

## 基于天线选择与协作通信联合的物理层安全增强方法

姚艳军<sup>1</sup>, 周武旻<sup>1</sup>, 寇保华<sup>2</sup>, 范丹丹<sup>2</sup>

(1.中国科学技术大学,安徽合肥 230026;2.空天宽带网络技术重点实验室,北京 100094)

**摘要:**目前物理层安全研究大多假设用户是静止的,并未考虑其移动性对安全性能所造成的影响,为此提出一种联合天线选择(TAS)与协作通信(Cop)的物理层安全传输方法 TAS-Cop.首先,两个彼此相隔一定距离的基站都具有多根天线,利用天线选择技术,每个基站都选择能使合法接收用户信噪比最大的天线发送保密信息;其次,当用户在两个基站覆盖范围内移动时,彼此之间通过协作以寻求最佳的安全性能.在此基础上推导了瑞利衰落信道下的非零安全容量概率和容量中断概率的闭式表达,并设计了基站之间的最佳功率分配策略.仿真结果表明,与已有的 TAS 方法相比, TAS-Cop 能更有效地满足当用户移动时的安全性能.

**关键词:**物理层安全;天线选择;协作通信

**中图分类号:** TN929.5      **文献标识码:** A      doi:10.3969/j.issn.0253-2778.2017.08.010

**引用格式:** 姚艳军,周武旻,寇保华,等. 基于天线选择与协作通信联合的物理层安全增强方法[J]. 中国科学技术大学学报,2017,47(8):323-330.

YAO Yanjun, ZHOU Wuyang, KOU Baohua, et al. Joint antenna selection and cooperative communication design to enhance physical layer security[J]. Journal of University of Science and Technology of China, 2017,47(8):323-330.

### Joint antenna selection and cooperative communication design to enhance physical layer security

YAO Yanjun<sup>1</sup>, ZHOU Wuyang<sup>1</sup>, KOU Baohua<sup>2</sup>, FAN Dandan<sup>2</sup>

(1. Key Lab. of Wireless-Optimal Communications, University of Science and Technology of China, Hefei 230026, China;  
2. Key Laboratory of Aerospace Broadband Network Technology, Beijing 100094, China)

**Abstract:** The prevailing research on physical layer security assumes that users are static, while takes no account of user mobility. In view of user mobility, a novel transmit antenna selection and cooperative communication design (TAS-Cop) to enhance physical layer security was proposed. The scenario considered contains two cooperative base stations, which are equipped with multiple antennas respectively. Firstly, both of the two transmitters apply TAS technology to maximize the signal to noise ratio (SNR) at the legal receiver. Next, when the legal receiver moves in the coverage of the two base stations, the transmitters cooperate with each other such that the best security performance can be acquired. Based on Rayleigh fading channel, key security metrics such as the closed-form expressions for non-zero secrecy capacity probability and secrecy outage probability were derived. Following that, an optimal power allocation strategy between the two transmitters was presented. Numerical simulation results show that

收稿日期:2016-09-26;修回日期:2016-11-07

基金项目:国家自然科学基金(61461136002)资助.

作者简介:姚艳军,男,1986年生,博士生.研究方向:物理层安全研究. E-mail yaoyanj@mail.ustc.edu.cn

通讯作者:周武旻,博士/教授. E-mail: wyzhou@ustc.edu.cn

the proposed scheme can achieve better security performance when compared with existing TAS schemes with user mobility is taken into consideration.

**Key words:** physical layer security; antenna selection; cooperative communication

## 0 引言

无线信道的广播特性使得当系统存在恶意窃听用户时,安全传输就显得尤为重要.有效的通信不仅要使信息准确无误地传递给接收方,还要能尽量避免窃听用户窃取有用信息.现有的安全机制大多数基于上层的鉴权和密钥加密方法<sup>[1]</sup>,然而传统的鉴权和加密安全方法需要物理层提供一条畅通且无差错的双向对称传输链路.在无线通信中,由于无线媒介的动态特性、终端的移动性、网络的复杂性,都会导致传统的方法在无线通信中难以保证绝对安全.针对无线信道的衰落特性,人们开始研究物理层安全传输方法.物理层安全(physical layer security)最先由 Wyner<sup>[2]</sup>从离散二进制信道提出了安全的基本性能.该文首次提出了保密容量(secretary capacity)的概念,即保证合法接收用户正确恢复信号而窃听用户无法获取有用信息的最大传输速率,得到如下结论:只要窃听用户的信道差于合法用户的信道,就能保证保密容量为正,即存在某种编码方法,使得系统以不大于安全容量速率传输时可保证通信的绝对安全.文献[3]研究了加性白高斯噪声信道和衰落信道下的安全性能.物理层安全的基本原理是充分利用信道的内在动态特性,挖掘主用户信道与窃听用户信道之间的差异性,从而尽可能限制窃听用户从信号中恢复有用信息.文献[4]给出了物理层安全领域的相关研究现状与发展水平.

