安全中断概率约束下MISOME系统安全性能分析

陈 璇,冯友宏
(南京邮电大学 通信与信息工程学院,江苏 南京 210003)

摘 要:针对MISOME系统安全性能问题,考虑发送端硬件条件受限的情况,提出一种利用发端天线选择(TAS)、发端波束成形(TBF)以及安全速率自适应方法的传输方案(TASTBF-adaptive)。安全中断概率(SOP)和有效安全吞吐量(EST)是衡量MISOME系统安全性能的两个重要指标。通过在安全中断概率约束下比较所提方案与传统人工噪声的物理层安全传输方法(AN-adaptive)的EST,分析两系统安全性能和研究影响安全性能的因素。仿真结果表明,在允许的最大SOP减小时,AN-adaptive方法比TASTBF-adaptive方法的安全性和鲁棒性更好;提高AN-adaptive方案安全性能应主要通过增大发送天线数和主信道平均信噪比,而提高TASTBF-adaptive方案安全性能应主要通过减小窃听天线数和窃听信道平均信噪比;TASTBF-adaptive方法中TAS选择多根天线比只选择一根天线安全性能更好。

关键词:物理层安全;有效安全吞吐量;天线选择;波束成形;人工噪声技术
中图分类号:TN918 **文献标识码**:A **文章编号**:1673-629X(2017)02-0076-05
doi:10.3969/j.issn.1673-629X.2017.02.018

Analysis of Security Performance of MISOME System with Security Outage Probability Constraints

CHEN Xuan, FENG You-hong
(College of Communications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: Regarding the security performance of MISOME system, a transmission scheme adopting Transmit Antenna Selection (TAS), Transmit Beamforming (TBF) is proposed as TASTBF-adaptive under the condition of limited hardware at transmitter. As Security Outage Probability (SOP) and Effective Security Throughput (EST) are two principal indicators in MISOME system, the proposed scheme is compared with traditional scheme (AN-adaptive) based on artificial noise technique under the constraint of SOP in order to analyze the security performance and its influence of the two schemes. Numerical results indicate that as the maximum allowed SOP decreases, TASTBF adaptive scheme shows a lower resilience than AN adaptive scheme. The improvement of security performance presents a strong sensitivity to the increase of transmit antennas and the average SNR of main channel in AN adaptive scheme while that in TASTBF adaptive scheme presents a profound sensitivity over the decrease of antennas at eavesdropper and the average SNR of eavesdropper channel. TAS provides better security performance of TASTBF adaptive scheme when using more transmit antennas than just one.

Key words: physical layer security; effective security throughput; transmit antenna selection; beamforming; artificial noise

0 引 言

由于无线信道的广播特性,使得安全问题成为无线网络中的一大挑战。近期物理层安全技术作为传统密码技术的补充被提出[1-2]。物理层安全的核心就在于利用无线信道的物理层特性(如衰落、噪声等),确保目的节点获得的安全信息的信息熵大于窃听者得到的安全信息的信息熵,以实现安全传输,从而为保障信息安全提供了一种全新的思路。要使安全容量非零,合法节点Alice和Bob之间的主信道瞬时信道质量必须比Alice与Eve之间的窃听信道瞬时信道质量要好,也就是主信道瞬时容量 C_B 要大于窃听信道瞬时容量 C_E。

窃听节点的信息率 R_E 是发送的码率 R_B 与安全速率 R 之差。要得到最优安全速率必须满足两个约束条

收稿日期:2016-03-14 **修回日期**:2016-06-16 **网络出版时间**:2017-01-04
基金项目:江苏省高校自然科学研究重大项目(14KJA510003)
作者简介:陈 旋(1991-),女,硕士研究生,研究方向为物理层安全技术;冯友宏,博士研究生在读,副教授,研究方向为协作通信、物理层安全。
网络出版地址:http://www.cnki.net/kcms/detail/61.1450.TP.20170104.1028.060.html

件[3]:$R_B \leqslant C_B$(可靠性约束);$R_E > C_E$(安全性约束)。要计算 C_E,Alice 必须知道窃听信道的瞬时信道状态信息(CSI)。然而在实际通信场景下,由于窃听用户处于被动捕获状态,因此 Alice 无法获得窃听信道的瞬时状态信息,安全性约束 $R_E > C_E$ 无法永远满足。在此情景下,为了保障通信安全进行,利用概率对通信系统进行分析显得非常必要,通过安全中断概率(SOP)来计算不能满足安全性约束的概率[4]。

