物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

无线多径信道中基于时间反演的物理层安全传输机制

朱江　王雁　杨甜

Secure transmission mechanism based on time reversal over wireless multipath channels

Zhu Jiang　Wang Yan　Yang Tian

引用信息 Citation: Acta Physica Sinica, 67, 050201 (2018)　DOI: 10.7498/aps.20172134
在线阅读 View online: http://dx.doi.org/10.7498/aps.20172134
当期内容 View table of contents: http://wulixb.iphy.ac.cn/CN/Y2018/V67/I5

无线多径信道中基于时间反演的物理层安全传输机制*

朱江 王雁† 杨甜

(移动通信技术重庆市重点实验室, 重庆 400065)

(2017 年 9 月 27 日收到; 2017 年 12 月 7 日收到修改稿)

宽带无线通信用户大多处在复杂的环境中, 其时变多径传播和开放特性将严重影响通信系统的性能. 针对物理层安全研究中的窃听信道问题, 提出了一种适用于宽带无线多径信道的联合时间反演技术和发端人工噪声的物理层安全传输机制. 首先, 在一个典型窃听信道模型中采用时间反演技术, 利用其时空聚焦性来提高信息在传输过程中的安全性; 其次, 由于时间反演的时空聚焦性, 信息在聚焦点附近容易被窃听, 通过在发送端加入人工噪声来扰乱窃听用户对保密信息的窃听, 由于合法用户采用零空间人工噪声法, 人工噪声对合法用户没有影响. 理论分析和仿真结果表明, 与已有物理层安全机制相比, 所提机制可以有效地提高系统的保密信干噪比和可达保密速率, 降低合法用户的误比特率, 系统的保密性能得到提升.

关键词: 窃听信道, 时间反演, 人工噪声, 时空聚焦

PACS: 02.10.Xm, 05.45.–a, 84.40.Ua, 43.60.Gk **DOI:** 10.7498/aps.67.20172134

1 引 言

时间反演 (time reversal, TR) 是近年来发展起来的电磁学新方向, 研究表明 TR 电磁波传播具有时-空同步聚焦、超分辨率聚焦等特性, 基于这些特性构建的新型电磁波应用系统将有可能为无线信息技术带来突破性的进步. 因此, TR 技术以其良好的电磁特性在通信和探测等研究领域存在巨大的潜力, 得到了越来越多的重视 [1−4]. 例如, 实现大容量无线通信 [1]、超分辨率成像 [5−7]、高精度定位 [8,9]、低能耗保密通信 [10] 等.

TR 技术在时域上对信道状态信息进行逆序操作, 等同于在频域上进行相位共轭 [11]. 无论是在均匀媒质环境中还是在非均匀媒质环境中, 经由 TR 技术处理过的信号具有时间和空间的同步聚焦特性 [12]. 而且这种时-空聚焦特性对环境是自适应的, 不需要获取任何的先验知识或进行任何被动控制. 因此, TR 技术可以引入到宽带无线通信系统的物理层安全研究 [13−18]. 目前, 较为普遍的物理层安全方法是人工噪声法 [16−18]. 在窃听信道模型下, 结合天线选择和人工噪声分析计算系统的安全中断概率, 以此分析影响系统安全的主要因素 [19−21]. 此外, 现有文献都是假设人工噪声位于合法信道的零空间内, 合法信道方向上的保密信号未被干扰, 但多天线窃听用户可以从多次的接收信号中将人工噪声和保密信号分开来窃听. 另外, 高速率宽带无线通信用户大多处在异常复杂的环境中, 其时变多径传播特性会严重影响通信性能. 通过 TR 技术, 可以利用合法信道特性的惟一性以及互易性来实现加密信息、产生密码、辨识合法用户等特性, 增强物理层传输的安全性. TR 技术在实现物理层安全方面有着独有的优势 [22]. TR 技术使得信号只有在特定的时间和特定的空间内才可以被检测出来, 而超出这个范围信号很难被检测出

* 国家自然科学基金 (批准号: 61771084) 和重庆市科委自然科学基金 (批准号: cstc2015jcyjA40050) 资助的课题.

† 通信作者. E-mail: xiaoyanzi_19911130@163.com

来, 从而提高信息传输安全. 研究表明, TR 技术的聚焦特性不仅改善了接收端的信噪比, 提高了整体的通信性能, 还降低了各个通信系统之间的互相干扰, 并且防止自己的有效信息被恶意窃听 [12]. 张光旻等 [12] 提出了一种新型的 TR 探测和信息传输方法, 利用 TR 技术的时空聚焦性来减少信号被截获位置点的数量, 提高信息传输的安全性. 文献 [23] 对比多输入多输出 (multiple input multiple output, MIMO) 系统中使用 TR 技术和不使用 TR 技术时的保密容量, 分析验证了 TR 技术可以提高系统的保密性能. TR 技术虽然保证了信息传输过程的安全性, 但是由于 TR 技术的时空聚焦性, 信息聚焦于接收点处, 无法避免窃听用户在接收点附近对信息的窃听.

本文提出一种适用于无线多径信道的物理层安全传输机制. 该机制将系统建模为多输入单输出 (multi-input single output, MISO) 窃听信道模型, 通过在发送方联合使用 TR 技术和人工噪声, 从而达到信息安全传输的目的, 同时降低了信息在接收方被窃听的风险. 在假设窃听用户对系统进行被动窃听的情况下, 本文的主要贡献如下:

1) 将 TR 技术用于 MISO 窃听信道模型中, 利用其时空聚焦性保证信息在传输过程中的安全性, 降低信息被截获的概率;

2) 针对信息容易在接收方附近被窃听, 提出一种联合 TR 技术和人工噪声的安全传输机制, 利用人工噪声对合法信道没有影响, 对窃听信道有干扰的特性, 减少信息在接收方被窃听的可能性.

2 物理层安全传输机制

机制的设计思路为在信源加入人工噪声, 发送端合法信道采用 TR 技术, TR 技术保证信息在非聚焦区域的安全性, 人工噪声使信息在聚焦区域附近很难被窃听. 假设窃听用户只进行被动窃听, 合法用户无法知道窃听用户的信道状态信息 [13−16]. 因此安全传输机制的实现不以窃听用户信道状态信息已知为前提. 其具体内容如图 1 所示.

基于图 1 机制提出如图 2 所示的采用 TR 技术的 MISO 窃听信道系统模型, 该模型包括一个发送方, 一个合法用户和一个窃听用户. 发送方有 M 根天线, 合法用户和窃听用户均为单接收天线. 根据图 2 模型, 下面讨论合法用户的接收信号.

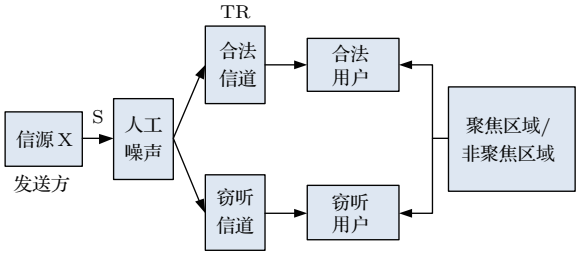

图 1 安全传输机制

Fig. 1. Secure transmission scheme.

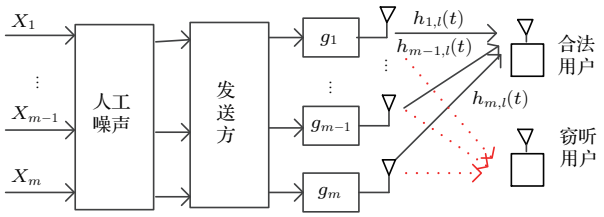

图 2 窃听信道模型

Fig. 2. Eavesdropping channel model.

