无线通信中使用随机天线阵列的物理层安全传输方法

穆鹏程[1,2]，殷勤业[1,2]，王文杰[1,2]
(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：为了在无线通信过程中保证信息安全，提出了一种使用随机天线阵列的物理层安全传输方法(RAA方法).该方法在基站端使用多天线而在移动用户端使用单天线，期望移动用户首先发送同步训练符号，基站根据接收到的训练符号估计信道，然后基站随机选取若干天线并根据估计到的信道使用分布式波束形成的方法进行加权发射，各天线发射信号最后在期望用户接收点同相叠加，期望用户可以直接进行最大似然解调.由于基站在发射每个符号时都随机变换天线，将会导致窃听者的信道随机快速变化，因此窃听者无法通过盲均衡算法解调，从而保证了信息的低截获概率.与经典的使用随机加权系数的方法相比，RAA方法具有功率利用率更高的特点.仿真结果表明，在总功率一定的情况下，RAA方法可以在期望用户处获得比已有方法低一个数量级的误码率，而窃听者始终无法正确解调.

关键词：无线通信；物理层安全；低截获概率；天线阵列；波束形成
中图分类号：TN929.5 **文献标志码**：A **文章编号**：0253-987X(2010)06-0062-05

A Security Method of Physical Layer Transmission Using Random Antenna Arrays in Wireless Communication

MU Pengcheng[1,2], YIN Qinye[1,2], WANG Wenjie[1,2]
(1. MOE Key Laboratory 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: A method of using random antenna arrays (RAA) is proposed to guarantee the information security during the physical layer transmission. The method uses multiple antennas at the base station and a single antenna at each mobile terminal. When expected mobile terminals (target users) transmit training symbols. the base station estimates the channel from the symbols. Then the base station randomly selects several antennas for weighted transmission, and the weighting coefficients are obtained by using the method of distributed beamforming according to the estimated channel. Signals from all the selected antennas are finally superimposed at the target user so that the maximum likelihood demodulation can be directly employed. The base station randomly changes antennas to transmit each symbol, which makes the channel of any eavesdropper change fast. Hence the eavesdropper can not demodulate his received signals by blind equalization, and the low probability of interception is achieved. A comparison with the traditional method of using random weighting coefficients shows that the RAA method improves the utilization of power. Simulation results show that the bit error rate of the RAA method is reduced by one order of magnitude at the target user, while the eavesdropper can not demodulate correctly.

Keywords: wireless communication; physical layer security; low probability of interception; antenna array; beamforming

收稿日期：2010-02-18. 作者简介：穆鹏程(1980—)，男，博士后；殷勤业(联系人)，男，教授，博士生导师. 基金项目：国家自然科学基金资助项目(60971113)；国家创新群体科学基金资助项目(60921003).

近年来，无线通信技术在军事民用等各方面得到了广泛应用，在给人们带来便利的同时，无线信道的开放性也使得信息安全问题变得越来越突出[1-2]. 传统的有线通信通常使用数据加密等方法来保障通信安全，尽管这些方法在无线通信中仍然可行，但它们都没有完全弥补由无线信道的开放性所造成的安全漏洞. 如果能够充分考虑无线信道的特点，那么就有可能从根源上解决无线通信安全问题.

针对无线信道特点解决无线通信安全问题的方法主要有 2 类：①利用无线信道的互易性和私密性，通信双方分别根据提取到的信道特征独立生成密钥进行加密的方法[3-4]，这类方法可以避免密钥的传输泄漏，但主要难点是在噪声干扰造成双方估计的无线信道参数不完全一致时如何生成一致的密钥；②利用无线信道的空域特征实现物理层安全传输，其主要思路是通过提高窃听者的误码率来达到防止信息被截获（低截获概率，LPI）的目的. 使用多无线技术的多输入多输出系统可以充分利用无线信道的空域特征，因此文献[5-6]提出了一种基于阵列冗余进行物理层安全传输的方法，通过随机选取各阵元的加权系数，造成基站与窃听者之间的等效信道快速随机变化，当窃听者使用恒模算法（CMA）等盲均衡[7-9]算法进行迭代时无法收敛，从而达到低截获概率的目的. 该方法的主要问题是功率利用率太低，需要很强的发射功率才能保证期望用户的通信质量.