90年代中后期出现的多人多出(MIMO)技术,由于其具有灵活的天线配置、良好的分集性能等特点,使得 MIMO 技术成为物理层安全领域研究的热点<sup>[5]</sup>.文献[6-7]提出使用发射波束成形(transmit beamforming, TBF)作为物理层安全传输方法,文献[8-10]研究了中继网络中的物理层安全传输方法,文献[11]提出在发射信号中加入人工噪声(artificial noise, AN)来增强安全性能,但是这些技术的应用需要已知精确的信道状态信息.在所有 MIMO 安全传输技术中,发射天线选择(transmit antenna selection, TAS)由于同时只需要一个并行的射频通道<sup>[12]</sup>,因此是一种简单有效的传输方法.文献[13-14]研究了在瑞利衰落信道下最大比合并(maximal ratio combining, MRC)的安全性能.文献[15]研究了在 Nakagami-M 衰落信道、瑞利衰落信

道下,使用通用选择性合并(generalized selection combining, GSC)的安全性能.文献[16]研究了更加广泛的场景,即 TAS/MRC, TAS/SC, TAS/GSC 的安全性能.文献[17-18]提出了联合发端天线选择和收端人工噪声的物理层安全传输方法.文献[19]提出了利用随机天线阵列增强物理层安全的传输方法.上述方法大多数基于 TAS 技术的研究都假设所有用户是静态的,并未考虑用户移动时对安全性能的影响.本文针对现有研究的不足,为了应对用户移动性带来的影响,提出了联合天线选择和协作通信(TAS-Cop)的安全传输方法.相比较现有文献,本文的贡献如下:

(I)提出了“无缝安全(seamless security)”的概念,考虑了用户在不同位置时的安全性能,即当用户在多个小区间穿越时保证安全性能始终达到预定的指标;

(II)在假设主信道、窃听信道都服从瑞利衰落的条件下,推导了合法用户、窃听用户信噪比的概率密度表达式,接着推导出非零安全容量概率、容量中断概率的闭式表达;

(III)提出了协作者之间最优的发射功率分配策略.

## 1 系统模型和方案描述

系统包含两个发射机(Alice1,2),一个合法接收用户(Bob),一个窃听用户(Eve).两个发射机分别具有  $N_{a1}, N_{a2}$  根天线,两个接收用户各有一根天线.两个发射机之间合作以增强物理层的安全性能,并且接收用户具备同时与两个发射机通信的能力,如在蜂窝移动通信中的软切换场景,两个基站(Alice1,2)分别使用不同的扩频码(码分多址)与 Bob 通信.整个系统模型如图 1 所示.

图 1 中,  $h_{b1}h_{b2}$  表示两个发射机与合法接收用户之间的信道系数向量,  $h_{e1}h_{e2}$  表示两个发射机与窃听用户之间的信道系数向量;同时假设信道之间是独立的,且服从瑞利快衰落,即每个快衰落内衰落系数是不变的,块与块之间衰落是独立的.在整个通信过程中, Bob 和 Alice1,2 分别交互能选择接收端信噪比最大的天线序号.具体地, Bob 利用 Alice1,2 在每帧开始发送的导频序列进行信道估计,执行天线选择后再反馈选择的结果.由于 Bob 和 Eve 之间

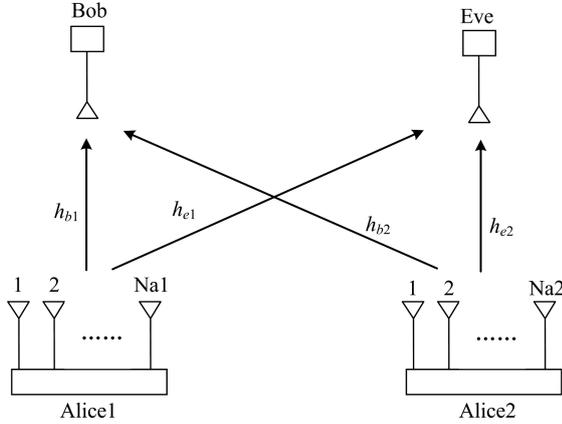


图 1 联合天线选择与协作通信安全系统框图  
Fig.1 The system of transmit antenna selection and cooperative communication