在 MISO 窃听信道下, 设发送方的发送信号向量为

$$\boldsymbol{X} = \boldsymbol{S} + \boldsymbol{W}, \tag{1}$$

$\boldsymbol{S}$ 为要发送的保密信息向量, $\boldsymbol{W}$ 为随机人工噪声向量, 且满足 $\boldsymbol{HW} = 0$, $\boldsymbol{H}$ 为合法信道矩阵. 系统整体功率设为 P, α 为功率分配因子, 即设定

$$E(\boldsymbol{S}^{\mathrm{H}}\boldsymbol{S}) = \alpha P, \tag{2}$$

$$E(\boldsymbol{W}^{\mathrm{H}}\boldsymbol{W}) = (1-\alpha)P. \tag{3}$$

复杂多径信道中, 用 $n \in \{r, e\}$ 分别表示合法用户和窃听用户, 且合法信道和窃听信道用维数为 $2M \times L$ 的矩阵 $\boldsymbol{H}_{\mathrm{I}} = [\boldsymbol{h}_{1,\mathrm{r}} \cdots \boldsymbol{h}_{M,\mathrm{r}} \boldsymbol{h}_{1,\mathrm{e}} \cdots \boldsymbol{h}_{M,\mathrm{e}}]^{\mathrm{T}}$ 表示, 则 $\boldsymbol{H} = [\boldsymbol{h}_{1,\mathrm{r}} \cdots \boldsymbol{h}_{M,\mathrm{r}}]$ 表示合法矩阵, L 为可分辨的多径的数目. 假设发送天线 $m(0 \leqslant m \leqslant M)$ 和用户之间的信道冲激响应 (channel impulse response, CIR) 可以表示为

$$h_{m,n}(t) = \sum_{l=0}^{L-1} \alpha_{mn,l}\delta(t - \tau_{mn,l}), \tag{4}$$

其中 L 为抽头总数, 且 $0 \leqslant l \leqslant L-1$, $\alpha_{mn,l}$ 和 $\tau_{mn,l}$ 分别表示第 l 个抽头的幅度和时延, 这里的抽头对应无线多径信道中的多径, CIR 在时域上离散化为矩阵 $\boldsymbol{h}_{m,n} \in C^{L\times 1}$, 对每条链路, $h_{mn}[l]$ 是循环对称复高斯 (circular symmetric complex Gaussian, CSCG) 随机变量, 即满足 $E[h_{mn}[l]] = 0$, $E[|h_{mn}[l]|^2] = \alpha_{mn,l}^2 = \mathrm{e}^{-lT_{\mathrm{S}}/\sigma_{\mathrm{T}}}$ [24], 其中 T_{S} 为系统采样周期, σ_{T} 为信道均方根延迟扩展. CIR 可以

通过TR探测阶段探测获得, 由于多径信道的复杂性, 这里假设CIR已知.

首先讨论合法用户的接收信号. 信息序列由TR镜 (time reversal mirror, TRM) 向量 $\boldsymbol{g}_{m,\mathrm{r}} \in C^{L\times 1}$ 调制, $\boldsymbol{g}_{m,\mathrm{r}}$ 由 $\boldsymbol{h}_{m,\mathrm{r}}$ 经TR和归一化后得到, 每个分量记为

$$\begin{aligned} g_{m,\mathrm{r}}[l] =& \frac{\bar{h}_{m,\mathrm{r}}[L-1-l]}{\sqrt{\sum\limits_{m=1}^{M} E[\|h_{m,\mathrm{r}}\|^2]}} \\ =& \frac{\bar{h}_{m,\mathrm{r}}[L-1-l]}{\sqrt{E[M\sum\limits_{l=0}^{L-1}|h_{m,\mathrm{r}}[l]|^2]}}, \end{aligned} \tag{5}$$

式中 $\|\cdot\|$ 表示Frobenius范数, $\bar{\cdot}$ 表示共轭.

合法用户的接收信号为

$$\boldsymbol{r}_{\mathrm{r}} = \sum_{m=1}^{M} \boldsymbol{S}(\boldsymbol{h}_{m,\mathrm{r}} * \boldsymbol{g}_{m,\mathrm{r}}) + \boldsymbol{n}_{\mathrm{r}}, \tag{6}$$

可以记为

$$\begin{aligned} r_{\mathrm{r}}[l] =& \sum_{n}\sum_{m=1}^{M}\sum_{k=0}^{2L-2}(h_{m,\mathrm{r}} * g_{m,\mathrm{r}})[k]S_n[l-k] \\ &+ n_{\mathrm{r}}[l], \end{aligned} \tag{7}$$

$*$ 表示卷积, $\forall k,l \in \{0,1,\cdots,2L-2\}$, $\boldsymbol{S}$ 表示要发送的保密信号向量, $\boldsymbol{n}_{\mathrm{r}}$ 为均值为0, 方差为 $\sigma(r)^2$ 的高斯白噪声向量, $n \in \{r,e\}$. (7) 式中

$$\begin{aligned} &(h_{m,\mathrm{r}} * g_{m,\mathrm{r}})[l] \\ =& \sum_{k=0}^{L-1} h_{m,\mathrm{r}}[k] g_{m,\mathrm{r}}[l-k] \\ =& \frac{\sum\limits_{k=0}^{L-1} h_{m,\mathrm{r}}[k]\bar{h}_{m,\mathrm{r}}[L-1-l+k]}{\sqrt{E[M\sum\limits_{l=0}^{L-1}|h_{m,\mathrm{r}}[l]|^2]}}, \end{aligned} \tag{8}$$

$l = L-1$ 对应自相关函数的最大功率中心峰值, 即

$$\begin{aligned} &(h_{m,\mathrm{r}} * g_{m,\mathrm{r}})[L-1] \\ =& \sum_{k=0}^{L-1}|h_{m,\mathrm{r}}[k]|^2 / \sqrt{E[M\sum_{l=0}^{L-1}|h_{m,\mathrm{r}}[l]|^2]}. \end{aligned} \tag{9}$$

由多径信道特性, (9) 式可以具体分为信号 (Signal)、符号间干扰 (inter symbol interference, ISI)、用户间干扰 (inter user interference, IUI) 和高斯噪声 (Noise) 四部分之和:

$$\begin{aligned} &R_{\mathrm{r}}[l] \\ =& \sum_{m=1}^{M}(h_{m,\mathrm{r}} * g_{m,\mathrm{r}})[L-1]S_{\mathrm{r}}[l-L+1] \quad \text{(Signal)} \\ &+ \sum_{k=0k\neq L-1}^{2L-2}\sum_{m=1}^{M}(h_{m,\mathrm{r}} * g_{m,\mathrm{r}})[k]S_{\mathrm{r}}[l-k] \quad \text{(ISI)} \\ &+ \sum_{k=0}^{2L-2}\sum_{m=1}^{M}(h_{m,\mathrm{e}} * g_{m,\mathrm{r}})[k]S_{\mathrm{e}}[l-k] \quad \text{(IUI)} \\ &+ n_{\mathrm{r}}[k] \quad \text{(Noise)} \end{aligned} \tag{10}$$

其中 S_{r} 为向合法用户发送的保密信号, S_{e} 为窃听用户可能截获的保密信号, $n_{\mathrm{r}}[l]$ 为每条多径对应的噪声信号.

下面分别讨论窃听用户位于合法用户的聚焦区域和非聚焦区域内时的接收信号.

