数足够多，SIMO系统的保密吞吐量仍能优于SISO系统。

关键词：无线通信；物理层安全；窃听信道；中断概率；保密速率；吞吐量
中图分类号：TN929.5 **文献标志码**：A **文章编号**：0253-987X(2015)04-0104-06

An Adaptive Secret Transmission Rate Scheme in SIMO Wireless Wiretap Channel

ZHONG Yiling[1], MU Pengcheng[2]
(1. Ministry of Education Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China; 2. School of Electronics and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: An adaptive secret transmission rate scheme with secret outage probability constraint in SIMO wireless wiretap channel is proposed to consider the physical layer security issue for the wireless communication with secrecy outage. The channel estimation and channel fading characteristics are used to obtain the channel state information (CSI) about the channel from the transmitter to the legitimate receiver (the main channel) and the CSI about the channel from the transmitter to the eavesdropper (the eavesdropper's channel), respectively. When the CSI about the main channel is known while the CSI about the eavesdropper's channel is not known by the transmitter, the secrecy rate is adjusted according to the CSI of the main channel and the probability density function of the eavesdropper's channel, and the emission threshold is obtained according to the definition of secrecy outage. Then the secrecy throughput is maximized in the condition of satisfying the constraint of secrecy outage probability. The quasi-static Rayleigh

收稿日期：2014-07-29。 作者简介：钟艺玲（1990—），女，硕士生；穆鹏程（通信作者），男，博士，讲师。 基金项目：国家自然科学基金资助项目（61071125，61172092，61231013）；国家自然科学基金创新群体资助项目（61221063）；教育部高等学校博士学科点专项科研基金资助项目（20130201130003）。
网络出版时间：2015-01-16 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20150116.1510.006.html

fading channel is used in the simulation. Simulation results show that when secrecy outage probability is lower than 0.1 and the antenna number of the legitimate receivers is no less than that of eavesdropper, the secrecy throughput of the proposed approach is twice that of the previous methods for SISO system, and that as long as there are sufficient antennas in the legitimate receiver, the secrecy throughput of SIMO system is larger than that of SISO system even if the antenna number of the legitimate receivers is smaller than that of eavesdropper.

Keywords: wireless communication; physical layer security; wiretap channel; outage probability; secrecy rate; throughput

近年来，在无线通信技术的快速发展与广泛应用给人们带来各种便利的同时，也带来了日益突出的信息安全问题[1-2]。无线通信安全问题的根源来自于电磁波的广播特性，即无线通信的物理层是不安全的。因此，如何从物理层保障无线通信安全是解决无线通信安全问题的关键所在。无线通信的物理层安全可以用窃听信道模型来描述，其中高斯窃听信道[3]是重要的无线窃听信道模型之一。窃听信道模型通常有一个发射端和两个接收端，其中包括一个合法接收端一个窃听接收端。发射端到合法接收端的信道称为主信道，发射端到窃听接收端的信道称为窃听信道。窃听信道下的信息论安全主要研究的是保密速率和保密容量，这种保密性通常也被称为物理层安全。

尽管围绕无线通信的物理层安全问题目前已经有很多研究工作，但早期大部分研究均假定信道增益是固定的，此时信道就等效成加性高斯信道[4-7]。文献[8-9]中利用分布式多天跳空收发技术来实现物理层安全，充分利用了空谱资源，但仍是在假设信道恒定的情况下考虑的。考虑到无线通信中普遍存在衰落现象，文献[10-13]对衰落信道的保密容量进行了研究。文献[10]在所有发射端和接收端信道状态信息(CSI)已知的情况下研究了慢衰落信道的保密中断性能。作为比较，文献[12]在假设发射端和合法接收端完全已知主信道 CSI 却不知道窃听信道 CSI 的条件下，从中断概率方面研究了保密容量。该文献使用固定的保密速率，因此中断概率总是要高于一个确定的下界。为了提高在任意小保密中断概率条件下的保密速率，文献[13]重新考虑了保密中断的定义，提出了一种对主信道 CSI 大小设置门限的开关式发射方法。在此基础上，文献[14]中提出了一种自适应保密速率的方法，即保密速率可以根据主信道的 CSI 动态调整。文献[14]还通过与文献[11]和文献[12]中方法进行对比，证明了自适应保密速率的方法可以获得更佳的保密吞吐量，然而，该文献中的信道只局限于单入单出(SISO)窃听信道，还没有充分利用无线通信中多天线技术的优势。