的信道是独立的,对于 Bob 来说是最优的天线,则对 Eve 并不一定是最优的。

经过天线选择后, Alice1,2 分别利用所选择的最佳天线发射有用信号  $x_1, x_2$ , 两个发射信号含有相同的原始信息.在 Bob 处接收到的信号可以如下表示:

$$y_b = \sqrt{P_1 \kappa_{b1}} h_{b1} x_1 + \sqrt{P_2 \kappa_{b2}} h_{b2} x_2 + n_b \quad (1)$$

式中,  $P_1, P_2$  为 Alice1,2 的发射功率,  $\kappa_{b1} = d_{b1}^{-\alpha}$ ,  $\kappa_{b2} = d_{b2}^{-\alpha}$  代表 Alice1,2 到 Bob 的路径损耗因子,  $d_{b1}, d_{b2}$  表示 Alice1,2 到达 Bob 的距离,  $\alpha$  为路损指数<sup>[13]</sup>.  $h_{b1}, h_{b2}$  为标量, 分别表示 Alice1,2 所选天线到达 Bob 的信道衰落值.另外,  $n_b$  表示 Bob 接收到的加性噪声.在 Eve 处接收到的信号表示如下:

$$y_e = \sqrt{P_1 \kappa_{e1}} h_{e1} x_1 + \sqrt{P_2 \kappa_{e2}} h_{e2} x_2 + n_e \quad (2)$$

式中所有参数物理意义与式(1)中类似。

## 2 安全性能分析

### 2.1 Bob 和 Eve 的信噪比概率密度

#### 2.1.1 Bob 的信噪比概率密度

Bob 和 Eve 都使用最大比合并的方法接收两个发射机的信号,因此, Bob 处接收信号的瞬时信噪比可以表示为

$$\gamma_b = \gamma_{b1} + \gamma_{b2} \quad (3)$$

式中,  $\gamma_{bi} = P_i \kappa_{bi} |h_{bi}|^2 / \sigma_b^2$  ( $i=1,2$ ).

平均信噪比  $\bar{\gamma}_{bi} = P_i \kappa_{bi} E[|h_{bi}|^2] / \sigma_b^2$  ( $i=1,2$ ), 其中  $E(\cdot)$  表示统计变量的期望.由文献[14]可得,  $\gamma_{bi}$  ( $i=1,2$ ) 的概率密度函数为

$$f_{\gamma_{bi}}(\gamma_{bi}) = \frac{N_{ai}}{\bar{\gamma}_{bi}} \cdot \exp\left(-\frac{\gamma_{bi}}{\bar{\gamma}_{bi}}\right) \cdot$$

$$\left[1 - \exp\left(-\frac{\gamma_{bi}}{\bar{\gamma}_{bi}}\right)\right]^{N_{ai}-1} \quad (4)$$

根据式(3)以及两个变量和的概率密度函数性质,可得 Bob 处接收信号的信噪比概率密度表达式  $f_{\gamma_b}(\gamma_b)$ . 通过基本推导,可得

$$f_{\gamma_b}(\gamma_b) = \frac{N_{a1}}{\bar{\gamma}_{b1}} \cdot \frac{N_{a2}}{\bar{\gamma}_{b2}} \sum_{i=0}^{N_{a1}-1} \sum_{k=0}^{N_{a2}-1} M_{ik} \cdot y(\gamma_b) \quad (5)$$

式中,  $M_{ik} = C_{N_{a1}-1}^i C_{N_{a2}-1}^k (-1)^{N_{a1}+N_{a2}-2-i-k}$ ,  $y(\gamma_b)$  的表达式如下:

$$y(\gamma_b) = \begin{cases} \frac{1}{e_k - d_i} [\exp(-d_i \gamma_b) - \exp(-e_k \gamma_b)], & e_k \neq d_i \\ \gamma_b \exp(-d_i \gamma_b), & e_k = d_i \end{cases} \quad (6)$$

式中, 记  $d_i = \frac{N_{a1} - i}{\bar{\gamma}_{b1}}$ ,  $e_k = \frac{N_{a2} - k}{\bar{\gamma}_{b2}}$ .