2.1 窃听用户位于合法用户的聚焦区域内

不加人工噪声时, 窃听用户接收信号

$$\boldsymbol{r}_{\mathrm{e}} = \sum_{m=1}^{M} \boldsymbol{S}(\boldsymbol{h}_{m,\mathrm{e}} * \boldsymbol{g}_{m,\mathrm{r}}) + \boldsymbol{n}_{\mathrm{e}}, \tag{11}$$

可以记为

$$\begin{aligned} r_{\mathrm{e}}[l] =& \sum_{n}\sum_{m=1}^{M}\sum_{k=0}^{2L-2}(h_{m,\mathrm{e}} * g_{m,\mathrm{r}})[k]S_n[l-k] \\ &+ n_{\mathrm{e}}[l]. \end{aligned} \tag{12}$$

不加人工噪声时, 经过TRM调制, 在窃听用户处的 $(2L-1)\times 1$ 的接收信号向量可以表示为

$$\begin{aligned} &R_{\mathrm{e}}[l] \\ =& \sum_{m=1}^{M}(h_{m,\mathrm{e}} * g_{m,\mathrm{r}})[L-1]S_{\mathrm{e}}[l-L+1] \quad \text{(Signal)} \\ &+ \sum_{k=0k\neq L-1}^{2L-2}\sum_{m=1}^{M}(h_{m,\mathrm{e}} * g_{m,\mathrm{r}})[k]S_{\mathrm{e}}[l-k] \quad \text{(ISI)} \\ &+ \sum_{k=0}^{2L-2}\sum_{m=1}^{M}(h_{m,\mathrm{r}} * g_{m,\mathrm{r}})[k]S_{\mathrm{r}}[l-k] \quad \text{(IUI)} \\ &+ n_{\mathrm{e}}[l] \quad \text{(Noise)}, \end{aligned} \tag{13}$$

加人工噪声时, 窃听用户接收信号

$$\begin{aligned} \boldsymbol{r}'_{\mathrm{e}} =& \sum_{m=1}^{M}\boldsymbol{S}(\boldsymbol{h}_{m,\mathrm{e}} * \boldsymbol{g}_{m,\mathrm{r}}) + \sum_{m=1}^{M}\boldsymbol{W}(\boldsymbol{h}_{m,\mathrm{e}} * \boldsymbol{g}_{m,\mathrm{r}}) \\ &+ \boldsymbol{n}_{\mathrm{e}} \end{aligned} \tag{14}$$

可以记为

$$r'_{\mathrm{e}}[l] = \sum_{n}\sum_{m=1}^{M}\sum_{k=0}^{2L-2}(h_{m,\mathrm{e}} * g_{m,\mathrm{r}})[k]S_n[l-k]$$

$$+\sum_{m=1}^{M}\sum_{k=0}^{2L-2}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[k]W[l-k]+n'_{\mathrm{e}}[l], \tag{15}$$

同理, 在窃听用户处的 $(2L-1)\times 1$ 的接收信号向量可以表示为

$$\begin{aligned}&R'_{\mathrm{e}}[l]\\ =&\sum_{m=1}^{M}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[L]S_{\mathrm{e}}[l-L+1]\ \ (\text{Signal})\\ &+\sum_{k=0\ k\neq L-1}^{2L-2}\sum_{m=1}^{M}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[k]S_{\mathrm{e}}[l-k]\ \ (\text{ISI})\\ &+\sum_{k=0}^{2L-2}\sum_{m=1}^{M}(h_{m,\mathrm{r}}*g_{m,\mathrm{r}})[k]S_{\mathrm{e}}[l-k]\ \ (\text{IUI})\\ &+n'_{\mathrm{e}}[k]\ \ (\text{Noise})\\ &+\sum_{m=1}^{M}\sum_{k=0}^{2L-2}(g_{m,\mathrm{r}}*h_{m,\mathrm{e}})[k]W[l-k]\ \ (\text{Art Noise}),\end{aligned} \tag{16}$$

式中 Art Noise 表示人工噪声.

由 (10), (13) 和 (16) 式可以看出, 聚焦区域内, 人工噪声对合法用户的接收信号没有影响, 但是人工噪声对窃听用户的接收信号造成了干扰. 对窃听用户, 人工噪声和高斯白噪声共同组成了噪声部分, 因此, 窃听用户的信干噪比 (signal to interference and noise ratio, SINR) 减小, 系统保密性能有所提升.

2.2 窃听用户位于合法用户的非聚焦区域内

非聚焦区域内系统安全性能可以通过以下定理说明.

定理 1 非聚焦区域内采用 TR 技术的安全性能要优于物理层零空间人工加扰法.

证明 令 $h^{\mathrm{MISO}}_{\mathrm{eq}(\boldsymbol{r}_0)}$ 表示位于 $\boldsymbol{r}_0=(x_0,y_0,z_0)$ 处的合法用户的等效 CIR. 对有一个合法用户和一个窃听用户的 $M\times 1$TR-MISO 系统, 第 m 根发射天线与用户 $n\in\{r,e\}$ 之间的 CIR 可以表示为 $h_{m,n}[l],(0\leqslant l\leqslant L-1)$, $h_{m,n}[l]$ 是第 l 条多径的 CIR, 对应的 TRM 向量 $\boldsymbol{g}_{m,n}\in C^{L\times 1}$ 的分量记为

$$g_{m,n}[l]=\frac{A_m\bar{h}_{m,n}[L-1-l]}{\sqrt{E\left[\sum\limits_{l=0}^{L-1}|h_{m,n}[l]|^2\right]}}, \tag{17}$$

A_m 为能量控制因子, 使功率归一化, 令 $A_m=1/\sqrt{M}$. 合法用户的等效 CIR 表示

$$\begin{aligned}&h^{\mathrm{MISO}}_{\mathrm{eq}(r_0)}[l]\\ =&\sum_{m=1}^{M}h_{m,\mathrm{r}}[l]*g_{m,\mathrm{r}}[l]\\ =&\sum_{m=1}^{M}\sum_{k=0}^{L-1}h_{m,\mathrm{r}}[l]g_{m,\mathrm{r}}[l-k]\\ =&\sum_{m=1}^{M}\frac{\sum\limits_{k=0}^{L-1}h_{m,\mathrm{r}}[k]\bar{h}_{m,\mathrm{r}}[L-1-l+k]}{\sqrt{M}\sqrt{E[\sum\limits_{k=0}^{L-1}|h_{m,\mathrm{r}}[k]|^2]}}\\ =&\sum_{m=1}^{M}\frac{1}{\sqrt{M}}\sqrt{E[\sum_{k=0}^{L-1}|h_{m,\mathrm{r}}[k]|^2]}*\delta[L-1-l].\end{aligned} \tag{18}$$

令 $h^{\mathrm{MISO}}_{\mathrm{eq}(\boldsymbol{r}_1)}[l]$ 代表处于非聚焦区域 $\boldsymbol{r}_1=(x_1,y_1,z_1)$ 处的窃听用户的 CIR. 对窃听用户, 忽略 ISI 和 IUI 其等效 CIR 为

$$h^{\mathrm{MISO}}_{\mathrm{eq}(r_1)}[l]=\sum_{m=1}^{M}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[l]. \tag{19}$$

由 (18) 式合法用户等效 CIR 的主要部分是所有多径分量的自相关之和, 而 (19) 式窃听用户等效 CIR 是各个多径的互相关之和, 无法有效地接收信息, 各个径的信息将会湮没在噪声之中. 因此, 非聚焦区域内多径信道条件下, 采用 TR 技术能在很大程度上保证信息传输的安全性.

物理层安全研究中的零空间人工噪声法 [17] 系统安全容量随着发送方与窃听用户之间距离的变化而变化, 且两者之间距离越近, 即在非聚焦区域内, 安全容量也越低 [25].