考虑到多天线的使用在无线通信系统中越来越普遍，本文将文献[14]中的工作扩展到单入多出(SIMO)窃听信道模型，该模型对应于蜂窝无线通信系统中单天线终端向多天线基站发送信息这一上行通信过程。在保密中断概率的约束下，本文研究了 SIMO 窃听信道中使用自适应保密速率方案提高保密吞吐量，根据保密中断的定义，给出了确定发射门限的算法，并研究接收端天线数对保密吞吐量的影响。本文的研究结果将为利用多天线技术提高无线通信物理层安全提供理论支持。

1　系统模型

本文所采用的 SIMO 窃听信道模型如图 1 所示，该模型包括 3 个部分：发射端 Alice、合法接收端 Bob 和窃听端 Eve。Alice 向合法接收端 Bob 发送信息，而 Eve 则试图窃听该信息。Alice 使用单天线发射，Bob 和 Eve 均使用多天线接收，其接收天线数分别为 M 和 N。$\boldsymbol{h}_{\mathrm{B}}$、$\boldsymbol{h}_{\mathrm{E}}$ 分别为 Alice 到 Bob(主信道)和 Alice 到 Eve(窃听信道)的信道，这里 $\boldsymbol{h}_{\mathrm{B}}$ 和 $\boldsymbol{h}_{\mathrm{E}}$ 分别为 $M\times 1$ 和 $N\times 1$ 的列向量。Alice 所发送的信号 x 是 0 均值复高斯信号，且满足 $E\{|x|^2\}=P$，其中 P 为 Alice 的发射功率，且满足 $P>0$。此时，Bob 与 Eve 接收到的信号分别为

$$\boldsymbol{y}_{\mathrm{B}}=\boldsymbol{h}_{\mathrm{B}}x+\boldsymbol{n}_{\mathrm{B}} \tag{1}$$

$$\boldsymbol{y}_{\mathrm{E}}=\boldsymbol{h}_{\mathrm{E}}x+\boldsymbol{n}_{\mathrm{E}} \tag{2}$$

式中：$\boldsymbol{n}_{\mathrm{B}}$ 和 $\boldsymbol{n}_{\mathrm{E}}$ 分别为 Bob 和 Eve 端接收到的加性高斯白噪声(AWGNS)，且分别满足 $E\{\boldsymbol{n}_{\mathrm{B}}\boldsymbol{n}_{\mathrm{B}}^{\mathrm{H}}\}=\boldsymbol{I}_M$ 和 $E\{\boldsymbol{n}_{\mathrm{E}}\boldsymbol{n}_{\mathrm{E}}^{\mathrm{H}}\}=\boldsymbol{I}_N$，这里 $\boldsymbol{I}_M$ 和 $\boldsymbol{I}_N$ 分别是 $M\times M$ 和 $N\times N$ 的单位矩阵。

假设无线信道为慢衰落，并建模为准静态瑞利衰落，此时 $\boldsymbol{h}_{\mathrm{B}}$ 和 $\boldsymbol{h}_{\mathrm{E}}$ 分别服从分布 $\boldsymbol{h}_{\mathrm{B}}\sim\mathrm{CN}(0,\Gamma_{\mathrm{B}}\boldsymbol{I}_M)$ 和 $\boldsymbol{h}_{\mathrm{E}}\sim\mathrm{CN}(0,\Gamma_{\mathrm{E}}\boldsymbol{I}_N)$，其中 $\mathrm{CN}(0,\Sigma)$ 表示均