为了提升安全性能,已经提出了一些信号处理的方法。文中采用三种信号处理技术:发端天线选择技术(TAS)、发端波束成形技术(TBF)和人工噪声技术(AN)。发端天线选择技术既能发挥空间分集的优点,又可以减少用于发射的射频链路,降低硬件成本和复杂度[5-7]。发端选择使合法接收端接收信噪比最大的一些天线发送信息。由于信道的独立性,基于 Bob 最强的信道对于 Eve 可以看作是一种随机信道。因此 TAS 适用于一些发端硬件条件受限的情况。AN 与 TAS 不同,不是通过提高主信道质量而是通过干扰窃听者来提高安全性[8-10]。

文献[8]提出了多输入单输出多天线窃听者(MISOME)系统,用有效安全吞吐量 Ψ 作为系统性能指标,定义 Ψ 为安全速率 R 与能同时满足可靠性和安全性约束的安全传输概率 P_{sec} 的乘积。采用自适应传输方法,已知合法信道的瞬时信噪比就可以自适应地调节 R 使 Ψ 达到最大。将 Ψ 作为目标函数,没有考虑到对 SOP 的约束。仅用 Ψ 衡量系统安全性有不合理之处,因为当系统有效安全吞吐量很大时 SOP 可能很小,Eve 仍有可能窃听到大量信息。文中在此基础上加入对 SOP 的约束[11],建立新的带有 SOP 约束机制的物理层传输方案—AN adaptive 传输方法。

同时,还考虑一种发端天线硬件条件受限的 MISOME 系统。由于发射链路成本和硬件复杂度的限制,不能同时使用发端所有天线发送信息,只能选取部分天线发送。此系统同时利用 TBF 技术提高安全性[12]。通过比较这两个系统的安全性能,进行系统安全性能分析方面的研究。

1　系统模型和传输机制分析

1.1　系统模型

MISOME 窃听信道中,Alice 是有 N 根天线的发送者,Bob 是单天线的合法接收端,Eve 是有 M 根天线的窃听者。在这个窃听系统中,将 Alice 与 Bob 之间的主信道记为 $\boldsymbol{h}$,$\boldsymbol{h} \in C^{1\times N}$。将 Alice 与 Eve 之间的窃听信道记 $\boldsymbol{G}$,$\boldsymbol{G} \in C^{M\times N}$。$\boldsymbol{h}$ 和 $\boldsymbol{G}$ 中的元素都是独立同分布(i.i.d)的瑞利衰落。做以下假设:

(1)假设 $N > M$,因为若是 $N \leqslant M$,Eve 就有能力完全去除人工噪声[8];

(2)在这个窃听信道中 Eve 是被动窃听,Alice 不知道 $\boldsymbol{G}$ 的瞬时信息;

(3)Bob 准确估算 $\boldsymbol{h}$ 并反馈给 Alice。

1.1.1　采用人工噪声技术的 MISOME 系统模型

Alice 同时传送信息信号 s_I 和人工噪声信号 s_N 给 Bob,$s_N \in C^{(N-1)\times 1}$,$s_I$ 的方差是 χ_I,s_N 每个元素的方差是 χ_N。假设 Alice 的总发射功率是 P_T,将功率分配比记为 φ,$\varphi = \dfrac{\text{传输信息所用功率}}{\text{总传输功率}}$,$0 < \varphi \leqslant 1$。因为 $\boldsymbol{G}$ 的信道状态信息对于 A 未知,所以 Alice 将发射功率均匀地分配给 S_N 中的每个元素,$\chi_N = (1-\varphi)P_T/(N-1)$。用波束成形矩阵 $\boldsymbol{V} \in C^{N\times N}$ 传输 s_I 和 s_N,$\boldsymbol{V} = [\boldsymbol{v}_I\ \boldsymbol{V}_N]$,其中 $\boldsymbol{v}_I$ 用来传输 s_I,$\boldsymbol{V}_N$ 用来传输 s_N。$\boldsymbol{V}$ 矩阵通过将 s_N 向除了 Bob 外的各个方向传输来降低窃听信道的信道质量。矩阵 $\boldsymbol{V}$ 是基于 Bob 反馈给 Alice 的 $\boldsymbol{h}$ 来构造的。定义 $\boldsymbol{H} \triangleq \boldsymbol{h}^H\boldsymbol{h}$,并对其进行特征值分解。$\boldsymbol{v}_I$ 作为原则特征向量对应于 $\boldsymbol{H}$ 中的最大特征值,$\boldsymbol{V}_N$ 作为 $\boldsymbol{H}$ 中剩下 $N-1$ 个特征向量,这样 $\boldsymbol{V}_N$ 就在主信道的零空间中。得到 Alice 发送的信号 $\boldsymbol{x} \in C^{N\times 1}$ 为:

$$\boldsymbol{x} = [\boldsymbol{v}_I\boldsymbol{V}_N]\begin{bmatrix} s_I \\ s_N \end{bmatrix} = \boldsymbol{v}_I s_I + \boldsymbol{V}_N s_N \tag{1}$$