针对上述随机加权系数造成功率利用率过低的问题，本文提出一种在天线阵列固定的情况下通过每次随机选取若干天线发射以达到等效信道随机变化的目的. 权系数的选择采用分布式发射波束形成[10]，使得各阵元发出的信号在期望用户处始终同相叠加以得到最高的发射增益，因此功率利用率极高. 信道的随机快变造成窃听者每次接收到的信号增益和相移都会随机变化，因此无法有效地通过盲均衡算法解调信息. 仿真实验表明，本文方法在保证窃听者低截获概率的同时，功率利用率更高，在发射总功率一定的情况下可使期望用户获得更低的接收误码率.

1　无线安全传输系统模型

图 1 给出了无线安全传输的系统模型，主要涉及 3 方：Alice 作为基站需要把信息安全传输给期望移动用户 Bob，Eve 作为窃听者只进行被动接收而不做任何主动发射. 一般情况下 Alice 和 Eve 均使用多天线，而 Bob 则使用单天线. 此外，这种无线安全传输模型中一般要求收发信道可以互易，当信道慢变时，这种互易性可以通过时分双工（TDD）得到充分保证[11].

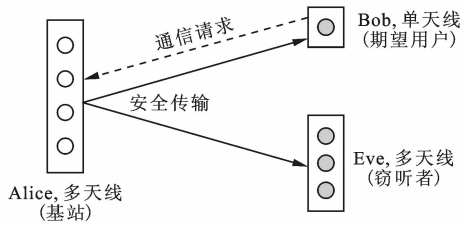

图 1　无线安全传输系统模型

通信过程中 Bob 首先向 Alice 发送未加密的请求信息，该请求信息同时包含用于信道估计的训练符号序列；Alice 使用多天线接收请求信息，并根据接收到的信号估计他们之间的信道. 考虑到系统使用时分双工并且信道慢变，则根据互易原理可以认为 Alice 与 Bob 之间的收发信道相同，因此 Alice 可以根据估计到的信道对即将发送给 Bob 的信息进行加权，也可以看作是一种加密. 在这种情况下，Alice 与 Bob 之间的信道即为 Alice 使用的密钥，加密过的信息经过无线传输到达 Bob 后自动完成解密，因此 Bob 无需知道 Alice 使用的密钥即可直接解出发射符号序列.

以上过程中只有 Bob 发送用于信道估计的训练符号序列，Alice 根据该训练符号估计信道而不发送任何训练符号序列，在这种情况下，Bob 和 Eve 均无法估计他们与 Alice 之间的信道信息，因此处于一种盲状态. 由于 Alice 发出的加密信号经过 Alice 与 Bob 之间的信道时自动完成解密，因此这种盲状态对于 Bob 没有任何影响；相反，该加密信号经过 Alice 与 Eve 的信道时并不能自动完成解密，而且由于 Eve 无法知道 Alice 与其之间的信道，因此也就无法准确得到 Alice 发送的经过加密的信号，更不可能对该信号进行解密.

假设 Alice 使用 J 根天线，Bob 使用单根天线，Eve 使用 M 根天线，则 Alice 与 Bob 之间的信道可以表示为如下 $J\times 1$ 维向量

$$\boldsymbol{h}_{\mathrm{AB}}=[h_{\mathrm{AB},1},h_{AB,2},\cdots,h_{AB,J}]^{\mathrm{T}} \tag{1}$$

而 Alice 与 Eve 之间的信道可以表示如下

$$\boldsymbol{h}_{\mathrm{AE}}=\begin{bmatrix} h_{\mathrm{AE},1,1} & h_{\mathrm{AE},1,2} & \cdots & h_{\mathrm{AE},1,M} \\ h_{\mathrm{AE},2,1} & h_{\mathrm{AE},2,2} & \cdots & h_{\mathrm{AE},2,M} \\ \vdots & \vdots & & \vdots \\ h_{\mathrm{AE},J,1} & h_{\mathrm{AE},J,2} & \cdots & h_{\mathrm{AE},J,M} \end{bmatrix} \tag{2}$$

Alice 把映射成星座点的符号 $b(n)$ 分配到各个天线上，再通过加权后发射出去，假设 Alice 的发射

总功率固定为 P，各天线的归一化权系数 $\boldsymbol{w}$（$\|\boldsymbol{w}\|=(\boldsymbol{w}^{\mathrm{H}}\boldsymbol{w})^{1/2}=1$），则由 J 根天线发出的信号构成的 $1\times J$ 维向量为

$$\boldsymbol{s}(n)=[s_1(n),s_2(n),\cdots,s_J(n)]=b(n)P\boldsymbol{w}^{\mathrm{H}} \tag{3}$$

这种安全传输方式类似于发射波束的形成，图 2 给出了从发射到接收的整个信号流程.