因此, 非聚焦区域内采用 TR 技术与物理层零空间人工噪声法相比, 安全性能要更高. **证毕**.

通过分析聚焦区域和非聚焦区域内系统安全性能, 可以得出以下结论:

1) 非聚焦区域内, TR 技术的安全性要优于只采用人工噪声时候的系统的安全性能;

2) 聚焦区域内, TR 技术并不能很好地保证系统的安全性, 与人工噪声相结合能增强系统的安全性.

由以上结论可知, TR 技术和人工噪声结合时系统的安全性能最好. 在实际应用中, 考虑到复杂度和实现代价问题, 在非聚焦区域内, 可以只采用

TR技术就能保证信息安全传输; 另一方面, 在聚焦区域内, 只采用TR技术存在一些局限性, 此时, 采用TR技术和人工噪声结合的方案才能够确保系统的安全性.

3 保密性能分析

本文从保密信干噪比、可达保密速率和误码率三个方面来分析系统的保密性能. 通过理论分析和推导得出保密信干噪比和可达保密速率的解析式. 根据文献[26]和文献[27]误比特率推导方式, 采用正交幅度调制(quadrature amplitude modulation, QAM), 具体分析合法信道和窃听信道的误码率, 并进行仿真验证. 由前面分析可知, 当采用TR技术后, 窃听用户只能在聚焦区域进行有效窃听, 因此, 只分析聚焦区域内的保密性能.

3.1 保密信干噪比

3.1.1 聚焦区域不考虑加人工噪声

假设发送信号s为0, 1随机序列, CIR随机生成[24,28], 由(10)和(13)式, 则合法用户和窃听用户的信号功率分别为:

$$P_{\mathrm{Sig}}(r)=\left|\sum_{m=1}^{M}(h_{m,\mathrm{r}}*g_{m,\mathrm{r}})[L-1]\right|^2, \tag{20}$$

$$P_{\mathrm{Sig}}(e)=\left|\sum_{m=1}^{M}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[L-1]\right|^2. \tag{21}$$

同理, 符号间干扰和用户间干扰功率分别为:

$$P_{\mathrm{ISI}}(r)=\sum_{l=0l\neq L-1}^{2L-2}\left|\sum_{m=1}^{M}(h_{m,\mathrm{r}}*g_{m,\mathrm{r}})[l]\right|^2, \tag{22}$$

$$P_{\mathrm{ISI}}(e)=\sum_{l=0l\neq L-1}^{2L-2}\left|\sum_{m=1}^{M}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[l]\right|^2, \tag{23}$$

$$P_{\mathrm{IUI}}(r)=\sum_{l=0}^{2L-2}\left|\sum_{m=1}^{M}(h_{m,\mathrm{e}}*g_{m,\mathrm{r}})[l]\right|^2, \tag{24}$$

$$P_{\mathrm{IUI}}(e)=\sum_{l=0}^{2L-2}\left|\sum_{m=1}^{M}(h_{m,\mathrm{r}}*g_{m,\mathrm{r}})[l]\right|^2. \tag{25}$$

对于一个窃听信道模型, 保密SINR可以衡量该系统的安全性能, 记为

$$\gamma_{\mathrm{S}}=(\gamma_{\mathrm{r}}-\gamma_{\mathrm{e}})/(1+\gamma_{\mathrm{e}}), \tag{26}$$

γ_{r}表示合法用户的SINR, γ_{e}表示窃听用户的SINR, $n\in\{r,e\}$, 则

$$\gamma_n=\frac{P_{\mathrm{Sig}}(n)}{P_{\mathrm{ISI}}(n)+P_{\mathrm{IUI}}(n)+\sigma(n)^2}, \tag{27}$$

平均SINR为

$$E[\gamma_n]=E\left[\frac{P_{\mathrm{Sig}}(n)}{P_{\mathrm{ISI}}(n)+P_{\mathrm{IUI}}(n)+\sigma(n)^2}\right]. \tag{28}$$

由(26)式, 平均保密SINR可表示为

$$\overline{\gamma}_{\mathrm{S}}=E[\gamma_{\mathrm{S}}]=E\left[\frac{\gamma_{\mathrm{r}}-\gamma_{\mathrm{e}}}{1+\gamma_{\mathrm{e}}}\right], \tag{29}$$

又因为

$$\begin{aligned}E\left[\frac{a}{b+c+d}\right]=&\frac{E[a]}{E[b]+E[c]+E[d]}\\&+\frac{\sum_{i=1}^{\infty}(-1)^iE[a]\langle^i(b+c+d)\rangle}{E[b+c+d]^{i+1}}\\&+\frac{\langle a,^i(b+c+d)\rangle}{E[b+c+d]^{i+1}},\end{aligned} \tag{30}$$

(30)式右边第二、三项涉及多重积分, 比较复杂, 所以忽略第二和第三项[30−32], 推导得出的平均保密SINR为

$$\overline{\gamma}_{\mathrm{s}}=\frac{E[\gamma_{\mathrm{r}}-\gamma_{\mathrm{e}}]}{E[1+\gamma_{\mathrm{e}}]}=\frac{E[\gamma_{\mathrm{r}}]-E[\gamma_{\mathrm{e}}]}{1+E[\gamma_{\mathrm{e}}]}. \tag{31}$$

由上述推导, (28)式可化为

$$E[\gamma_n]\approx\frac{E[P_{\mathrm{Sig}}(n)]}{E[P_{\mathrm{ISI}}(n)]+E[P_{\mathrm{IUI}}(n)]+\sigma^2(n)}. \tag{32}$$

将(32)式代入(31)式可得平均保密SINR.

3.1.2 聚焦区域考虑加人工噪声

由第2节分析, 人工噪声对合法用户接收信号没有影响, 根据(2), (10)和(20)式得合法用户功率为$\alpha PE[P_{\mathrm{Sig}}(r)]$, 所以合法用户平均SINR

$$E[\gamma_{\mathrm{r}}]=\frac{\alpha PE[P_{\mathrm{Sig}}(r)]}{E[P_{\mathrm{ISI}}(r)]+E[P_{\mathrm{IUI}}(r)]+\sigma(r)^2}, \tag{33}$$

系统整体功率设为P, α为功率分配因子. 又

$$E[|h[k]|^2]=\mathrm{e}^{-kT_{\mathrm{S}}/\sigma_{\mathrm{T}}}, \tag{34}$$

$$E[|h[k]|^4]=2(E[|h[k]|^2])^2=2\,\mathrm{e}^{-2kT_{\mathrm{S}}/\sigma_{\mathrm{T}}}. \tag{35}$$

由上式得$E[P_{\mathrm{Sig}}(r)]$, $E[P_{\mathrm{ISI}}(r)]$, $E[P_{\mathrm{IUI}}(r)]$如下:

$$\begin{aligned}&E[P_{\mathrm{Sig}}(r)]\\&=\frac{1+\exp(-LT_{\mathrm{S}}/\sigma_{\mathrm{T}})}{1+\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})}+M\frac{1-\exp(-LT_{\mathrm{S}}/\sigma_{\mathrm{T}})}{1-\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})},\end{aligned} \tag{36}$$

$$\begin{aligned}&E[P_{\mathrm{ISI}}(r)]\\&=\frac{2\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})(1-\exp(-(L-1)T_{\mathrm{S}}/\sigma_{\mathrm{T}}))}{1-\exp(-2T_{\mathrm{S}}/\sigma_{\mathrm{T}})},\end{aligned} \tag{37}$$

$$E[P_{\mathrm{IUI}}(r)]=(N-1)\frac{[1+\exp(-2LT_{\mathrm{S}}/\sigma_{\mathrm{T}})][1+\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})]-2\exp[-(L+1)T_{\mathrm{S}}/\sigma_{\mathrm{T}}][1+\exp(T_{\mathrm{S}}/\sigma_{\mathrm{T}})]}{[1-\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})][1+\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})][1-\exp(-LT_{\mathrm{S}}/\sigma_{\mathrm{T}})]},\tag{38}$$

(38) 式中, N 为用户数, 即合法用户和窃听用户.