根据式(1)可得 Bob 处的接收信号为:

$$\boldsymbol{y} = \boldsymbol{h}\boldsymbol{x} + \boldsymbol{n}_B = \boldsymbol{h}\boldsymbol{v}_I s_I + \boldsymbol{n}_B \tag{2}$$

式(2)中,$\boldsymbol{n}_B$ 是 Bob 处的加性高斯白噪声,方差为 σ_B^2。

基于式(2)可得 Bob 处的瞬时信噪比为:

$$\gamma_B = \varphi\bar{\gamma}_B \parallel \boldsymbol{h} \parallel^2 \tag{3}$$

其中,$\bar{\gamma}_B$ 是主信道的平均信噪比,$\bar{\gamma}_B = P_T/\sigma_B^2$。

根据式(1)得 Eve 处接收到的信号为:

$$\boldsymbol{z} = \boldsymbol{G}\boldsymbol{x} + \boldsymbol{n}_E = \boldsymbol{G}\boldsymbol{v}_I s_I + \boldsymbol{G}\boldsymbol{V}_N s_N + \boldsymbol{n}_E \tag{4}$$

其中,$\boldsymbol{n}_E$ 是 Eve 处的 $M \times 1$ 维高斯加性白噪声向量,满足 $E[\boldsymbol{n}_E\boldsymbol{n}_E^H] = \sigma_E^2\boldsymbol{I}_M$。

可以看出,当 $N > M$ 时 Eve 不能去除 $\boldsymbol{V}_N s_N$ 引起的干扰[13-15],这是因为当 $N > M$ 时 $\boldsymbol{G}\boldsymbol{G}^H$ 是不可逆的。基于式(4)可以求出 Eve 处的瞬时接收信干噪比为[16-17]:

$$\gamma_E = \varphi\boldsymbol{v}_I^H\boldsymbol{G}^H\left(\frac{1-\varphi}{N-1}\boldsymbol{G}\boldsymbol{V}_N\boldsymbol{V}_N^H\boldsymbol{G}^H + \frac{1}{\bar{\gamma}_E}\boldsymbol{I}_M\right)^{-1}\boldsymbol{G}\boldsymbol{v}_I \tag{5}$$

其中,$\bar{\gamma}_E$ 是窃听信道平均信噪比,$\bar{\gamma}_E = P_T/\sigma_E^2$。

因为 Eve 是被动窃听,所以 Alice 不知道 λ_E 的值,在这种情况下 Alice 也不知道 $\boldsymbol{G}$。

1.1.2　采用 TAS 和 TBF 技术的 MISOME 系统模型

与上述采用 AN 技术不同的是,TAS 是从发端 N

根天线与合法接收端单天线组成的 N 个信道中选择一个使 Bob 处接收信噪比最大的信道来传输信息。因此主信道为：

$$\boldsymbol{h}_{tas} = \arg \max_{k \in \{1,2,\cdots,N\}} \| \boldsymbol{h}_k \| \tag{6}$$

其中，$\boldsymbol{h}_k$ 是 Alice 的第 k 个天线与 Bob 组成的信道的系数。

采用 TBF 技术，$\Phi = 1$，没有人工噪声。Bob 处收到的信号为：

$$\boldsymbol{y} = \boldsymbol{h}_{tas} \boldsymbol{v}_I s_I + \boldsymbol{n}_B \tag{7}$$

Bob 处的瞬时信噪比为：

$$\gamma_B = \bar{\gamma}_B \| \boldsymbol{h}_{tas} \|^2 \tag{8}$$

Eve 处收到的信号为：

$$\boldsymbol{z} = \boldsymbol{G} \boldsymbol{v}_I s_I + \boldsymbol{n}_E \tag{9}$$

Eve 处的瞬时信噪比为：

$$\gamma_E = \boldsymbol{v}_I^H \boldsymbol{G}^H \boldsymbol{G} \boldsymbol{v}_I \bar{\gamma}_E \tag{10}$$

在 MISOME 窃听信道中可达安全速率（安全容量）为：

$$C_S = \begin{cases} C_B - C_E, \gamma_B > \gamma_E \\ 0, \gamma_B \leqslant \gamma_E \end{cases} \tag{11}$$