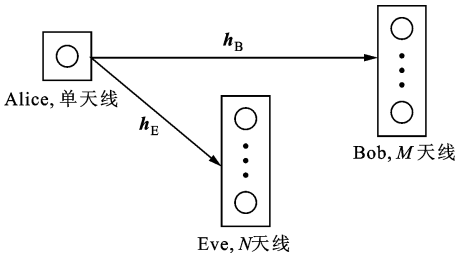

图 1 系统模型

值为 0、、方差为 Σ 的圆对称复高斯分布，$\Gamma_B>0$ 和 $\Gamma_E>0$ 反映了 2 个信道的大尺度衰落。记 Bob 和 Eve 第 i 根天线上的信噪比分别为 $\Upsilon_{B,i}$ 和 $\Upsilon_{E,i}$，由于各支路服从独立同分布的瑞利衰落，因此 Bob 与 Eve 第 i 根天线上的信噪比的概率密度分别为

$$f_{B,i}(\Upsilon_{B,i})=\begin{cases}\dfrac{1}{\widetilde{\Gamma}_B}\exp\left(-\dfrac{\Upsilon_{B,i}}{\widetilde{\Gamma}_B}\right), & \Upsilon_{B,i}\geqslant 0\\ 0, & \Upsilon_{B,i}<0\end{cases} \tag{3}$$

$$f_{E,i}(\Upsilon_{E,i})=\begin{cases}\dfrac{1}{\widetilde{\Gamma}_E}\exp\left(-\dfrac{\Upsilon_{E,i}}{\widetilde{\Gamma}_E}\right), & \Upsilon_{E,i}\geqslant 0\\ 0, & \Upsilon_{E,i}<0\end{cases} \tag{4}$$

式中：$\widetilde{\Gamma}_B=P\Gamma_B$，$\widetilde{\Gamma}_E=P\Gamma_E$。

在 SIMO 系统中，Bob 与 Eve 可以分别对多个天线接收到 Alice 发射的信号进行最大比合并以提高接收信噪比。经过最大比合并处理后主信道的输出信噪比为 $\Upsilon_{\Sigma,B}=\sum_{i=1}^{M}\Upsilon_{B,i}$，窃听信道的输出信噪比为 $\Upsilon_{\Sigma,E}=\sum_{i=1}^{N}\Upsilon_{E,i}$。此时，主信道的信道容量与窃听信道的信道容量分别为

$$C_B=\mathrm{lb}(1+\Upsilon_{\Sigma,B}) \tag{5}$$

$$C_E=\mathrm{lb}(1+\Upsilon_{\Sigma,E}) \tag{6}$$

相应的保密容量为

$$C_S=[C_B-C_E]^+ \tag{7}$$

式中：$[a]^+$ 表示 $\max\{0,a\}$，其中 a 为实数。

考虑到各支路都是独立同分布的瑞利衰落，此时 $\Upsilon_{\Sigma,B}$ 和 $\Upsilon_{\Sigma,E}$ 分别服从自由度为 $2M$ 和 $2N$ 的卡方（χ^2）分布，其数学期望分别为 $\overline{\Upsilon}_{\Sigma,B}=M\widetilde{\Gamma}_B$ 和 $\overline{\Upsilon}_{\Sigma,E}=N\widetilde{\Gamma}_E$，方差分别为 $2M\widetilde{\Gamma}_B$ 和 $2N\widetilde{\Gamma}_E$。因此，$\Upsilon_{\Sigma,B}$ 和 $\Upsilon_{\Sigma,E}$ 的概率密度函数可以分别表示如下

$$p_B(\Upsilon_{\Sigma,B})=\begin{cases}\dfrac{\Upsilon_{\Sigma,B}^{M-1}}{\widetilde{\Gamma}_B^M(M-1)!}\exp\left(-\dfrac{\Upsilon_{\Sigma,B}}{\widetilde{\Gamma}_B}\right), & \Upsilon_{\Sigma,B}\geqslant 0\\ 0, & \Upsilon_{\Sigma,B}<0\end{cases} \tag{8}$$

$$p_E(\Upsilon_{\Sigma,E})=\begin{cases}\dfrac{\Upsilon_{\Sigma,E}^{N-1}}{\widetilde{\Gamma}_E^N(N-1)!}\exp\left(-\dfrac{\Upsilon_{\Sigma,E}}{\widetilde{\Gamma}_E}\right), & \Upsilon_{\Sigma,E}\geqslant 0\\ 0, & \Upsilon_{\Sigma,E}<0\end{cases} \tag{9}$$