下面分析加人工噪声时窃听用户平均SINR以及对应的保密SINR.

由 (3), (16) 和 (21) 式得人工噪声平均功率为

$$E[P(AN)]=E\left[\boldsymbol{W}\boldsymbol{W}^{\mathrm{H}}\left|\sum_{m=1}^{M}(g_{m,\mathrm{r}}*h_{m,\mathrm{e}})\right|^2\right]=(1-\alpha)PE[P_{\mathrm{Sig}}(e)],\tag{39}$$

Art Noise即为AN, 窃听用户的平均SINR为

$$E[\gamma_{\mathrm{e}}']=\frac{\alpha PE[P_{\mathrm{Sig}}(e)]}{(1-\alpha)PE[P_{\mathrm{Sig}}(e)]+E[P_{\mathrm{ISI}}(e)]+E[P_{\mathrm{IUI}}(e)]+\sigma(e)^2}.\tag{40}$$

同理

$$E[P_{\mathrm{Sig}}(e)]=\frac{1+\exp(-LT_{\mathrm{S}}/\sigma_{\mathrm{T}})}{1+\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})},\tag{41}$$

$$E[P_{\mathrm{ISI}}(e)]=\frac{2\exp(-3T_{\mathrm{S}}/\sigma_{\mathrm{T}})[1-\exp[-(L-1)T_{\mathrm{S}}/\sigma_{\mathrm{T}}]]}{1-\exp(-2T_{\mathrm{S}}/\sigma_{\mathrm{T}})},\tag{42}$$

$$E[P_{\mathrm{IUI}}(e)]=(N-1)\frac{[1+\exp(-2LT_{\mathrm{S}}/\sigma_{\mathrm{T}})][1+\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})]-2\exp[-(L+1)T_{\mathrm{S}}/\sigma_{\mathrm{T}}][1+\exp(T_{\mathrm{S}}/\sigma_{\mathrm{T}})]}{[1-\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})][1+\exp(-T_{\mathrm{S}}/\sigma_{\mathrm{T}})][1-\exp(-LT_{\mathrm{S}}/\sigma_{\mathrm{T}})]},\tag{43}$$

平均保密SINR,

$$\overline{\gamma}_{\mathrm{s}}'=\frac{E[\gamma_{\mathrm{r}}]-E[\gamma_{\mathrm{e}}']}{1+E[\gamma_{\mathrm{e}}']}.\tag{44}$$

综上, 无论是否加人工噪声, 合法用户接收到的信号功率肯定大于窃听用户接收的信号功率, 因此, 在功率分配因子一定、合法用户和窃听用户噪声功率相同的情况下, 随着SNR的增加, 保密SINR逐渐增大.

3.2 可达保密速率

可达保密速率的数学描述为

$$R_{\mathrm{sec}}=\max[I(x,r_{\mathrm{r}})-I(x,r_{\mathrm{e}})],\tag{45}$$

r_{r}, r_{e} 分别表示合法用户和窃听用户接收到的信号.

3.2.1 聚焦区域不考虑加人工噪声

根据信息论知识以及前面的分析, 经过多径信道的合法用户和窃听用户的收发互信息表达式为

$$I(x;r_{\mathrm{r}})=\log_2(1+\gamma_{\mathrm{r}}),\tag{46}$$

$$I(x;r_{\mathrm{e}})=\log_2(1+\gamma_{\mathrm{e}}).\tag{47}$$

将 (46), (47), (27) 式代入 (45) 式可得可达保密速率表达式.

3.2.2 聚焦区域考虑加人工噪声

由物理层零空间法[10,17], 可达保密速率计算公式为

$$R_{\mathrm{sec}}=\max_{r,P}\log(1+\alpha P|H_{\mathrm{r}}|^2/\sigma_{\mathrm{r}}^2)-\log\left\{1+\frac{\alpha P|H_{\mathrm{e}}|^2}{(1-\alpha)P|H_{\mathrm{e}}h|^2+\sigma_{\mathrm{e}}^2}\right\},\tag{48}$$

其中 P 表示发送方的发射功率, α 表示功率分配因子, 定义为信号占发射功率的比值 ($0\leqslant\alpha\leqslant1$); σ_{r}^2, σ_{e}^2 分别为合法用户和窃听用户的信道噪声, 且 $\sigma_{\mathrm{r}}^2=\sigma_{\mathrm{e}}^2$; $h\in C^{M\times1}$ 表示 H_{r} 的零空间的标准正交基, 即 $H_{\mathrm{r}}H=0$, 且 $|h|^2=1$, 分配给噪声的那部分功率为 $(1-\alpha)P$. 采用TR技术后, 由 (27) 式, (45) 式可以表示为

$$R_{\mathrm{sec}}=\max_{\alpha,P}\log_2\{1+E[\gamma_{\mathrm{art}}(r)]\}-\log_2\{1+E[\gamma_{\mathrm{art}}(e)]\},\tag{49}$$

$\gamma_{\mathrm{art}}(r)$ 和 $\gamma_{\mathrm{art}}(e)$ 分别表示采用人工噪声后的合法用户和窃听用户的SINR, 且

$$E[\gamma_{\mathrm{art}}(r)]=\frac{\alpha PE[P_{\mathrm{Sig}}(r)]}{E[P_{\mathrm{ISI}}(r)]+E[P_{\mathrm{ISI}}(r)]+\sigma_{\mathrm{r}}^2},\tag{50}$$

$$E[\gamma_{\mathrm{art}}(e)]=\frac{\alpha PE[P_{\mathrm{Sig}}(e)]}{(1-\alpha)PE[P_{\mathrm{Sig}}(e)]+E[P_{\mathrm{ISI}}(e)]+E[P_{\mathrm{IUI}}(e)]+\sigma_{\mathrm{e}}^2}.\tag{51}$$

将(50), (51)式代入(49)式, 得可达保密速率表达式.

由上述推导可得出以下结论:

1) 随着α的逐渐增大, 即人工噪声比例越来越小, 直到$\alpha=1$时, 可达保密速率为0, 此时系统极不安全;

2) α一定的情况下, 总功率P逐渐增大, 可达保密速率逐渐增加.