其中，$C_B = \log_2(1 + \gamma_B)$ 是主信道容量；$C_E = \log_2(1 + \gamma_E)$ 是窃听信道容量。

R 是安全速率，R_B 是传输码率，$R_B - R$ 就是为了抵抗 Eve 窃听保证信息安全损耗的速率。因为 Alice 准确知道 C_B，所以 Alice 选择 $R_B = C_B$ 来传输信息。而 Alice 不知道 C_E，所以 Alice 假设窃听信道的容量是 R_E，$R_E \neq C_E$。

1.2 传输机制

首先介绍自适应传输方案，然后给出加入安全中断概率约束后的有效安全吞吐量表达式，最后通过最优化算法找到使有效安全吞吐量 Ψ 最高的最优安全速率 $R_{optimal}$。

1.2.1 自适应传输方案

这里的自适应指的是传输过程中安全速率 R 和功率分配比 φ 是可变的，R 和 φ 的取值决定于 $\bar{\gamma}_B = \bar{\gamma}_B \| \boldsymbol{h} \|^2$ 和 $\bar{\gamma}_E$，$\bar{\gamma}_B$ 是主信道功率分配前的瞬时信噪比。Alice 选择一个安全速率 R，$0 < R < \bar{C}_B$，其中 $\bar{C}_B = \log_2(1 + \bar{\gamma}_B)$。Alice 选取 $R_B = \bar{C}_B$，满足可靠性条件，这时通信不会中断。因此自适应传输中只存在安全中断，当 $R_E < C_E$ 时发生安全中断。

为了量化分析安全性能，推导出两个概率表达式：安全传输概率 $P_{sec}(R)$ 和安全中断概率 $S_{out}(R)$。安全传输概率指的是 Alice 安全地将信息传输给 Bob 的概率；安全中断概率指的是信息泄露给 Eve 的概率。

$$P_{sec}(R) = 1 - T_{out}(R) - S_{out}(R) = 1 - S_{out}(R) =$$

$$\Pr(C_E \leqslant R_E) = \Pr(C_E \leqslant C_B - R) =$$

$$\Pr(\gamma_E \leqslant \frac{(1 + \varphi \bar{\gamma}_B)}{2^R} - 1) \tag{12}$$

其中，$T_{out}(R)$ 是通信中断概率，$T_{out}(R) = 0$。

观察式(5)中的 γ_E 发现，GV 中的元素是独立同分布的零均值复杂高斯随机变量。基于式(4)得到：

(1)当 $\frac{2^{R-1}}{\bar{\gamma}_B} < \Phi < 1$ 时，有：

$$P_{sec}(R) = F_{\gamma_E}\left(\frac{k}{2^R}\right) =$$

$$1 - e^{-\frac{k}{\varphi \bar{\gamma}_E 2^R}} \left(1 + \frac{(1-\varphi)k}{\varphi(N-1)2^R}\right)^{-(N-1)} \times$$

$$\sum_{p=1}^{M} \frac{1}{\Gamma(p)} \left(\frac{k}{\varphi \bar{\gamma}_E 2^R}\right)^{p-1} \times$$

$$\sum_{q=0}^{M-p} \binom{N-1}{q} \left(\frac{(1-\varphi)k}{\varphi(N-1)2^R}\right)^q \tag{13}$$

(2)当 $\Phi = 1$ 时，也就是采用 TBF 技术，没有人工噪声时，有：

$$P_{sec}(R) = R\left(1 - e^{-\frac{k}{2^R \bar{\gamma}_E}} \sum_{p=1}^{M} \frac{(1 + \bar{\gamma}_B \| \boldsymbol{h}_{tas} \|^2)^{p-1}}{\Gamma(p) (2^R \bar{\gamma}_E)^{p-1}}\right) \tag{14}$$

安全中断概率为：

$$S_{out}(R) = 1 - P_{sec}(R) \tag{15}$$

根据有效安全吞吐量的定义得到表达式：

$$\Psi(R) = R P_{sec}(R) \tag{16}$$

1.2.2 优化算法描述

(1) R 一定时，穷举 φ 找到使 $P_{sec}(R)$ 最大的 φ'，$\frac{2^{R-1}}{\bar{\gamma}_B} < \varphi \leqslant 1$。

$$\varphi' = \underset{\frac{2^{R-1}}{\bar{\gamma}_B} < \varphi \leqslant 1}{\arg\max} P_{sec}(R) \tag{17}$$

$$\min S_{out}(R) = 1 - \max P_{sec}(R) \tag{18}$$

(2)加入安全中断概率约束后的有效安全吞吐量为：

$$\Psi_M(R) = \begin{cases} \Psi(R), \min S_{out}(R) \leqslant S \\ 0, \min S_{out}(R) > S \end{cases} \tag{19}$$