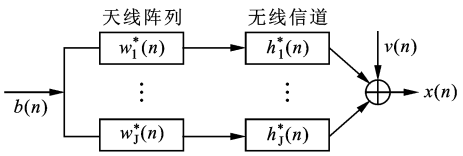

图 2 无线安全通信中的发射波束形成

对于 Bob 和 Eve 来说，他们的接收信号可以分别表示为

$$\boldsymbol{x}_{\mathrm{Bob}}(n)=s(n)\boldsymbol{h}_{\mathrm{AB}}+\boldsymbol{v}_{\mathrm{Bob}}(n)=b(n)P\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AB}}+\boldsymbol{v}_{\mathrm{Bob}}(n) \tag{4}$$

$$\boldsymbol{x}_{\mathrm{Eve}}(n)=\boldsymbol{s}(n)\boldsymbol{h}_{\mathrm{AE}}+\boldsymbol{v}_{\mathrm{Eve}}(n)=b(n)P\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AE}}+\boldsymbol{v}_{\mathrm{Eve}}(n) \tag{5}$$

式中：$\boldsymbol{v}_{\mathrm{Bob}}(n)$和 $\boldsymbol{v}_{\mathrm{Eve}}(n)$分别为 Bob 和 Eve 接收到的噪声信号.

2 无线安全传输方法

当信道缓慢变化时，如果阵列加权系数 $\boldsymbol{w}$ 不变或者也缓慢变化，那么 Eve 可以通过 CMA 等盲均衡算法[7-9]估计出式(5)中的 $P\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AE}}$，进而得到发射符号 $b(n)$. 为了防止信息被截获，在信道缓慢变化的情况下只有让加权系数 $\boldsymbol{w}$ 快速变化才能防止 Eve 对 $P\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AE}}$的跟踪. 为了达到这一目的，文献[5]提出了一种基于阵列冗余的随机加权无线安全传输方法，其核心思想是在 Alice 完全知道信道信息 $\boldsymbol{h}_{\mathrm{AB}}$的前提下随机选取 $\boldsymbol{w}$ 并使其满足

$$\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AB}}=\|\boldsymbol{h}_{\mathrm{AB}}\| \tag{6}$$

式中：$\|\boldsymbol{h}_{\mathrm{AB}}\|=(\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AB}})^{1/2}$. 具体实施时可以随机选定 $\boldsymbol{w}$ 中的 $J-1$ 个权系数，而最后一个权系数的选择必须使 $\boldsymbol{w}$ 满足式(6).

考虑到发射总功率固定为 P，因此还需对满足式(6)的权系数进行归一化，在这种情况下 Bob 的接收信号为

$$\boldsymbol{x}_{\mathrm{Bob}}(n)=b(n)\frac{P}{\|\boldsymbol{w}\|}\|\boldsymbol{h}_{\mathrm{AB}}\|+\boldsymbol{v}_{\mathrm{Bob}}(n) \tag{7}$$

于是 Bob 不需要额外的处理就可以通过下式直接解映射得到发射符号的估计值

$$\hat{b}(n)=\arg\min_{b(n)}\left|b(n)\frac{P}{\|\boldsymbol{w}\|}\|\boldsymbol{h}_{\mathrm{AB}}\|-\boldsymbol{x}_{\mathrm{Bob}}(n)\right|^2 \tag{8}$$

如果使用 BPSK 或 QPSK 等基于相位调制的数字调制方法，由于信息全部包含在发射符号的相位中，幅度的影响可以完全忽略，因此解调时只需考虑接收符号的相位，于是式(8)可以进一步简化为

$$\hat{b}(n)=\arg\min_{b(n)}|b(n)-\boldsymbol{x}_{\mathrm{Bob}}(n)|^2 \tag{9}$$

对于 Eve 来说，其接收信号可以表示为

$$\boldsymbol{x}_{\mathrm{Eve}}(n)=b(n)\frac{P}{\|\boldsymbol{w}\|}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AE}}+\boldsymbol{v}_{\mathrm{Eve}}(n) \tag{10}$$

上式表明，权系数 $\boldsymbol{w}$ 的随机变化使 Eve 无法有效地跟踪$\frac{P}{\|\boldsymbol{w}\|}\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AE}}$的变化，从而无法解出发射符号. 仿真与实际测试均表明这种方法能够很好地完成无线安全传输的功能，但它最大的问题是功率利用率太低，需要很大的发射功率才能使 Bob 获得较低的误码率.

