论 文

随机发送参考的多天线系统物理层安全传输算法

吉江*, 刘璐, 金梁, 黄开枝

国家数字交换系统工程技术研究中心, 郑州 450002

* 通信作者. E-mail: jijinjiang@sohu.com.cn

收稿日期: 2013-04-23; 接受日期: 2013-11-01

国家自然科学基金 (批准号: 61171108) 资助项目

摘要 文中提出基于随机发送参考的多天线系统传输算法, 用于保障物理层信息安全传输. 该算法将授权用户的信道分解为多个独立并行的信道, 并在其中的一个信道中发送随机化的导频信息, 同时对其他信道加密. 由于窃听方信道与授权用户不同, 很难通过自身的信道分解出独立的随机化导频信道, 从而无法正常解调、还原信息. 通过理论分析及算法仿真表明, 随机发送参考算法可使窃听方的误码率稳定在较高水平, 并且在同等发送功率的情况下性能优于现有加性人工方法.

关键词 无线通信 多天线系统 物理层安全 导频 随机参考

1 引言

多天线系统可等价于多个独立的并行信道, 能够提供较高的系统容量, 因此已被广泛地应用于各种通信场景中. 但由于信道的开放性, 无线信号极易被捕获, 导致多天线系统在高速传输数据的同时存在较大的物理层安全隐患. 现有针对多天线系统物理层安全的研究主要集中于三个方面: 1) 利用传统的密钥思路对物理层进行加密^[1], 这类方法在密钥产生、传输、管理等方面都存在着安全隐患; 2) 利用通信的多个协议层进行跨层设计, 在设计中主要利用各层特点实现联合加密, 但其设计和实现复杂度通常较高^[2]; 3) 利用无线信道的差异性实现物理层的无密钥安全传输, 是目前最受关注的研究方向. 其主要衡量指标是保密容量^[3,4], 其表达式为

$$C_s = \max_{P_X, P_{Y|Z|X}} [I(X; Y) - I(X; Z)], \quad (1)$$

其中 X 为发送信息; Y 为授权用户接收的信息; Z 为窃听用户接收的信息. (1) 式的含义是当发送端与授权用户通信时, 存在某种安全信道编码, 使得窃听方完全无法截获信息的前提下授权用户所能达到的最大信道容量即为 C_s . 第三类中, 较为典型算法如文献 [5,6] 所提出利用天线阵列冗余的安全传输算法, 文献 [7,8] 提出了在多天线系统中引入加性人工噪声的方法. 这两种方法本质上均是在授权用户的信道状态向量方向上稳定传输信息, 同时在其正交的方向上引入人工噪声. 导致授权用户顺利接收信号的同时恶化窃听者的信号质量, 从而形成较大的保密容量. 但这种思路的前提是利用额外的一份功率去干扰窃听者, 其功率利用率较低. 尤其是当信道向量相似度较高时, 将耗费巨大的功率开销. 因此如何以较高的功率利用率实现无密钥安全传输, 是亟待解决的问题.

引用格式: 吉江, 刘璐, 金梁, 等. 随机发送参考的多天线系统物理层安全传输算法. 中国科学: 信息科学, 2014, 44: 254-262, 10.1360/112012-450

图 1 多天线系统物理层安全传输模型

Figure 1 The physical layer security model of MIMO system

为此, 文中提出基于随机发送参考的多天线传输算法. 参照传统研究工作, 算法假设合法通信双方已经获得了信道信息, 而窃听者可以获知自身信道, 但未知合法信道信息. 首先通过奇异值分解将授权用户的信道状态分解为多个独立并行的信道; 在其中一个信道上传输随机的导频信号, 该导频主要用于对其他信道进行实时加密. 授权用户可凭借该导频信道的信息完成其他信道的信号解调, 而窃听者由于信道的差异性, 很难获得该随机导频并进行信号还原, 从而实现了多天线系统的安全传输.

2 MIMO 系统的安全传输模型

文中所讨论的 MIMO 系统安全模型如图 1 所示, 用 Alice 表示发送者, 其具有 N 根发射天线; Bob 表示合法接收者, Eve 表示窃听者, 二者均具有 M 根接收天线. Alice 发送的信息 X 经编码、加密系统 G 后传输到无线信道. G 表示对 X 的线性预处理时变矩阵, 本文的设计目标即是设计 G 使得信息 X 可以安全的传输到 Bob 端. Bob 和 Eve 的接收信号分别为 Y_B 和 Y_E , 经过符号硬判决后得到 $\hat{X}_B$ 和 $\hat{X}_E$, 最后经过解码分别输出信息 X_B 和 X_E . 图 1 所示的模型中, 编码的主要功能是实现信息的安全传输, 即通过特定的编码使系统逼近或达到保密容量 [3]. 经过信道的接收信号可表示为

$$Y_B = H_B \cdot G \cdot X + N_B, \quad Y_E = H_E \cdot G \cdot X + N_E, \quad (2)$$