(3)以使 $\Psi_M(R)$ 最大为目标，穷举找到最优安全速率 $R_{optimal}$，$0 < R < C_B$。

$$R_{optimal} = \underset{0 < R < C_B}{\arg\max} \Psi_M(R) \tag{20}$$

2 AN adaptive 传输方案与 TASTBF adaptive 传输方案的安全性能比较分析

定义：将 AN adaptive 传输方案相比于 TASTBF adaptive 传输方案有效安全吞吐量的相对增益定义为：

$$G(R_{\text{AN-optimal}},R_{\text{TASTBF-optimal}})\triangleq\frac{\Psi(R_{\text{AN-optimal}})}{\Psi(R_{\text{TASTBF-optimal}})}\quad(21)$$

其中，$\Psi(R_{\text{AN-optimal}})$ 和 $\Psi(R_{\text{TASTBF-optimal}})$ 分别对应于 AN adaptive 传输方案和 TASTBF adaptive 传输方案中的最大有效安全吞吐量。

3　仿真分析

用 Matlab 进行数值仿真得到性能曲线图，可以直观地观测与分析发射天线数、窃听天线数、TAS 中选择的天线数，以及 $\bar{\gamma}_B$ 和 $\bar{\gamma}_E$ 对两个系统安全性能和相对增益的影响。

图 1 给出了有效安全吞吐量 EST 与安全速率 R 之间的关系，其中 $n_E=2,\bar{\gamma}_E=\bar{\gamma}_B/3$。

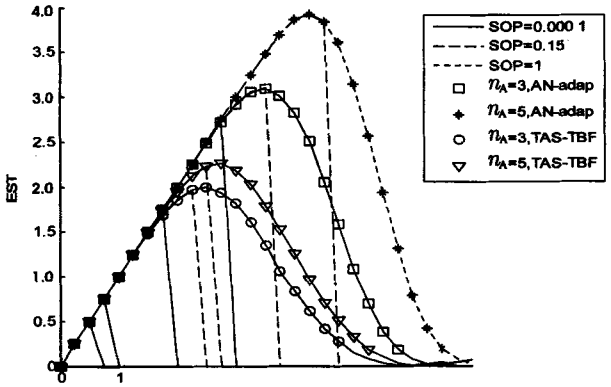

图 1　Eve 的天线数

由图可知，AN adaptive 方案比 TASTBF adaptive 方案的 EST 高。没加中断概率约束之前两个方案都能达到最大有效安全吞吐量，而加入安全中断概率约束 SOP = 0.15 后，TASTBF adaptive 方案已经不能达到最大 EST 和最优安全速率，而 AN adaptive 方案依然可以。说明当最大允许的中断概率减小时，AN adaptive 方案比 TASTBF 的安全性、鲁棒性更强。

当中断概率约束很严格，比如 SOP = 0.000 1 时，AN adaptive 方案和 TASTBF adaptive 方案都不能达到最大 EST。

对于 TASTBF adaptive 方案，当发送天线数增大时，最优安全速率 R_{optimal} 增加很小；而对于 AN adaptive 方案，当发送天线数增大时，最优安全速率 R_{optimal} 增加较大。

图 2 显示了安全中断概率和发送天线数的关系，其中 $n_E=2,\bar{\gamma}_E=5$ dB，$R=3$，$S=1$。

由图可知，当发送天线数增加时安全中断概率快速下降，AN adaptive 方案比 TASTBF adaptive 方案下降得更快。

图 3 给出了 EST 与 $\bar{\gamma}_E/\bar{\gamma}_B$ 的关系，其中 $n_E=2,\bar{\gamma}_B=15$ dB。