#### 2.1.2 Eve 的信噪比概率密度

由于 Eve 也使用最大比合并,因此 Eve 处接收信号的信噪比表达式为

$$\gamma_e = \gamma_{e1} + \gamma_{e2} \quad (7)$$

式中,  $\gamma_{ei} = P_i \kappa_{ei} |h_{ei}|^2 / \sigma_e^2$  ( $i=1,2$ ).平均信噪比  $\bar{\gamma}_{ei} = P_i \kappa_{ei} E[|h_{ei}|^2] / \sigma_e^2$  ( $i=1,2$ ).由文献[14]可得  $\gamma_{ei}$  ( $i=1,2$ ) 的概率密度函数为

$$f_{\gamma_{ei}}(\gamma_{ei}) = \frac{1}{\bar{\gamma}_{ei}} \cdot \exp\left(-\frac{\gamma_{ei}}{\bar{\gamma}_{ei}}\right) \quad (8)$$

按照  $\bar{\gamma}_{e1} \leq \bar{\gamma}_{e2}$  顺序排列信噪比可得

$$f_{\gamma_e}(\gamma_e) = \begin{cases} \frac{\gamma_e}{\bar{\gamma}_{e1}^2} \cdot \exp\left(-\frac{\gamma_e}{\bar{\gamma}_{e1}}\right), & \bar{\gamma}_{e1} = \bar{\gamma}_{e2} \\ \exp\left(-\frac{\gamma_e}{\bar{\gamma}_{e1}}\right) \\ \frac{\gamma_e}{\bar{\gamma}_{e2} - \bar{\gamma}_{e1}} \cdot \gamma(1, a\gamma_e), & \bar{\gamma}_{e1} < \bar{\gamma}_{e2} \end{cases} \quad (9)$$

证明 当  $\bar{\gamma}_{e1} = \bar{\gamma}_{e2}$  时,由两个变量和的概率密度性质可得

$$\begin{aligned} f_{\gamma_e}(\gamma_e) &= f_{\gamma_{e1}}(\gamma_{e1}) * f_{\gamma_{e2}}(\gamma_{e2}) = \\ &F^{-1}(Y_1(\bar{\omega}) \cdot Y_2(\bar{\omega})) = F^{-1}(Y_1^2(\bar{\omega})) = \\ &F^{-1}\left[\frac{1}{\bar{\gamma}_{e1}^{2N_e} \cdot (N_e - 1)!} \cdot \frac{1}{\left(\frac{1}{\bar{\gamma}_{e1}} + j\bar{\omega}\right)^{2N_e}}\right] = \\ &\frac{\gamma_e}{\bar{\gamma}_{e1}^2} \cdot \exp\left(-\frac{\gamma_e}{\bar{\gamma}_{e1}}\right) \end{aligned} \quad (10)$$

式中,  $*$  表示卷积运算,  $F^{-1}$  表示傅里叶反变换,  $Y_1(\bar{\omega}), Y_2(\bar{\omega})$  为两个变量的傅里叶变换。

当  $\bar{\gamma}_{e1} < \bar{\gamma}_{e2}$  时,由基本的概率密度运算可得

$$f_{\gamma_e}(\gamma_e) = \int_0^{\gamma_e} f_{\gamma_{e1}}(\gamma_{e1}) \cdot f_{\gamma_{e2}}(\gamma_e - \gamma_{e1}) d\gamma_{e1} = \int_0^{\gamma_e} \frac{1}{\bar{\gamma}_{e1}} \cdot \exp\left(-\frac{\gamma_{e1}}{\bar{\gamma}_{e1}}\right) \cdot \frac{1}{\bar{\gamma}_{e2}} \cdot \exp\left(-\frac{\gamma_e - \gamma_{e1}}{\bar{\gamma}_{e2}}\right) d\gamma_{e1},$$

$$\frac{\exp\left(-\frac{\gamma_e}{\bar{\gamma}_{e2}}\right)}{\bar{\gamma}_{e2} - \bar{\gamma}_{e1}} \cdot \gamma(1, a\gamma_e) \quad (11)$$