2 SIMO 窃听信道的保密中断

为了在保证通信可靠性的同时获得更大的保密吞吐量，本文采用文献[14]中的自适应保密速率方案（ADP 方案）的传输信息，所不同的是本文研究 SIMO 窃听信道，并且使用不同于文献[14]中平均功率约束的最大功率约束。假设通信系统所需要满足的保密中断概率为 ε，并且 $0<\varepsilon<1$。R_S 表示通信系统的保密速率。根据 $\Upsilon_{\Sigma,B}$ 值动态调整码字发送速率 R_B 的值，使之满足 $R_B=C_B$，则 R_S 将满足 $R_S\leqslant C_B$，此时中断发生在无法保证保密性的情况下，即保密中断。根据文献[14]中保密中断的定义可得

$$\varepsilon=P_r\{C_B-R_S\leqslant C_E\,|\,\boldsymbol{h}_B\}=P_r\{\Upsilon_{\Sigma,E}\geqslant B\,|\,\boldsymbol{h}_B\}=\exp\left(-\frac{B}{\widetilde{\Gamma}_E}\right)\sum_{k=1}^{N}\frac{1}{(k-1)!}\left(\frac{B}{\widetilde{\Gamma}_E}\right)^{k-1} \tag{10}$$

其中 $B=(1+\Upsilon_{\Sigma,B})2^{-R_S}-1$，其值可以通过解方程 $\exp\left(-\dfrac{B}{\widetilde{\Gamma}_E}\right)\sum_{k=1}^{N}\dfrac{1}{(k-1)!}\left(\dfrac{B}{\widetilde{\Gamma}_E}\right)^{k-1}=\varepsilon$ 得到。下面将分析如何通过二分法解方程得到 B 的值，即

$$f(B)=\exp\left(-\frac{B}{\widetilde{\Gamma}_E}\right)\sum_{k=1}^{N}\frac{1}{(k-1)!}\left(\frac{B}{\widetilde{\Gamma}_E}\right)^{k-1}-\varepsilon \tag{11}$$

对 $f(B)$ 求导可得

$$\frac{\mathrm{d}f}{\mathrm{d}B}=-\frac{1}{\widetilde{\Gamma}_E}\exp\left(-\frac{B}{\widetilde{\Gamma}_E}\right)\frac{1}{(N-1)!}\left(\frac{B}{\widetilde{\Gamma}_E}\right)^{N-1}<0 \tag{12}$$

因此，$f(B)$ 是关于 B 的单调递减函数。考虑到 $\lim_{B\to 0}f(0)=1-\varepsilon>0$ 以及 $\lim_{B\to+\infty}f(B)=-\varepsilon<0$，因此 $f(B)=0$ 在区间 $(0,+\infty)$ 上有且仅有一个根，通过二分法数值求解方程 $f(B)=0$ 可以得到 B 的值。此时为确定 $f(B)=0$ 的根所在的区间，可先假设其根区间 (a,b)，根据 $f(B)=0$ 在区间 $(0,+\infty)$ 上有且仅有一个根可知 $a=0$，$b>0$，若 $f(b)\geqslant 0$，则将根区间扩大直至 $f(b)<0$，获得正确的根区间。具体求解 B 的算法如算法 1 所示。

算法 1 利用二分法求 B 的值

(1)初始化：设 $a=0$；$b=100$；$\delta=0.001$；

(2)确定根所在的区间：

while($f(b)\geqslant 0$){

$b \leftarrow 2b$；二分法求解区间扩大 2 倍

}End

(3)二分法：

while 1{

$x \leftarrow \dfrac{(a+b)}{2}$；取根所在区间的中点

$fx \leftarrow f(x)$；求中点处函数值

if 中点处函数值 $fx>0$ do

$a \leftarrow x$；根区间左端点移至中点处

else

$b \leftarrow x$；根区间右端点移至中点处

end if

if abs$(a-b)<\delta$do

$B \leftarrow \dfrac{(a+b)}{2}$；break；

end if

}End

另一方面，由 $B=(1+\Upsilon_{\Sigma,\mathrm{B}})2^{-R_\mathrm{S}}-1$ 可得保密速率 R_S 的表达式为

$$R_\mathrm{S}=\mathrm{lb}\left(\frac{1+\Upsilon_{\Sigma,\mathrm{B}}}{1+B}\right) \tag{13}$$