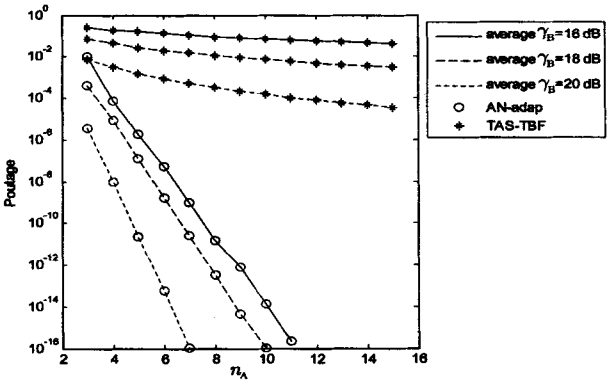

图 2　安全中断概率和发送天线数的关系

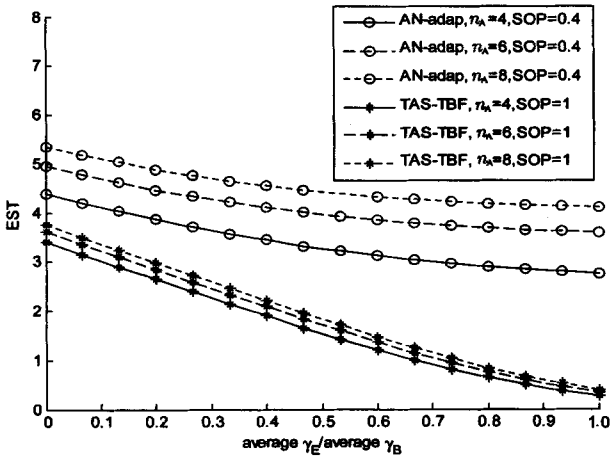

图 3　EST 与 $\bar{\gamma}_E/\bar{\gamma}_B$ 的关系

由图可知：当 $\bar{\gamma}_E$ 增大并逐渐接近 $\bar{\gamma}_B$ 时，TASTBF adaptive 方案有效吞吐量下降得比 AN adaptive 方案快，也就是说 TASTBF adaptive 方案的安全性能对窃听容量增大更为敏感。AN adaptive 方案在安全中断概率比 TASTBF adaptive 方案小的情况下，有效吞吐量依然比 TASTBF adaptive 方案高。也就是说发送天线数相同时，AN adaptive 方案比 TASTBF adaptive 方案安全中断概率更小，安全性更高。

图 4 给出了安全中断概率约束对系统安全性的影响，其中 $n_A=9,\bar{\gamma}_E=\bar{\gamma}_B/2$。

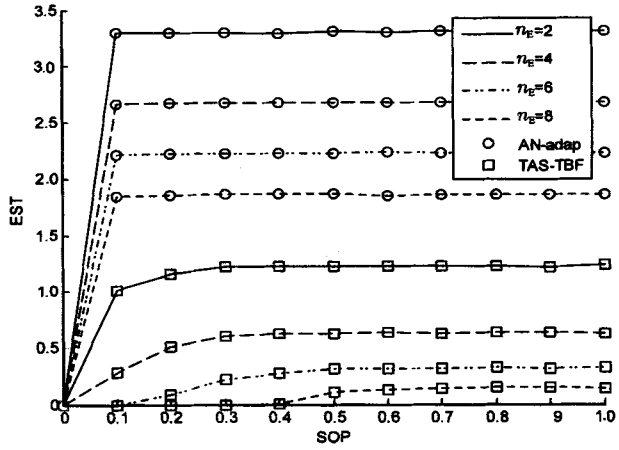

图 4　安全中断概率约束对系统安全性的影响

由图可以看出，当 $n_E = 6$，允许的最大 SOP 小于 0.5 时，TASTBF adaptive 方案的有效安全吞吐量快速下降，这时就要在吞吐量和安全性之间做出选择。若是选择较大的吞吐量，那么超过一半的信息可能会泄露；若是选择保证信息安全，那么系统的吞吐量就会很小。而 AN adaptive 方案对 SOP 变化的鲁棒性就比 TASTBF adaptive 方案强得多，可以工作在吞吐量较大、泄露信息很少的状态。

图 5 给出了 EST 与 n_A/n_E 的关系，其中 $\bar{\gamma}_E = \bar{\gamma}_B/2$，SOP = 1。

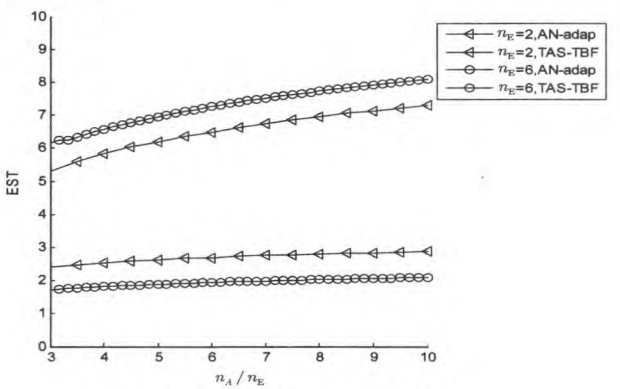

图 5 EST 与 n_A/n_E 的关系

由图可以看出：n_A/n_E 越大，EST 越大，且 AN adaptive 方案比 TASTBF adaptive 方案对 n_A/n_E 增长更敏感。说明增大 n_A 与 n_E 的比值，对 TASTBF adaptive 方案增大 EST 作用不大，但对 AN adaptive 方案增大 EST 的作用较大。在相同 n_A/n_E 下，n_E 越大（相应的 n_A 也越大），AN adaptive 方案 EST 越大，而 TASTBF adaptive 方案的 EST 则越小。说明对 AN adaptive 方案来说，n_A 是影响 EST 的主导因素，而对 TASTBF adaptive 方案来说，n_E 是主导因素。