式中,  $\gamma(\cdot)$  表示 lower incomplete gamma 函数<sup>[20]</sup>,

$$a = \frac{1}{\bar{\gamma}_{e1}} - \frac{1}{\bar{\gamma}_{e2}}.$$

$$\Pr(C_s > 0) =$$

$$\left\{ \begin{array}{l} \frac{N_{a1} N_{a2}}{\bar{\gamma}_{b1} \bar{\gamma}_{b2} \bar{\gamma}_{e1} \bar{\gamma}_{e2}} \cdot \sum_{i=0}^{N_{a1}-1} \sum_{k=0}^{N_{a2}-1} \left[ \frac{M_{ik} \bar{\gamma}_{e1} \bar{\gamma}_{e2}}{d_i e_k} - \frac{M_{ik} \bar{\gamma}_{e2}^3}{a(1+e_k \bar{\gamma}_{e2})(1+d_i \bar{\gamma}_{e2})} + \frac{M_{ik} \bar{\gamma}_{e1}^3}{a(1+e_k \bar{\gamma}_{e1})(1+d_i \bar{\gamma}_{e1})} \right], \bar{\gamma}_{e1} < \bar{\gamma}_{e2} \\ \frac{N_{a1} N_{a2}}{\bar{\gamma}_{b1} \bar{\gamma}_{b2}} \cdot \sum_{i=0}^{N_{a1}-1} \sum_{k=0}^{N_{a2}-1} \left[ \frac{M_{ik}}{e_k d_i} - M_{ik} \bar{\gamma}_{e1}^2 \frac{3+2\bar{\gamma}_{e1}(e_k+d_i)+d_i e_k \bar{\gamma}_{e1}^2}{(e_k \bar{\gamma}_{e1}+1)^2 (d_i \bar{\gamma}_{e1}+1)^2} \right], \bar{\gamma}_{e1} = \bar{\gamma}_{e2} \end{array} \right. \quad (14)$$

见文后附录

**证明** 首先将式(5),(9)代入(13),利用文献[20]中公式 eq(1.111)进行二项式展开;然后用积分基本的性质,就可以得到式(14)的最终结果.

### 2.3 容量中断概率

容量中断概率为:  $P_{\text{out}}(R_s) = \Pr(C_s < R_s)$ , 具体由下式计算得出

$$P_{\text{out}}(R_s) = \Pr(C_s < R_s | \gamma_b > \gamma_e) \cdot \Pr(\gamma_b > \gamma_e) + \Pr(C_s < R_s | \gamma_b < \gamma_e) \cdot \Pr(\gamma_b < \gamma_e) \quad (15)$$

式中,  $R_s > 0$  为非零安全容量. 当  $\gamma_b < \gamma_e$  且  $R_s > 0$  时,  $C_s = 0$ , 因此  $\Pr(C_s < R_s | \gamma_b < \gamma_e) = 1$ . 同时,  $\Pr(\gamma_b < \gamma_e)$  可由式(14)得到. 式(15)中的第一项经过推导, 得到

$$\Pr(C_s < R_s | \gamma_b > \gamma_e) \cdot \Pr(\gamma_b > \gamma_e) = \int_0^{+\infty} \int_{\gamma_e}^{2R_s \cdot (1+\gamma_e)-1} f_{\gamma_e}(\gamma_e) \cdot f_{\gamma_b}(\gamma_b) d\gamma_b d\gamma_e =$$

$$\left\{ \begin{array}{l} \frac{N_{a1} N_{a2}}{\bar{\gamma}_{b1} \bar{\gamma}_{b2} \bar{\gamma}_{e1} \bar{\gamma}_{e2}} \cdot (X_1 - X_2 - X_3 + X_4), \bar{\gamma}_{e1} < \bar{\gamma}_{e2} \\ \frac{N_{a1} N_{a2}}{\bar{\gamma}_{b1} \bar{\gamma}_{b2} \bar{\gamma}_{e1} \bar{\gamma}_{e2}} \cdot (X'_1 - X'_2 - X'_3 + X'_4), \bar{\gamma}_{e1} = \bar{\gamma}_{e2} \end{array} \right. \quad (16)$$

**证明** 首先将式(5),(9)代入(16),利用文献[20]中公式 eq(1.111)进行二项式展开,然后用积分基本的性质,同时利用文献[20]中公式 eq(6.455), 就可以得到式(16)的最终结果. 为了使文章表达结构合理, 式(16)中  $X_1, X_2, X_3, X_4, X'_1, X'_2, X'_3,$

### 2.2 非零安全容量概率

非零安全容量定义如下:

$$C_s = [\log(1 + \gamma_b) - \log(1 + \gamma_e)]^+ \quad (12)$$

式中,  $[x]^+$  表示  $\max\{0, x\}$ . 非零安全容量通过计算下式得到

$$\Pr(C_s > 0) = \Pr(\gamma_b > \gamma_e) = \int_0^{+\infty} \int_0^{\gamma_b} f_{\gamma_b}(\gamma_b) \cdot f_{\gamma_e}(\gamma_e) d\gamma_e d\gamma_b \quad (13)$$

非零安全容量最终表达式由下式给出

$X'_4$  的具体表达式不在此展开, 有兴趣的作者可与作者或编辑部联系.