事实上，无线信道加密的关键是让 Eve 无法有效跟踪 $P\boldsymbol{w}^{\mathrm{H}}\boldsymbol{h}_{\mathrm{AE}}$的变化，从而使 CMA 等盲均衡算法失效，同时还需要在功率受限的情况下尽可能地提高 Bob 的通信质量. 为此，本文提出以下无线安全通信机制：

(1)Bob 向 Alice 发送训练符号序列，Alice 通过接收该序列估计出他们之间的信道 $\boldsymbol{h}_{\mathrm{AB}}$；

(2)Alice 把符号 $b(n)$随机分配到若干个天线上分别进行加权后发射，使得各天线发射的信号在 Bob 处始终同相位叠加，而在 Eve 处具有随机变化的幅度和相位.

假定 Alice 在每次发送符号 $b(n)$时均随机使用 J_{rand}根天线，记 $\boldsymbol{I}_{\mathrm{rand}}(n)$是一个 $J\times J$ 维的随机选择矩阵，其中 $\boldsymbol{I}_{\mathrm{rand}}(n)$的对角线上随机排布了 J_{rand}个 1，其余元素均为 0，这种随机性体现在发送每个符号 $b(n)$时 $\boldsymbol{I}_{\mathrm{rand}}(n)$都会随机变化. 为了保证同相叠加，各天线的加权系数可以使用下式表示

$$\boldsymbol{w}(n)=\frac{\boldsymbol{h}_{\mathrm{AB}}}{\|\boldsymbol{h}_{\mathrm{AB}}\|} \tag{11}$$

则经过随机选择后各天线的归一化权系数变为

$$\boldsymbol{w}(n)=\frac{\boldsymbol{I}_{\mathrm{rand}}(n)\boldsymbol{h}_{\mathrm{AB}}}{\|\boldsymbol{I}_{\mathrm{rand}}(n)\boldsymbol{h}_{\mathrm{AB}}\|} \tag{12}$$

它仍然满足同相叠加的要求. 将式(12)带入式(4)得

$$\boldsymbol{x}_{\mathrm{Bob}}(n)=b(n)P\frac{\boldsymbol{h}_{\mathrm{AB}}^{\mathrm{H}}\boldsymbol{I}_{\mathrm{rand}}(n)}{\|\boldsymbol{I}_{\mathrm{rand}}(n)\boldsymbol{h}_{\mathrm{AB}}\|}\boldsymbol{h}_{\mathrm{AB}}+\boldsymbol{v}_{\mathrm{Bob}}(n)=b(n)P\|\boldsymbol{I}_{\mathrm{rand}}(n)\boldsymbol{h}_{\mathrm{AB}}\|+\boldsymbol{v}_{\mathrm{Bob}}(n) \tag{13}$$

于是 Bob 可以使用下式解出发射符号 $b(n)$

$$\hat{b}(n)=\arg\min_{b(n)}\mid b(n)P\parallel \boldsymbol{I}_{\mathrm{rand}}(n)\boldsymbol{h}_{\mathrm{AB}}\parallel -\boldsymbol{x}_{\mathrm{Bob}}(n)\mid^2 \tag{14}$$

这里虽然 $\boldsymbol{I}_{\mathrm{rand}}(n)$ 会随机变化，但是幅度部分 $P\parallel \boldsymbol{I}_{\mathrm{rand}}(n)\boldsymbol{h}_{\mathrm{AB}}\parallel$ 基本不变，保证 Bob 可以正确解映射. 如果采用 BPSK 或 QPSK 等相位调制方法，则幅度变化对解映射没有影响，因此还可以使用简化了的式(9)解出发射符号.