3.3 误码率分析

3.3.1 聚焦区域不考虑加人工噪声

发送端采用QAM调制方式, 合法接收用户的接收功率为

$$P(r)=\left|\sum_{m=1}^{M}(g_{m,\mathrm{r}}*h_{m,\mathrm{r}})[L]\right|^2. \tag{52}$$

设合法信道和窃听信道噪声功率$\sigma_{\mathrm{r}}^2=\sigma_{\mathrm{e}}^2$. 则合法用户平均信噪比为$\mathrm{SNR}(r)=P(r)/\sigma_{\mathrm{r}}^2$, 对于合法用户, 各天线发送信号根据信道系数进行了加权, 与采用多接收天线, 并采用最大比值合并方式相当, 根据文献[26, 27], 合法用户平均误比特率

$$p_{\mathrm{e}}^{\mathrm{r}}=\left(\frac{1-\mu_{\mathrm{r}}}{2}\right)^M\sum_{i=0}^{M-1}\binom{M-1-i}{i}\times\left(\frac{1+\mu_{\mathrm{r}}}{2}\right)^i, \tag{53}$$

其中M为发射端的天线数量, μ_r的数学表达式是$\mu_r=\sqrt{\overline{\mathrm{SNR}}/(1+\overline{\mathrm{SNR}})}$, $\overline{\mathrm{SNR}}=\mathrm{SNR}/M$表示平均比特信噪比. 则(53)式中

$$\mu_{\mathrm{r}}=\sqrt{(\mathrm{SNR}(r)/M)/(1+\mathrm{SNR}(r)/M)},$$

对窃听用户而言, 平均接收功率

$$P(e)=\left|\sum_{m=1}^{M}(g_{m,\mathrm{r}}*h_{m,\mathrm{e}})[L]\right|^2. \tag{54}$$

窃听用户的平均信噪比为$\mathrm{SNR}(e)=P(e)/\sigma_{\mathrm{e}}^2$, 本文窃听用户信道状态已知, 窃听用户平均误比特率也可以根据(53)式来计算, 并且根据上述分析$\mu_{\mathrm{e}}=\sqrt{(\mathrm{SNR}(e)/M)/(1+\mathrm{SNR}(e)/M)}$.

3.3.2 聚焦区域考虑加人工噪声

由前面分析, 合法用户接收功率为

$$P'(r)=\alpha PP(r), \tag{55}$$

其中, P为总发送功率. 合法用户平均误比特率计算公式同(53)式.

窃听用户接收功率为

$$P'(e)=aPP(e), \tag{56}$$

而噪声功率为人工噪声功率与信道噪声功率之和. $n'(e)=\sigma_{\mathrm{e}}^2+(1-\alpha)P$, 窃听用户的平均信噪比$\mathrm{SNR}'(e)=P'(e)/[\sigma_{\mathrm{e}}^2+(1-a)P]$, 同3.3.1节分析, 窃听用户平均误比特率也可根据(53)式计算,

$$\mu_{\mathrm{e}}'=\sqrt{[\mathrm{SNR}'(e)/M]/[1+\mathrm{SNR}'(e)/M]},$$

窃听信道性能将在第4节通过仿真的方式说明.

由上述分析, 随着信噪比的逐渐增大, μ_{r}也逐渐增大, 由(53)式, 误比特率将逐渐减小, 即信噪比越大, 误比特率越小.

本节对影响系统安全性能的保密SINR、可达保密速率和误码率进行了分析, 得出如下结论:

1) 随着SNR的增加, 保密SINR逐渐增大;

2) α和P对可达保密速率有较大的影响;

3) 误比特率随SNR的增加逐渐减小.

4 仿真分析

本节通过链路级的仿真平台对所提出的传输机制进行仿真验证, 并与已有的物理层安全机制比较, 最后对所提出的机制进行性能分析.

在仿真中, 合法信道和窃听信道均服从多径瑞利衰落信道, 信道增益服从均值为0, 方差为$E[|h[l]|^2]=\mathrm{e}^{-lT_{\mathrm{S}}/\sigma_{\mathrm{T}}}$的CSCG随机变量. 设信道带宽$B=500$ MHz, 采样周期$T_{\mathrm{S}}=1/B=2$ ns, 均方根延迟扩展$\sigma_{\mathrm{T}}=100/B$, 典型信道长度$L$为80到150, 仿真中, 设置$L=117$. 本文分析了所提机制的多项性能, 包括合法用户的保密SINR、可达保密速率和误码率. 对比的机制包括文献[24]和文献[27]. 并且对这三种机制的理论结果和仿真结果进行了仿真, 下面对图3—图6的理论结果和仿真结果的来源进行说明.

图3中天线数$M=4$时, 从上往下看, 第一条实线表示本文TR+人工噪声的理论结果, 它是由(33)—(44)式得到的. 第二条略粗的实线表示的是由文献[24]方法得到的理论结果, 由(20)—(32)式得到. 第三条更粗的实线表示的是只加人工噪声的理论结果, 根据文献[27]方法得到. 方框表示的是本文TR+人工噪声的仿真结果, 由(20)—(33), (40)和(44)式得到. 三角表示的是由文献[24]方法得到的仿真结果, 由(20)—(29)式得到. 圆圈表示

的是只加人工噪声的仿真结果, 由文献 [27] 方法得到. 天线数 $M=2$ 时, 同理.

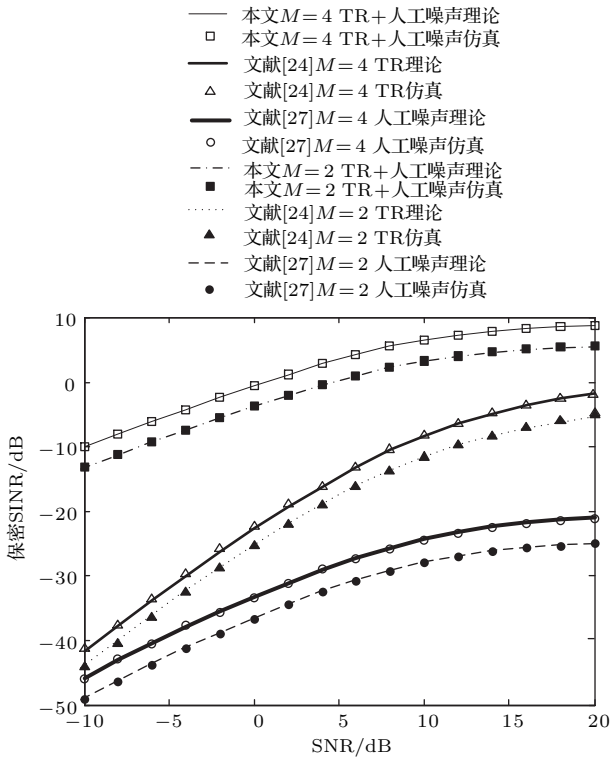

图 3 保密 SINR 与 SNR 的关系

Fig. 3. The Relationship between secure SINR and SNR.

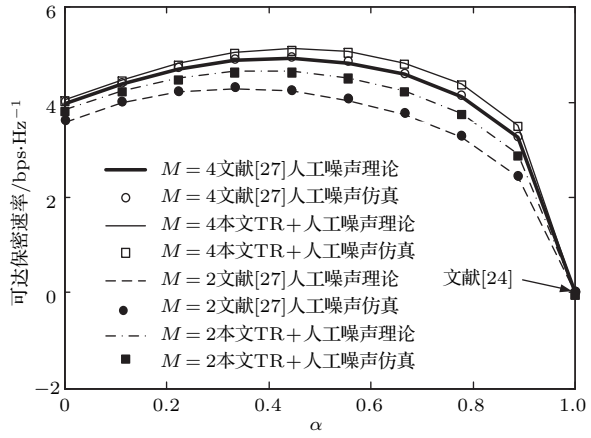

图 4 可达保密速率随 α 的变化

Fig. 4. Change of the security rate with α.

图 4 中天线数 $M=4$ 时, 第一条实线表示, 本文 TR+ 人工噪声的理论结果, 由 (36)—(38) 式, (41)—(43) 式和 (48)—(51) 式得到. 第二条较粗的实线表示的是只加人工噪声的理论结果, 根据文献 [27] 方法由公式得到. 方框表示的是本文 TR+ 人工噪声的仿真结果, 由 (20)—(25) 式和 (48)—(51) 式得到. 圆圈表示的是只加人工噪声的仿真结果, 由文献 [27] 方法得到. 由箭头指出的点由文献 [24] 方法得到. $M=2$ 时, 同理. 图 5 中理论结果与仿真结果, 与图 4 类似, 同理得到.