### 2.4 最佳功率分配

本文所提出的协作通信联合方法目的是为了寻求两个发射机最佳的功率分配  $P_1, P_2$ , 使得物理层安全性能达到最佳, 也即最小化容量中断概率. 最佳的功率分配策略可由下式求得

$$\left. \begin{array}{l} \min_{P_1, P_2} P_{\text{out}}(R_s) \\ P_1 \geq 0 \\ \text{subject to } P_2 \geq 0 \\ P_1 + P_2 \leq P \end{array} \right\} \quad (17)$$

式中,  $P$  是两个发射机总的发射功率. 由于  $P_{\text{out}}(R_s)$  的表达式非常复杂, 并且随着 Alice1,2 发射天线数量的变化, 其单调性也不断变化, 并不是恒定的, 因此不易求得  $P_1, P_2$  的闭式表达, 但可以通过计算机数值分析的方法, 简单有效地求出  $P_1, P_2$  的功率分配.

## 3 仿真实验

图 2 和图 3 分别分析了非零安全容量概率  $\Pr(C_s > 0)$  和容量中断概率  $P_{\text{out}}(R_s)$  随  $\bar{\gamma}_{b1}, N_{a1}, N_{a2}, N_e$  不同取值的变化情况. 除了在图中标明的参数外, 仿真参数选取如下:  $\bar{\gamma}_{b2} = -5$  dB,  $\bar{\gamma}_{e1} = 0$  dB,  $\bar{\gamma}_{e2} = 5$  dB. 由图 2 可以看出,  $\Pr(C_s > 0)$  随着  $\bar{\gamma}_{b1}$  或  $N_{a1}$  的增加而增大, 这是因为信噪比提升或天线数

量增加自然会带来安全性能的提升.另外,随着  $N_e$  的增加,安全性能随之恶化,这是因为窃听用户的窃听能力随之增加.图 3 分析了在安全速率  $R_s = 1$  时,容量中断概率  $P_{out}(R_s)$  的性能.由图 3 可以看出,随着  $\bar{\gamma}_{b1}$ ,  $N_{a1}$  或  $N_{a2}$  的增加,  $P_{out}(R_s)$  将随之降低,这也是因为信噪比提升或天线数量增加自然会带来安全性能的提升.另外,随着  $N_e$  的增加,  $P_{out}(R_s)$  将随之增加.最后,在图 2 和图 3 中,本文还利用蒙特拉罗仿真分析了安全性能,在图中用“仿真”标记.由图 2,3 可以看出,理论分析与仿真结果相吻合,证明了理论推导的正确性.

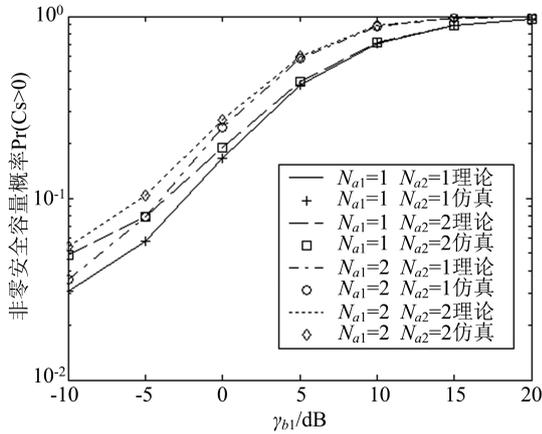


图 2 非零安全容量概率  $\Pr(C_s > 0)$  vs.  $\bar{\gamma}_{b1}$ ,

Fig.2 Nonzero safety capacity probability  $\Pr(C_s > 0)$  vs.  $\bar{\gamma}_{b1}$

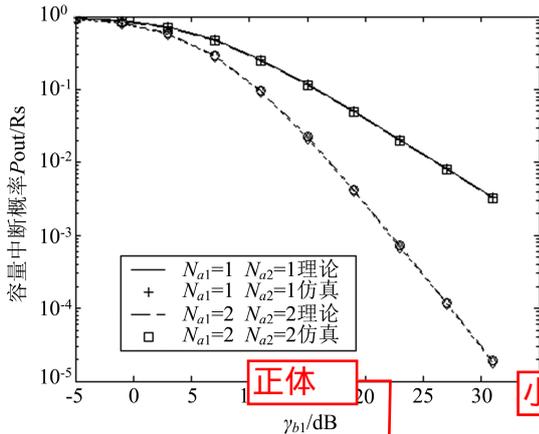


图 3 容量中断概率  $P_{out}(R_s)$  vs.  $\bar{\gamma}_{b1}$

Fig.3 Capacity outage probability  $P_{out}(R_s)$  vs.  $\bar{\gamma}_{b1}$

图 4 设置了一个典型的用户移动仿真场景,所有用户都位于二维坐标系中.具体地说, Alice1,2, Eve 的坐标分别为  $(-2.5, 0)$ ,  $(2.5, 0)$ ,  $(0, -1)$ . Bob 初始位于  $(-1.5, 0)$  且具有移动性,逐渐移动到坐标  $(1.5, 0)$ .设置这个场景 的目的是为了验证最佳的功率分配情况,并验证用户在移动时的安全性能.仿真中,设置如下的参数:  $P = 10$ ,  $\alpha = 4$ ,  $\sigma_b^2 = \sigma_e^2 = 1$ ,