图 6 给出了 n_E 和 n_{TAS} 对 $G(R_{AN-optimal}, R_{TASTBF-optimal})$ 的影响，其中 $n_A = 6, \bar{\gamma}_E = \bar{\gamma}_B/3, n_E \in \{1,2,3,4,5\}, n_{TAS} \in \{1,2,3,4,5,6\}$。

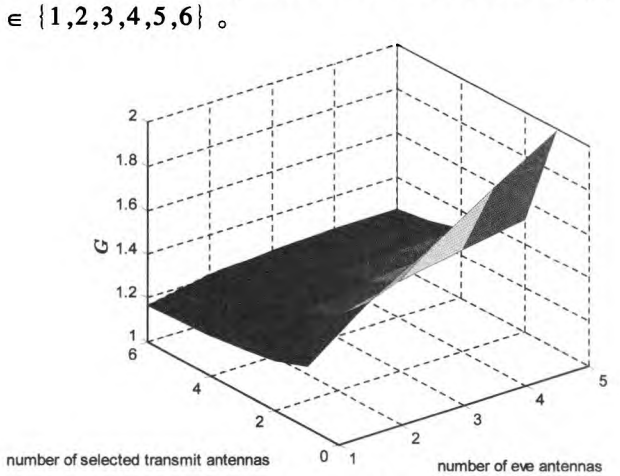

图 6 n_E 和 n_{TAS} 对 $G(R_{AN-optimal}, R_{TASTBF-optimal})$ 的影响

由图可以看出：G 随着 n_E 增大而增大，说明 AN adaptive 方案对窃听容量增加的适应性比 TASTBF adaptive 方案强。也就是说窃听天线越多，AN adaptive 方案比 TASTBF adaptive 方案越有优势。G 是随着 TAS 中选择的天线数增大而减小。

4 结束语

文中比较了两种物理层安全传输方案，一种是采用人工噪声辅助的 AN adaptive 方案，另一种是利用发端天线选择和发端波束成形技术的 TASTBF adaptive 方案。在两种方案中都加入了安全中断概率约束，推导出了安全传输概率和有效安全吞吐量的表达式，给出了求最大有效安全吞吐量的算法，并对两种方案的安全性能进行了深入对比分析。仿真结果表明：在允许的最大 SOP 减小时，AN-adaptive 方法比 TASTBF-adaptive 方法的安全性和鲁棒性更好；提高 AN-adaptive 方案安全性能应主要通过增大发送天线数和主信道平均信噪比，而提高 TASTBF-adaptive 方案安全性能应主要通过减小窃听天线数和窃听信道平均信噪比；TASTBF-adaptive 方法中 TAS 选择多根天线比只选择一根天线安全性能更好。

参考文献：

[1] Barros J, Rodrigues M R D. Secrecy capacity of wireless channels[C]//IEEE international symposium on information theory. Seattle, WA: IEEE, 2006.

[2] Blochand M, Barros J. Physical-layer security: from information theory to security engineering[M]. Cambridge, UK: Cambridge University Press, 2011.

[3] 龙 航，袁广翔，王 静，等. 物理层安全技术研究现状与展望[J]. 电信科学，2011，27(9)：60-65.

[4] 刘在爽，王 坚，孙 瑞，等. 无线通信物理层安全技术综述[J]. 通信技术，2014，47(2)：128-135.

[5] Yang N, Yeoh P L, Elkashlan M, et al. Transmit antenna selection for security enhancement in MIMO wiretap channels[J]. IEEE Transactions on Communications, 2013, 61(1): 144-154.

[6] Hong Y W P, Lan P C, 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] 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.

[8] Yang N, Elkashlan M, Duong T Q, et al. Optimal transmission with artificial noise in MISOME wiretap channels[J]. IEEE Transactions on Vehicular Technology, 2016, 53(3): 1.