图 6 中天线数 $M=4$ 时, 从下往上, 第一条实线表示本文 TR+ 人工噪声的理论结果, 由 (36)—(38) 式, (41)—(43) 式和 (53), (55), (56) 式得到; 第二条略粗的实线表示的是由文献 [24] 方法得到的理论结果, 由 (36)—(38) 式, (41)—(43) 式和 (52)—(54) 式得到; 第三条更粗的实线表示的是只加人工噪声的理论结果, 根据文献 [27] 方法得到; 方框表示的是本文 TR+ 人工噪声的仿真结果, 由 (20)—(25) 式和 (53), (55), (56) 式得到; 三角表示的是由文献 [24] 方法得到的仿真结果, 由 (20)—(25) 式和 (52)—(54) 式得到; 圆圈表示的是只加人工噪声的仿真结果, 由文献 [27] 方法得到; 上面两条近似平行的线表示的是窃听信道的理论结果和仿真结果, 由文献 [27] 和本文方案得到.

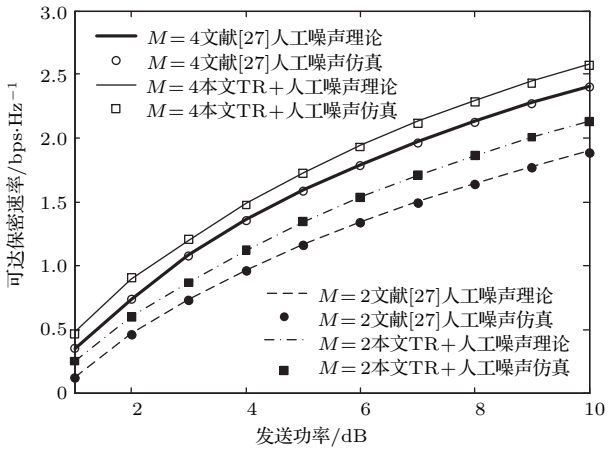

图 5 可达保密速率随功率 P 的变化

Fig. 5. Change of the security rate with P.

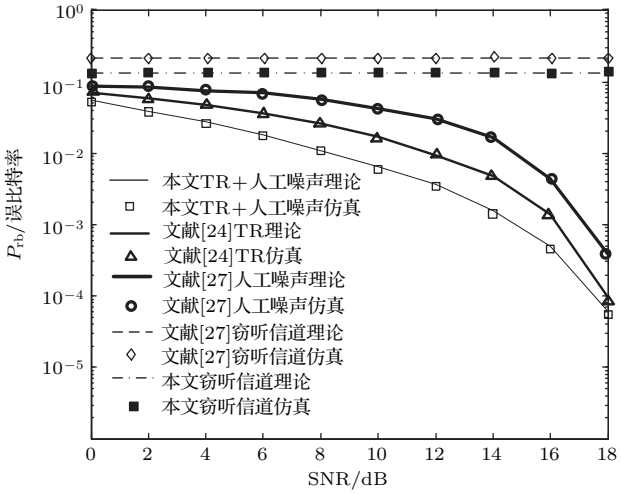

图 6 误比特率随 SNR 的变化

Fig. 6. Change of the bit error rate with SNR.

图3是多径信道下保密SINR随SNR变化的仿真结果, 发送天线数设为4和2, 用户数为2, 功率分配因子$\alpha = 0.3$. 从图中看出, 保密SINR随SNR的增加而增大, 天线数越多, 保密SINR越大. 对比文献[27]物理层人工噪声法和文献[24]只采用TR技术两种机制, 本文机制采用人工噪声和TR技术相结合的方法保密SINR更高, 安全性能更好, 且三种机制理论分析和仿真结果一致.

由(45)式, 可达保密速率衡量存在窃听用户时的系统的保密性能. 图4是功率分配因子随可达保密速率变化的仿真结果, 发送方总功率固定为$P = 20$ dB, 天线数$M = 4$和$M = 2$. 可达保密速率由10000次独立的蒙特卡罗仿真结果取平均得到, 下同.

从图4可以看出, 天线数越多, 可达保密速率越大. 相同条件下, 本文机制得到的可达保密速率始终大于文献[27]只采用人工噪声时的可达保密速率, 且两种机制的理论分析和仿真结果一致. 在P和M一定的条件下, 随着α增大, 可达保密速率先增大后减小, 并且两种机制的差异越来越小. 由可达保密速率表达式可以看出, 当$\alpha = 1$时, 即全部发送有用信号, 可达保密速率为0, 图4正好反映了这一点. 文献[24]只采用了TR技术, 此时的可达保密速率如图中箭头所示. 该结果表明, 信号和人工噪声功率的分配影响可获得的可达保密速率, 存在一个最佳的功率分配机制使可达保密速率最大. 当α较小时, 发送人工噪声的功率较多, 本文机制利用TR时间聚焦性在发端加干扰对合法接收方性能改善较大, 而随着α的增大, 人工噪声功率逐渐减小, 本文机制对合法接收端信噪比的改善作用也逐渐减小, 因此对可达保密速率的提升也相应减小.

图5是在最优的功率分配因子下, 可达保密速率随发射总功率P变化的仿真结果, 发射天线数目$M = 4$和$M = 2$. 从图中可以看出, 天线数越多, 可达保密速率越大. 当采用最优的功率分配因子时, 可达保密速率随发送方功率的增大而增大, 且可达保密速率近似呈线性增加, 本文机制的性能始终优于只采用人工噪声机制的性能, 且两种机制理论分析和仿真结果一致.

图6是QAM调制下合法用户和窃听用户的平均误比特率随SNR变化的结果, 发送端天线$M = 8$, 合法用户和窃听用户均采用最大似然译码. 从仿真结果可以看出, 合法用户误比特率的仿真结果与理论分析结果一致. 与传统人工噪声机制和只采用TR技术机制比较, 本文提出的机制在保证窃听用户误比特率基本不变的条件下, 降低了合法用户的误比特率, 提高了系统的安全性能.

5 总 结

针对物理层窃听信道模型, 本文首先提出一种基于TR技术的物理层安全传输机制, 得出保密SINR的闭合表达式. 通过理论分析和仿真得出: SNR越大, 系统的保密性能越好. 其次, 提出了一种人工噪声干扰和TR技术相结合的物理层安全传输机制, 并在保密SINR表达式的基础上, 推导得出可达保密速率的表达式. 仿真分析表明所提机制的可达保密速率较传统机制有明显提升. 最后, 基于传统零空间人工噪声方法, 推导得出只采用TR技术和人工噪声与TR技术相结合的合法接收用户和窃听用户的误比特率表达式. 仿真结果表明, 所提机制的合法用户的误比特率比传统机制合法用户的误比特率更低. 因此, 该传输机制可以提高系统的保密性能.