3　仿真验证

通过仿真对本文提出的无线安全传输方法进行验证. 发送 10 000 包测试数据，每包数据由 100 个随机生成的 QPSK 调制符号组成. 测试过程中做以下假设：

(1)信道在每包数据的持续期内保持不变，而在不同数据包之间独立变化；

(2)每对发射/接收天线之间的随机信道相互独立，每个信道的实虚部也相互独立，都服从均值为 0、方差为 0.5 的正态分布，因此信道增益为 1；

(3)每根接收天线收到的噪声信号的实虚部相互独立，都服从均值为 0、方差为 0.5 的正态分布，因此噪声功率为 1.

仿真中把本文方法与文献[5]中的方法进行对比，并称该方法为参考方法，其中除了与最大信道增益(即$|\boldsymbol{h}_{\mathrm{AB},i}|$最大)所对应的天线加权系数待定外，其余 $J-1$ 根天线的随机权系数均服从均值为 0、实虚部方差分别为 0.25 的正态分布，待定的天线加权系数通过式(6)确定.

首先对比在不同发射功率情况下本文方法与参考方法的安全传输性能. 仿真中要求 Alice 使用 8 根天线，Bob 使用单天线，Eve 使用 4 根天线. 本文方法每次随机选取 4 根天线，图 3 给出不同发射功率下本文方法与参考方法的误码率对比. 可以看出，随着发射功率的增加，Bob 的误码率会显著降低，并且在发射功率相同的情况下本文方法能够获得比参考方法更低的误码率，而 Eve 在不知道 $\boldsymbol{h}_{\mathrm{AB}}$ 和 $\boldsymbol{h}_{\mathrm{AE}}$ 的盲状态下误码率恒为 50%. 假设在理想情况下 Eve 知道了 $\boldsymbol{h}_{\mathrm{AB}}$ 和 $\boldsymbol{h}_{\mathrm{AE}}$，则使用两种方法时 Eve 的误码率都会有所降低，并且会随着发射功率的提高而下降. 尽管这种情况下本文方法比参考方法表现稍差，但是 Eve 的误码率与 Bob 比起来仍然非常高. 事实上，这种在 Eve 看来的理想状况正是本文方法要极力避免的，而在本文的传输机制下实际上也是不可能出现的，图 3 中本文方法的理想状态误码曲线仅仅被当作是 Eve 误码率的极限.

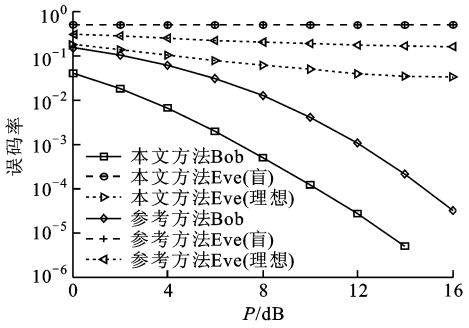

图 3　误码率随发射功率的变化情况

图 4 给出了不同发射功率下本文方法与参考方法在不同接收端的信噪比，可以看出，使用本文方法之所以能让 Bob 获得更低的误码率是因为该方法使 Bob 的接收信噪比相比参考方法有很大提高(5 dB)，这正是同相叠加带来的好处. 由于两种方法都没有针对 Eve 做特殊处理，因此两种情况下 Eve 的接收信噪比完全相同.

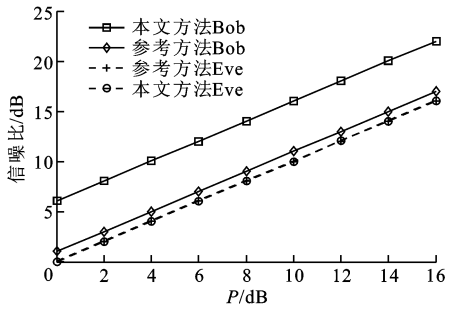

图 4　信噪比随发射功率的变化情况

在发射功率一定的情况下还可以测试安全传输性能与随机天线数之间的关系. 为此，Alice 仍然使用 8 根天线，Bob 使用单天线，Eve 使用 4 根天线，固定发射功率为 8 dB. 如图 5 所示，由于发射功率不变，参考方法的误码率保持不变，但是本文方法中 Bob 的误码率会随着随机天线数的增加而降低，Eve 在盲状态下的误码率始终为 50%. 假设在完全理想的情况下，Eve 知道了 $\boldsymbol{h}_{\mathrm{AB}}$ 和 $\boldsymbol{h}_{\mathrm{AE}}$，那么信道的随机性会随着选取天线数的增加而越来越差，Eve 的误码率也就会随着随机天线数的增加而下降.