可以证明，当以该保密速率进行传输时能够同时满足可靠性。事实上，由于 $B>0$，由式(12)可得

$$R_\mathrm{S}=\mathrm{lb}\,\frac{1+\Upsilon_{\Sigma,\mathrm{B}}}{1+B}<\mathrm{lb}(1+\Upsilon_{\Sigma,\mathrm{B}})=C_\mathrm{B} \tag{14}$$

此时保密速率小于主信道容量，因此通信是可靠的。

此外，考虑到保密速率必须是非负的，因此 R_S 最终可以表示为

$$R_\mathrm{S}(\Upsilon_{\Sigma,\mathrm{B}})=\begin{cases}\mathrm{lb}\,\dfrac{1+\Upsilon_{\Sigma,\mathrm{B}}}{1+B}, & \Upsilon_{\Sigma,\mathrm{B}}>B\\ 0, & \Upsilon_{\Sigma,\mathrm{B}}\leqslant B\end{cases} \tag{15}$$

以上结果是在已知主信道 CSI 的情况下得到的自适应保密速率。考虑到主信道也具有衰落特性，因此需要使用保密吞吐量来衡量系统的保密传输性能。根据文献[14]对保密吞吐量的定义可以得到此时的保密吞吐量如式(16)所示

$$\bar{R}_\mathrm{S}^{M}=\int_0^{+\infty}R_\mathrm{S}(\Upsilon_{\Sigma,\mathrm{B}})p_\mathrm{B}(\Upsilon_{\Sigma,\mathrm{B}})\mathrm{d}\Upsilon_{\Sigma,\mathrm{B}}=$$

$$\int_B^{+\infty}\log\left(\frac{1+\Upsilon_{\Sigma,\mathrm{B}}}{1+B}\right)\frac{\Upsilon_{\Sigma,\mathrm{B}}^{M-1}}{\tilde{\Gamma}_\mathrm{B}^{M}(M-1)!}\exp\left(-\frac{\Upsilon_{\Sigma,\mathrm{B}}}{\tilde{\Gamma}_\mathrm{B}}\right)\mathrm{d}\Upsilon_{\Sigma,\mathrm{B}}\overset{(a)}{=}$$

$$\frac{1}{\ln 2}\int_B^{+\infty}\frac{1}{1+\Upsilon_{\Sigma,\mathrm{B}}}\exp\left(-\frac{\Upsilon_{\Sigma,\mathrm{B}}}{\tilde{\Gamma}_\mathrm{B}}\right)\sum_{k=1}^{M}\frac{1}{(k-1)!}\cdot$$

$$\left(\frac{\Upsilon_{\Sigma,\mathrm{B}}}{\tilde{\Gamma}_\mathrm{B}}\right)^{k-1}\mathrm{d}\Upsilon_{\Sigma,\mathrm{B}}=\frac{1}{\ln 2}\int_D^{+\infty}\frac{1}{\tilde{\Gamma}_\mathrm{B}x}\exp\left(-\frac{\tilde{\Gamma}_\mathrm{B}x-1}{\tilde{\Gamma}_\mathrm{B}}\right)\cdot$$

$$\sum_{k=1}^{M}\frac{1}{(k-1)!}\left(\frac{\tilde{\Gamma}_\mathrm{B}x-1}{\tilde{\Gamma}_\mathrm{B}}\right)^{k-1}\tilde{\Gamma}_\mathrm{B}\mathrm{d}x=$$

$$\frac{1}{\ln 2}\exp\left(\frac{1}{\tilde{\Gamma}_\mathrm{B}}\right)\sum_{k=1}^{M}\frac{1}{(k-1)!}\int_D^{+\infty}\frac{1}{x}\exp(-x)\cdot$$

$$\sum_{m=0}^{k-1}\frac{(k-1)!x^m(-1)^{k-1-m}}{m!(k-1-m)!\tilde{\Gamma}_\mathrm{B}^{k-1-m}}\mathrm{d}x=\frac{1}{\ln 2}\exp\left(\frac{1}{\tilde{\Gamma}_\mathrm{B}}\right)\cdot$$