$$E[|h_{b1}|^2] = E[|h_{b2}|^2] = 1, E[|h_{e1}|^2] = E[|h_{e2}|^2] = 1.$$

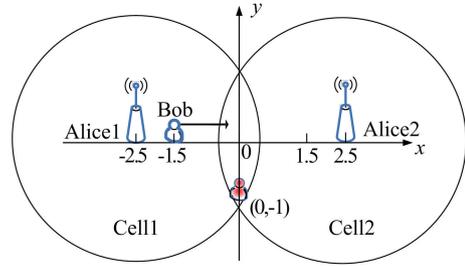


图 4 仿真场景

Fig.4 Simulation scene

图 5 仿真的是随着不同的  $N_{a1}, N_{a2}$ , 最佳的功率分配情况.由图 5 可以看出两个现象,首先在 Bob 向 Alice2 移动的过程中,分配给 Alice2 的功率将越来越多,这是由于 Bob 与 Alice2 之间的距离缩短导致路损减小.当 Alice1 的天线数量多于 Alice2 的天线数量时,更多的功率将被分配给 Alice1,反之亦然.这是因为分配更多的功率给具有更多天线的基站,将获得更多的多天线分集,从而安全性能更优.

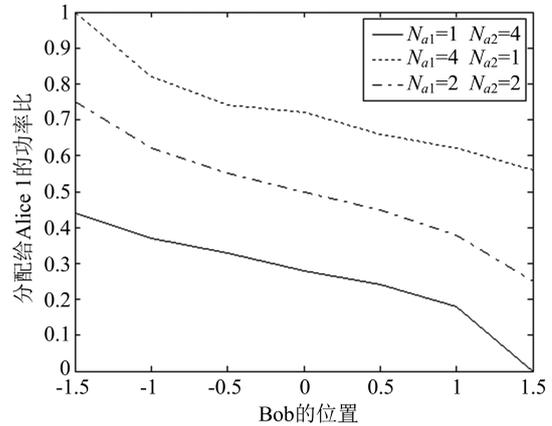


图 5 最佳功率分配策略

Fig.5 Optimal Power allocation strategy

图 6 对比了本文提出的安全传输方法与文献 [3] 中的方法,分别以 TAS-Cop 和 TAS-without Cop 标志.为了在同等条件下比较本文提出的方法与现有方法的性能,便于读者理解,首先对 TAS-Without Cop 方法加以说明:该方法同样设置两个基站, Alice1,2, 且具有与 TAS-Cop 具有相同的天线设置.在 Bob 从 Alice1 的小区移动到 Alice2 的小区的过程中, TAS-without Cop 的方法是从两个基站中选择一个基站的一根天线,然后使用全功率发射,即等于 TAS-Cop 方法中 Alice1 和 2 发射功率的总和.由图 6 可以看出,本文的 TAS-Cop 方法性能要优于 TAS-without Cop 方法的性能.另外,在

$N_{a1} = N_{a2} = 2$  的条件下,当 Bob 位于(0,0),即位于两个小区的交叠覆盖区域时,两种方法的性能差距达到最大,这是因为当用户位于两个小区交叠覆盖区域时,宏分集效果最明显,并且这种分集可以通过两个基站的合作完全被利用.当  $N_{a1} = 1, N_{a2} = 4$  时,两种方法的性能差距最大点并不是发生在小区的交叠处,而是在 Alice1 的覆盖小区内,这是因为由于 Alice2 具有更多数量的天线,能力更强.在这种情况下,当 Bob 离 Alice1 更近时,宏分集的效果最明显.由仿真结果可知,在两种方法性能差距最大点处,相较于 TAS-without Cop 方法,本文所提出的 TAS-Cop 方法能把安全容量中断概率从 0.05 降低到 0.003,性能优化了一个数量级.