图 6 给出了不同随机天线数下接收端的信噪比. 从图中可以看出，参考方法由于每次使用全部的 8 根天线，因此其信噪比不会随着随机天线数的变化而变化，而本文方法中 Bob 的接收信噪比会随着随机天线数的增加而增加，并且很快超过参考方法所能达到的信噪比，这也就是图 5 中 Bob 的误码率能够随着随机天线数的增加而降低的原因.

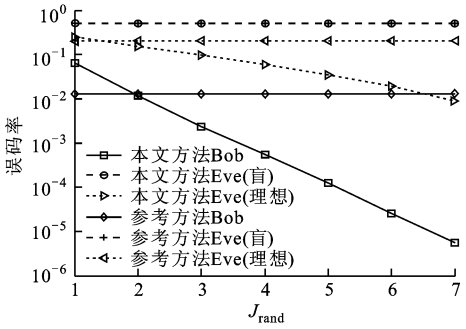

图5 误码率随随机天线数的变化情况

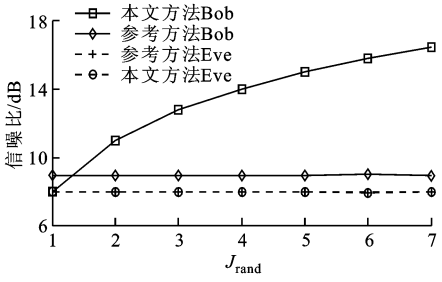

图6 信噪比随随机天线数的变化情况

4 结 论

无线通信安全除了需要使用传统的数据加密方法外,还应当充分利用无线信道本身的特点在物理层进行安全传输.本文提出了一种新的使用多天线的无线安全传输方法,该方法在基站端天线阵列固定的情况下通过每次随机选取若干天线以达到加权系数随机变化的目的,而权系数的选择采用分布式发射波束形成的思想,使得各阵元发出的信号在期望用户处同相叠加以得到最高的发射增益.这种通过阵列加权使得发射信号在接收点同相叠加的思想其本质上是一种"点聚焦",而发射信号由于聚焦于一点,因此功率非常集中,利用率也就非常高.天线的随机选择使得基站与窃听者之间的信道随机快速变化,因此窃听者无法有效地通过盲均衡算法来获取基站所发射的信息.仿真结果表明,本文的方法在保证窃听者低截获概率的同时,由于其功率利用率更高,使得在发射总功率一定的情况下期望用户可以获得更低的误码率.与经典的使用随机加权系数的方法相比,本文方法具有更好的安全传输性能,也更适合于在实际系统中使用.

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): 455-466.

[2] PATHAN 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] AONO K, HIGUCHI T, OHIRA B, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels [J]. IEEE Transactions on Antennas and Propagation, 2005, 53(11): 3776-3784.

[4] WILSON R, TSE D, SCHOLTZ R A. Channel identification: Secret sharing using reciprocity in UWB channels [J]. IEEE Transactions on Information Forensics and Security, 2007, 2(3): 364-375.

[5] LI Xiaohua, HWU J, RATAZZI E P. Array redundancy and diversity for wireless transmissions with low probability of interception [C] // Proceedings of the 2006 IEEE International Conference on Acoustics, Speech and Signal Processing. Piscataway, NJ, USA: IEEE, 2006: 525-528.

[6] LI Xiaohua, HWU J, RATAZZI E P. Using antenna array redundancy and channel diversity for secure wireless transmissions [J]. Journal of Communications, 2007, 2(3): 24-32.

[7] GODARD D N. Self-recovering equalization and carrier tracking in two-dimensional data communication systems [J]. IEEE Transactions on Communications, 1980, 28(11): 1867-1875.

[8] HAYKIN S. Unsupervised adaptive filtering, II: blind deconvolution [M]. New York, USA: Wiley, 2000.

[9] LI Xiaohua. Blind channel estimation and equalization in wireless sensor networks based on correlations among sensors [J]. IEEE Transactions on Signal Processing, 2005, 53(4): 1511-1519.

[10] JOHNSON D H, DUDGEON D E. Array signal processing, concepts and techniques [M]. Upper Saddle River, NJ, USA: Prentice Hall, 1993.

[11] PROAKIS J. Digital communications [M]. New York, USA: McGraw-Hill, 2000.

(编辑 刘杨)