$$\sum_{k=1}^{M}(-1)^{k-1}\sum_{m=0}^{k-1}\frac{(-1)^m}{m!(k-1-m)!\tilde{\Gamma}_\mathrm{B}^{k-1-m}}\cdot$$

$$\int_D^{+\infty}x^{m-1}\exp(-x)\mathrm{d}x=\frac{1}{\ln 2}\exp\left(\frac{1}{\tilde{\Gamma}_\mathrm{B}}\right)\cdot$$

$$\sum_{k=1}^{M}(-1)^{k-1}\left(\frac{\mathrm{Ei}(D)}{(k-1)!\tilde{\Gamma}_\mathrm{B}^{k-1}}+\right.$$

$$\left.\sum_{m=1}^{k-1}\frac{(-1)^m\exp(-D)}{m(k-1-m)!\tilde{\Gamma}_\mathrm{B}^{k-1-m}}\sum_{n=0}^{m-1}\frac{D^{m-1-n}}{(m-1-n)!}\right) \tag{16}$$

式中：步骤(a)由分布积分法得到，$D=(1+B)\tilde{\Gamma}_\mathrm{B}^{-1}$，$\mathrm{Ei}(D)=\int_D^{+\infty}x^{-1}\exp(-x)\mathrm{d}x$ 为指数积分函数。

当 $M=1$ 时，系统模型退化为 SISO 窃听信道，根据式(16)可以得到相应的系统保密容量为

$$\bar{R}_\mathrm{S}^{1}=\frac{1}{\ln 2}\exp\left(\frac{1}{\tilde{\Gamma}_\mathrm{B}}\right)\mathrm{Ei}(D) \tag{17}$$

该 SISO 信道将作为参考标准在下面的仿真中与本文 SIMO 窃听信道进行对比。

3　仿真结果

本节通过数值仿真的方法来比较文献[14]中的 BSISO 系统与本文中的 SIMO 系统在自适应保密速率方案下的保密吞吐量，并证明 SIMO 系统对提升无线通信物理层安全的有效性。在本文仿真中设 $P=0$ dB，$\Gamma_\mathrm{B}=5$ dB，$\Gamma_\mathrm{E}=0$ dB。

首先来看保密吞吐量随保密中断概率变化的情况。Eve 天线数固定为 $N=5$，Bob 天线数分别取 3、5、7，图 2 给出了这 3 种条件下的 SIMO 系统以及 SISO 系统保密吞吐量的差异。由图 2 可见，当发射天线数少于窃听天线数时(图中 $M=3$)，SISO 系统的保密吞吐量略优于 SIMO 系统，且保密中断概率 ε 越小，二者之间的差异越小。当发射天线数等于窃听天线数时(图中 $M=5$)，无论保密中断概率 ε 取何值，SIMO 系统的保密吞吐量均显著大于 SISO 系统的保密吞吐量。二者之间的差异在保密中断概率 ε 取较大值时稍微有所减小。当发射天线数大于窃

听天线数时(图中 $M=7$),与前述其他 3 种情况相比,系统的保密吞吐量均有显著提高。可见,增加合法接收端的接收天线数,可以提高无线窃听信道的保密吞吐量。

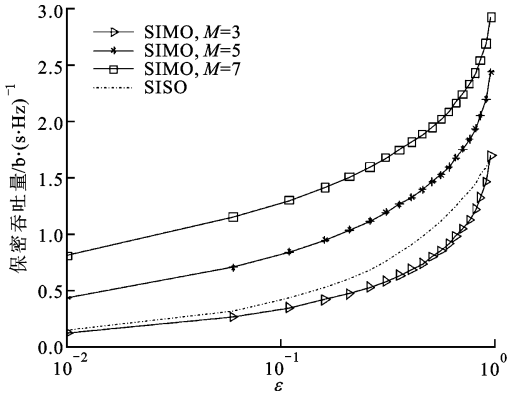

图 2 $N=5$ 时保密吞吐量随保密中断概率的变化

由于接收天线数与窃听天线数会影响 SIMO 系统的保密吞吐量,所以本文在仿真中研究了不同保密中断概率情况下 SIMO 系统的保密吞吐量随接收天线数变化的情况。图 3 给出了固定 $N=3$,在保密中断概率 ε 分别为 0.01、0.1、0.5 时,SIMO 系统的保密吞吐量随接收天线数变化的情况。由图 3 可见,在保密中断概率 ε 的所有 3 种取值条件下,SIMO 系统的保密吞吐量均随着接收天线数的增加而增大。