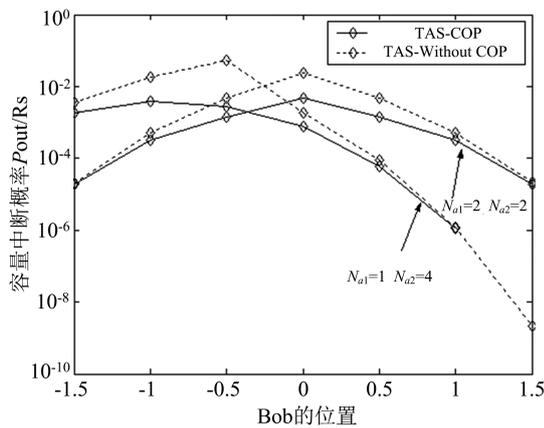


图 6 本文方法 TAS-Cop 与现有文献方法 TAS 的性能比较  
Fig.6 Performance comparison between TAS-cop and TAS

## 4 结论

针对现有物理层安全文献中未及考虑用户移动性带来的影响,本文提出了 TAS-Cop 安全传输新方法.基于该方法,详细推导了非零安全容量概率、容量中断概率的闭式表达.接着,提出了用于合作通信的最佳功率分配策略.仿真结果表明,与现有其他的 TAS 传输策略比较,当考虑到用户移动性时该方法具有更好的安全性能.

插入附录

参考文献 (References)

- [1] MASSEY J L. An introduction to contemporary cryptology [J]. Proceedings of the IEEE, 1988, 76(5): 533-549.
- [2] WYNER A D. The wire-tap channel [J]. Bell System Technical Journal, 2014, 54(8): 1355-1387.
- [3] CHEONG S L Y, HELLMAN M. The Gaussian wire-tap channel [J]. IEEE Transactions on Information Theory, 2003, 24(4): 451-456.
- [4] MUKHERJEE A, FAKOORIAN S A, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: A survey [J]. IEEE Communications Surveys and Tutorials, 2014, 16(3): 1550-1573.
- [5] 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.
- [6] LIAO W C, CHANG T H, MA W K, 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.
- [7] BASHAR S, DING Z, LI G Y. On secrecy of codebook-based transmission beamforming under receiver limited feedback [J]. IEEE Transactions on Wireless Communications, 2011, 10(4): 1212-1223.
- [8] 王东,李永成,白铂,等. 放大转发中继网络中绿色的物理层安全通信技术 [J]. 电子与信息学报, 2016, 38(4): 841-847.
- [9] 雷维嘉,左莉杰,江雪,等. 中继网络中不准确信道状态信息下抗多窃听者的物理层安全方案 [J]. 电子与信息学报, 2015, 37(9): 2191-2197.
- [10] 王鼎宇,付晓梅,厚丽君. 中继行为的物理层安全博弈模型研究 [J]. 南开大学学报, 2015, 5(5): 96-101.
- [11] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.
- [12] SANAYEI S, NOSRATINIA A. Antenna selection in MIMO systems [J]. IEEE Communication Magazine, 2004, 42(10): 68-73.
- [13] ALVE H, SOUZA R D, DEBBAH M, et al. Performance of transmit antenna selection physical layer security schemes [J]. IEEE Signal Processing Letters, 2012, 19(6): 372-375.
- [14] CHEN Z, YUAN J, VUCETIC B. Analysis of transmit antenna selection/maximal-ratio combining in rayleigh fading channels [J]. IEEE Transactions on Vehicular Technology, 2005, 54(4): 1312-1321.
- [15] WANG L F, ELKASHALN M, HUANG J, et al. Secure transmission with antenna selection in MIMO nakagami-m fading channels [J]. IEEE Transactions on Wireless Communications, 2014, 13(11): 6054-6067.
- [16] YANG N, YEOH P L, ELKASHLAN M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels [J]. IEEE Transactions on Wireless Communications, 2013, 61(1): 144-154.
- [17] 张亚军,梁涛,柳永祥,等. 联合发端天线选择和收端人工噪声的物理层安全传输方法 [J]. 电子与信息学报, 2015, 37(9): 2183-2190.
- [18] 邓单,王伟,赵明. 联合天线选择和人工噪声的安全传输技术 [J]. 系统仿真学报, 2016, 28(2): 321-327.
- [19] 洪涛,宋茂忠,王保云. 基于随机天线阵列的物理层安全通信系统峰均功率比问题研究 [J]. 电子与信息学报, 2015, 37(1): 188-192.
- [20] GRADSHTEYN I S, RYZHIK I M. Table of Integrals, Series and Products [M]. San Diego: Elsevier, 2007: 25, 337, 340-341.