[9] 李 为，陈 彬，魏急波，等. 基于接收机人工噪声的物理

（下转第 85 页）

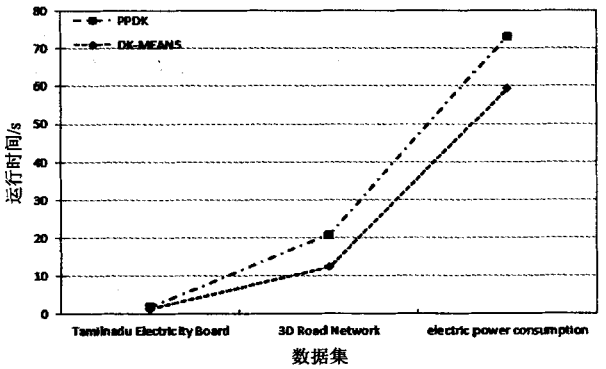

图5　算法运行时间对比

参与方拥有不同的密钥,从而避免合谋攻击和窃听攻击。理论分析和实验结果表明,PPDK能在保持挖掘结果精确度的同时防止各参与方隐私数据的泄露,且时间增加在可容忍的范围内。

参考文献:

[1] Han J W, Micheline K. 数据挖掘概念与技术[M]. 范　明,孟晓峰,译. 北京:机械工业出版社,2012.

[2] 周水庚,李　丰,陶宇飞,等. 面向数据库应用的隐私保护研究综述[J]. 计算机学报,2009,32(5):847-861.

[3] Prakash M, Singaravel G. A review on approaches, techniques and research challenges in privacy preserving data mining[J]. Australian Journal of Basic & Applied Sciences, 2014, 8(10):251-259.

[4] 郑苗苗,吉根林. DK-Means—分布式聚类算法K-Dmeans的改进[J]. 计算机研究与发展,2007,44(s2):84-88.

[5] 杨丹凤,余青松,郑冀之. 分布式数据隐私保护K-均值聚类算法[J]. 计算机与数字工程,2008,36(7):113-116.

[6] 张国荣,印　鉴. 分布式环境下保持隐私的聚类挖掘算法[J]. 计算机工程与应用,2007,43(18):165-167.

[7] Vaidya J, Clifton C. Privacy-preserving k-means clustering over vertically partitioned data[C]//Ninth ACM SIGKDD international conference on knowledge discovery & data mining. [s. l.]: ACM, 2003:206-215.

[8] 刘英华,杨炳儒,曹丹阳,等. 分布式聚类算法的隐私保护研究[J]. 计算机科学,2012,39(3):160-162.

[9] 方炜炜,杨炳儒,夏红科. 基于SMC的隐私保护聚类模型[J]. 系统工程与电子技术,2012,34(7):1505-1510.

[10] Erkin Z, Veugen T, Toft T, et al. Privacy-preserving distributed clustering[J]. EURASIP Journal on Information Security, 2013, 2013(1):1-15.

[11] Yi X, Zhang Y. Equally contributory privacy-preserving k-means clustering over vertically partitioned data[J]. Information Systems, 2013, 38(1):97-107.

[12] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[C]//International conference on theory and application of cryptographic techniques. [s. l.]: Springer-Verlag, 1999:223-238.

[13] Elgamal T. A public key cryptosystem and a signature scheme based on discrete logarithms[J]. IEEE Transactions on Information Theory, 1985, 31(4):469-472.

[14] 黄汝维,桂小林,余　思,等. 云环境中支持隐私保护的可计算加密方法[J]. 计算机学报,2011,34(12):2391-2402.

[15] Patel S J, Chouhan A, Jinwala D C. Comparative evaluation of elliptic curve cryptography based homomorphic encryption schemes for a novel secure multiparty computation[J]. Journal of Information Security, 2014, 5(1):12-18.

(上接第80页)

层安全技术及保密区域分析[J]. 信号处理,2012,28(9):1314-1320.

[10] 李翔宇,金　梁,黄开枝. 基于人工噪声的中继网络物理层安全传输机制[J]. 计算机应用研究,2012,29(9):3467-3469.

[11] Monteiro M P, Rebelatto J L, Souza R D, et al. Maximum secrecy throughput of transmit antenna selection with eavesdropper outage constraints[J]. IEEE Signal Processing Letters, 2015, 22(11):2069-2072.

[12] 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.

[13] Zhou X, McKay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation[J]. IEEE Transactions on Vehicular Technology, 2010, 59(8):3831-3842.

[14] 徐以标,张会生,李立欣. 多中继AF协作系统功率分配研究[J]. 信息安全与通信保密,2011,9(12):65-67.

[15] 张　鹏. 双向协作通信系统的中继选择与功率分配技术研究[D]. 南京:南京邮电大学,2014.

[16] Mukherjee A, Swindlehurst A L. Robust beamforming for security in MIMO wiretap channels with imperfect CSI[J]. IEEE Transactions on Signal Processing, 2011, 59(1):351-361.

[17] Li Q, Ma W K. Spatially selective artificial-noise aided transmit optimization for miso multi-eves secrecy rate maximization [J]. IEEE Transactions on Signal Processing, 2013, 61(10):2704-2717.