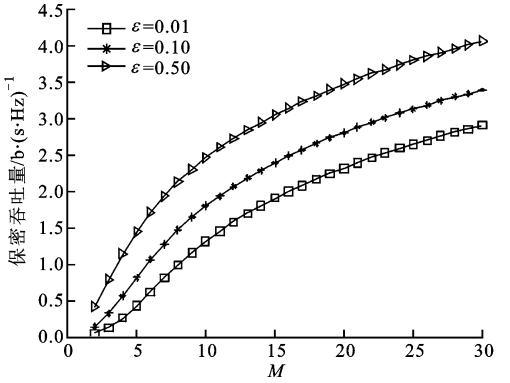

图 3 $N=3$ 时 SIMO 系统的保密吞吐量随 Bob 端天线数的变化

为了进一步研究 Bob 端天线数与 Eve 端天线数同时变化对 SIMO 系统的保密吞吐量的影响,设 $\beta=\dfrac{M}{N}$,观察 β 取不同值时保密吞吐量随窃听天线数的变化情况。图 4 给出了 β 分别取 0.5、1.0、1.5 时,3 种条件下保密吞吐量随窃听天线数的变化情况,其中保密中断概率 ε 分别为 0.01 和 0.05,同时给出了文献[12]中的 SISO 系统的保密吞吐量作为参考。由图 4 可见,在 $\varepsilon=0.01$ 时,当 Bob 端天线数少于 Eve 端天线数(图中 $\beta=0.5$)时,若窃听天线数较少,SISO 系统的保密吞吐量略优于 SIMO 系统。若窃听天线数较多(例如 $N>20$),SIMO 系统的保密吞吐量将优于 SISO 系统。当 Bob 端天线数不少于 Eve 端天线数(图中 $\beta=1.0,1.5$)时,无论窃听天线数为多少,SIMO 系统的保密吞吐量均显著高于 SISO 系统的保密吞吐量。在 $\varepsilon=0.05$、$\beta=0.5$ 时,开始时 SISO 系统的保密吞吐量优于 SIMO 系统,但随着 2 个接收端天线数的增加,SIMO 系统的保密吞吐量将逐渐超过 SISO 系统的保密吞吐量(例如 $N>50$)。可见,增加接收端天线数对提高无线通信物理层安全是有好处的,即使 Eve 端接收天线数超过 Bob 端的接收天线数,当 Bob 端的接收天线数多于一定数量时仍能取得比 SISO 系统更高的保密吞吐量,且中断概率越大,SIMO 系统要获得高于 SISO 系统的保密吞吐量所需的合法接收端天线数就越多。这是因为 SISO 系统的门限值 A 由 $\exp\left(-\dfrac{A}{\widetilde{\Gamma}_{\mathrm{E}}}\right)-\varepsilon=0$ 决定,而 SIMO 系统的门限值 B 由 $\exp\left(-\dfrac{B}{\widetilde{\Gamma}_{\mathrm{E}}}\right)\sum_{k=1}^{N}\dfrac{1}{(k-1)!}\left(\dfrac{B}{\widetilde{\Gamma}_{\mathrm{E}}}\right)^{k-1}-\varepsilon=0$ 决定,随着 ε 的增大,A 收敛于 0 的速度大于 B,因而 SIMO 系统要获得与 SISO 系统相同的保密吞吐量,就需要更多的接收端天线数来弥补发射门限的劣势。