参考文献

[1] Zhao D S, Yue W J, Yu M, Zhang S X 2012 *Acta Phys. Sin.* **61** 074102 (in Chinese) [赵德双, 岳文君, 余敏, 张升学 2012 物理学报 **61** 074102]

[2] Ding S, Wang B Z, Ge G D, Wang D, Zhao D S 2011 *Acta Phys. Sin.* **60** 104101 (in Chinese) [丁帅, 王秉中, 葛广顶, 王多, 赵德双 2011 物理学报 **60** 104101]

[3] Chen Y, Wang B, Han Y, Lai H Q, Safar Z, Liu K J R 2016 *IEEE Signal Process. Mag.* **33** 17

[4] Wang B Z, Zang R, Zhou H C 2013 *J. Microwaves* **29** 22 (in Chinese) [王秉中, 臧锐, 周洪澄 2013 微波学报 **29** 22]

[5] Chen Y M, Wang B Z, Ge G D 2012 *Acta Phys. Sin.* **61** 024101 (in Chinese) [陈英明, 王秉中, 葛广顶 2012 物理学报 **61** 024101]

[6] Ge G D, Wang B Z, Huang H Y, Zheng G 2009 *Acta Phys. Sin.* **58** 8249 (in Chinese) [葛广顶, 王秉中, 黄海燕, 郑罡 2009 物理学报 **58** 8249]

[7] Nardis L D, Fiorina J, Panaitopol D, Benedetto M G D 2013 *Telecommun. Syst.* **52** 1145

[8] Zang R, Wang B Z, Ding S, Gong Z S 2016 *Acta Phys. Sin.* **65** 204102 (in Chinese) [臧锐, 王秉中, 丁帅, 龚志双 2016 物理学报 **65** 204102]

[9] Feng J, Liao C, Zhang Q H, Sheng N, Zhou H J 2014 *Acta Phys. Sin.* **63** 134101 (in Chinese) [冯菊, 廖成, 张青洪, 盛楠, 周海京 2014 物理学报 **63** 134101]

[10] Francisco P R, Juan V V, Pablo P, Francisco L V, Rafael L B, Miguel A L G 2016 *Sensors-Basel* **6** 1

[11] Lerosey G, de Rosny J, Tourin A, Derode A, Montaldo G 2004 *Phys. Rev. Lett.* **92** 1

[12] Zhang G M 2013 *M. S. Dissertation* (Chengdu: University of Electronic Science and Technology) (in Chinese) [张光旻 2013 硕士学位论文 (成都: 电子科技大学)]

[13] Alves H, Souza R D, Debbah M, Bennis M 2012 *IEEE Signal Process. Lett.* **19** 372

[14] Yang N, Suraweera H A, Collings I B, Yuen C 2013 *IEEE Trans. Inf. Forensics Security* **8** 254

[15] Tran D D, Ha D B, Tran H V, Hong E K 2015 *Iete J. Res.* **61** 363

[16] Rahmanpour A, Vakili V T, Razavizadeh S M 2017 *Wireless Pers. Commun.* **95** 1533

[17] Zhang L, Zhang H, Wu D, Yuan D 2015 *IEEE Global Communications Conference* San Diego, CA, USA, Dec. 6–10, 2015 p1

[18] Wang W, Teh K C, Li K H 2017 *IEEE Trans. Inf. Forensics Security* **12** 1470

[19] Alves H, Souza R D, Debbah M, Bennis M 2012 *IEEE Signal Process. Lett.* **19** 372

[20] Tran D D, Ha D B, Tranha V, Hong E K 2015 *Iete J. Res.* **61** 363

[21] Cao W, Lei J, Liu W, Li X T 2014 *Communications Security Conference* Beijing, China, May 22–24, 2014 p1

[22] Tran V T, Ha D B, Tran D D 2014 *Computing, Management and Telecommunications* Da Nang, Vietnam April 27–29, 2014 p70

[23] Amirzadeh A, Taieb M H, Chouinard J Y 2017 *Canadian Workshop on Information Theory* Quebec City, QC, Canada June 11–14, 2017 p1

[24] Han F, Yang Y H, Wang B B, Wu Y L, Rayliu K J 2012 *IEEE Trans. Commun.* **60** 1953

[25] Feng Y, Hou X Y, Wei H, Zhu Y, Gao L 2014 *Computer Technol. Develop.* **12** 146 (in Chinese) [冯元, 侯晓赟, 魏浩, 朱艳, 高磊 2014 计算机技术与发展 **12** 146]

[26] Simon M, Alouini M 2005 *Digital Communication over Fading Channels of Second Order* (Hoboken: Wiley-Interscience) pp17–43

[27] Lei W J, Lin X Z, Yang X Y, Xie X Z 2016 *JEIT* **38** 2887 (in Chinese) [雷维嘉, 林秀珍, 杨小燕, 谢显中 2016 电子与信息学报 **38** 2887]

[28] Wang B, Wu Y, Han F, Yang Y H, Liu K J R 2011 *IEEE J. Sel. Area. Commun.* **29** 1698

[29] Zhao L K 2013 *M. S. Dissertation* (Zhengzhou: The PLA Information Engineering University) (in Chinese) [赵刘可 2013 硕士学位论文 (郑州: 解放军信息工程大学)]

[30] Emami M, Vu M, Hansen J, Paulraj A J, Papanicolaou G 2004 *Signals, Systems and Computers* Pacific Grove, CA, USA, USA, Nov. 7–10, 2004 p218

[31] Moose P H 1994 *IEEE Trans. Common.* **42** 2908

[32] Lee J, Lou H L, Toumpakaris D, Cioffi J M 2006 *IEEE Trans. Wireless Commun.* **5** 3360

Secure transmission mechanism based on time reversal over wireless multipath channels*

Zhu Jiang Wang Yan† Yang Tian

(*Chongqing Key Laboratory of Mobile Communications Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China*)

(Received 27 September 2017; revised manuscript received 7 December 2017)

Abstract

Broadband wireless communication is implemented primarily in a complicated environment. The complex environment with time-varying multi-path propagation characteristics will seriously affect the performance of communication. To solve the problem of insecurity in information transmission in wireless channels, in this paper a system is modeled by using the multi-input single output eavesdropping channel model and the security of information transmission through time reversal technology is ensured. Another problem is that the information focuses on the receiving point. Owing to the temporal and spatial focusing characteristics of the time reversal technology the information near the receiving point can be eavesdropped easily. To solve this problem, a secure transmission scheme based on time reversal technology with artificial noise interference on the transmitter side is proposed. One of the core technologies to solve this problem is to introduce the environment adaptive technique—time reversal in the wireless link. Further, the problem of a wiretap channel in physical layer security research has become a popular research topic in recent years. To solve the problems about the physical layer wiretap channel and multi-path fading in wireless channels, a novel concept combining time reversal technology with physical layer security technology is proposed. In this paper, a physical layer secure transmission scheme based on the joint time reversal technique and artificial noise at the sending end is proposed for the wireless multi-path channel. First, in a typical wiretap channel model the time reversal technique is used to improve the security of the information transmission process by using the properties of spatial and temporal focusing. It refers to the fact that information can be focused at a given moment and in space. Second, as the information is easily eavesdropped near the focus point, artificial noise is added to the sending end to disrupt the ability of the eavesdropper to eavesdrop. The artificial noise has no effect on legitimate user due to the use of null-space artificial noise in legitimate user. Based on this scheme, a closed expression, such as secure signal-to-interference and signal-to-noise ratio, an achievable secrecy rate and bit error rate are obtained, and the influences of the number of antennas, signal-to-noise ratio, and artificial noise are analyzed. The theoretical analysis and simulation results show that the proposed scheme has a higher secrecy signal-to-noise ratio, a higher rate of secrecy, and a lower bit error rate of the legitimate user than the the existing physical layer security schemes.

Keywords: wiretap channel, time reversal, artificial noise, spatial and temporal focusing

PACS: 02.10.Xm, 05.45.–a, 84.40.Ua, 43.60.Gk **DOI:** 10.7498/aps.67.20172134

* Project supported by the National Natural Science Foundation of China (Grant No. 61771084) and the Natural Science Foundation of Chongqing Science and Technology Commission, China (Grant No. cstc2015jcyjA40050).

† Corresponding author. E-mail: xiaoyanzi_19911130@163.com