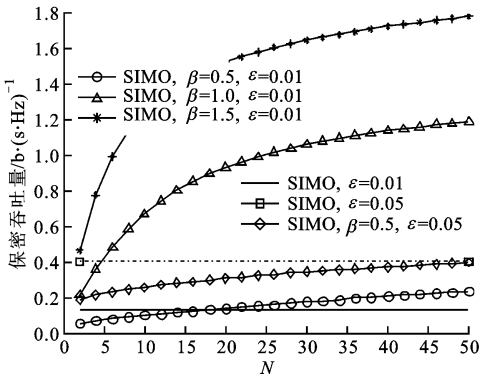

图 4 SIMO 系统的保密吞吐量随 Eve 端天线数的变化

4 结 论

本文研究了基于保密中断概率的慢衰落无线通信系统的物理层安全问题。与以往研究工作不同的是,本文将自适应保密速率方案扩展到 SIMO 系统,并给出了确定发射门限的算法。仿真结果表明:当合法接收端天线数不少于窃听端天线数时,无论保密中断概率取何值,SIMO 系统的保密吞吐量均

显著高于 SISO 系统的保密吞吐量；若窃听端接收天线数超过接收端的接收天线数，当接收端的接收天线数多于一定数量时也能取得比 SISO 系统更高的保密吞吐量。因此，只要合法接收端的天线数足够多，SIMO 系统的保密吞吐量会得到显著提升。考虑到未来蜂窝移动通信系统中的基站端将会配置大规模的天线阵列，本文方法对提高该系统的上行保密吞吐量提供了理论支持。另一方面，蜂窝移动通信的上行过程是多用户通信中一种典型的多接入通信过程，如何将本文单用户 SIMO 系统推广到多用户接入，从而进一步提高系统的保密吞吐量，将是我们下一步需要研究并解决的问题。

参考文献：

[1] SHIN M，MA J，MISHRA A，et al. Wireless network security and interworking [J]. Proceedings of the IEEE，2006，94(2)：455-433.

[2] PAHAN A S K，LEE H W，HONG C S. Security in wireless sensor networks：issues and challenges [C]// Proceedings of the 8th International Conference on Advanced Communication Technology. Piscataway，NJ，USA：IEEE，2006：1043-1048.

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

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

[5] KHISTI A，WORNELL G. Secure transmission with multiple antennas：I　The MISOME wiretap channel [J]. IEEE Transactions on Information Theory，2010，56(6)：3088-3104.

[6] KHISTI A，WORNELL G. Secure transmission with multiple antennas：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 Information Theory，2011，57(8)：4961-4972.

[8] 殷勤业，贾曙乔，左莎琳，等. 分布式多天线跳空收发技术：I [J]. 西安交通大学学报，2013，47(1)：1-6.
YIN Qinye，JIA Shuqiao，ZUO Shalin，et al. A distributed multi-antenna space hopping transceiver technique：I [J]. Journal of Xi'an Jioatong University，2013，47(1)：1-6.

[9] 殷勤业，张建国，郑通兴，等. 分布式多天线跳空收发技术：II　权值反馈型反向训练模式下的 0/1 跳空技术 [J]. 西安交通大学学报，2013，47(6)：1-5.
YIN Qinye，ZHANG Jianguo，ZHENG Tongxing，et al. A distributed multi-antenna space hopping transceiver technique：part II　0/1 space hopping technique in backward training mode with weight-feedback [J]. Journal of Xi'an Jioatong University，2013，47(6)：1-5.

[10] LIANG Yingbin，POOR H，SHAMAI S. Secure communication over fading channels [J]. IEEE Transactions on Information Theory，2008，54(6)：2470-2492.

[11] GOPALA P K，LAI Lifeng，GAMAL H E. On the secrecy capacity of fading channels [J]. IEEE Transactions on Information Theory，2008，54(10)：4687-4698.

[12] BARROS J，RODRIGUES M. Secrecy capacity of wireless channels [C]// Proceedings of 2006 IEEE International Symposium on Information Theory. Piscataway，NJ，USA：IEEE，2006：356-360.

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

[14] MU Pengcheng，YANG Peizhi，WANG Bo，et al. A new scheme to improve the secrecy throughput under the constraints of secrecy outage probability and average transmit power [C] // Proceedings of IEEE ICC2014 WS-WPLS. Piscataway，NJ，USA：IEEE，2014：777-782.

[本刊相关文献链接]

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]

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]

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]

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]

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]

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]

（编辑　刘杨）