其中发送信号 $X = [x_1, x_2, \dots, x_N]^T$ 满足功率约束, $\text{tr}(\mathbf{E}[GXX^+G^+]) \leq P$, $\text{tr}(\cdot)$ 表示矩阵的迹, 符号 “+” 表示共轭转置. 信道状态 H_B, H_E 为 $M \times N$ 维复矩阵, $H_B \neq H_E$, 其第 i 行 j 列个元素 $\text{element}[H_B, (i, j)] = h_{b,(i,j)}$; $\text{element}[H_E, (i, j)] = h_{e,(i,j)}$; 在后文的讨论中假设 Alice 和 Bob 已知信道状态矩阵 H_B , Eve 未知 H_B ; 信道噪声 N_B, N_E 为 $M \times 1$ 维复循环对称高斯噪声向量, 其中元素独立同分布, 并且实部与虚部具有相同的均值和方差.

3 基于随机发送参考的安全传输算法

随机发送参考的物理层安全传输算法的主要思想是发送端对授权用户发送具有随机性的参考导频信号, 用于其接收端的信号解调. 而同时根据无线信道的差异性原理, 窃听方所接收到的导频与真实参考导频存在较大差异, 导致其很难顺利解调信息.

首先将信道分解为多个并行独立信道, 对 H_B 进行奇异值分解可得 $H_B = S_B V_B D_B$, 其中 $V_B = \begin{bmatrix} \mathbf{v}_B \\ \mathbf{0} \end{bmatrix}$, $\mathbf{v}_B = \text{diag}(v_{b,1}, v_{b,2}, \dots, v_{b,K_B}) (\text{diag}(\cdot)$ 表示依照降序排列的对角阵), $K_B = \text{rank}(H_B)$, $\text{rank}(\cdot)$ 表示矩阵的秩, S_B 为 $M \times M$ 维酉矩阵; D_B 为 $N \times N$ 维酉矩阵.

选择 $\mathbf{v}_B$ 中第 K_c 个奇异值对应的信道作为发送随机参考导频的信道, 并且满足 $1 \leq K_c \leq K_B$. 用于发送随机加密的矩阵写为 $G_d = \text{diag}(g_{d,1}, g_{d,2}, \dots, g_{d,K_B})$, 依照奇异值分解的结果在发送端和接收端进行均衡后, Bob 和 Eve 的接收信号可分别写为

$$\tilde{Y}_B = S_B^\dagger H_B D_B^\dagger G_d X + S_B^\dagger N_B = V_B G_d X + \tilde{N}_B, \quad Y_E = H_E \cdot G \cdot X + N_E, \quad (3)$$

其中 $\tilde{y}_B = [\tilde{y}_{b,1}, \tilde{y}_{b,2}, \dots, \tilde{y}_{b,M}]^T$. 由于 Alice 根据 H_B 进行均衡, 所以 Eve 端是否均衡均无法得到独立并行的信道, 其中 $G = D_B^\dagger G_d$. G_d 的元素取值依照下述的随机化导频发送准则.

随机化导频发送准则 在时刻 t , 随机变量 $g_{d,K_c}(t)$ 依照其概率分布取任意值, 而对于 $i \neq K_c$, $g_{d,i}(t) = g_{d,K_c}(t) v_{b,K_c} / v_{b,i}$. 且根据发射功率约束满足 $\text{tr}(\mathbf{E}[GXX^+ G^+]) \leq P$.

发送端对应于导频信道应有 $x_{K_c}(t) = 1$. 在 Bob 端对于 $i \neq K_c$, 其判决后的解调结果为

$$\tilde{x}_i(t) = \min_{x_i(t)} \{ \|\tilde{y}_i(t) - v_{b,i} g_{d,i}(t) x_i(t)\|^2 \}, \quad (4)$$

其中 $\tilde{X}(t) = [\tilde{x}_1(t), \tilde{x}_2(t), \dots, \tilde{x}_{K_B-1}(t)]^T$, 元素 $\tilde{x}_i(t)$ 为除导频外其余并行信道的输出信号. 为求出满足 (4) 式的解, 借助于导频信号可得解调信号

$$\tilde{x}_i(t) = \tilde{y}_{b,i}(t) / y_{b,K_c}(t) = (v_{b,i} g_{d,i}(t) x_i(t) + \tilde{n}_{B,i}(t)) / (v_{b,K_c} g_{d,K_c}(t) + \tilde{n}_{B,K_c}(t)). \quad (5)$$

根据 (5) 式, Bob 可得到 $x_i(t)$ 的估计值 $\tilde{x}_i(t)$, 从而获得信息. 但一般意义下, Bob 是在接收导频信号的条件下来解调获取 $\tilde{x}_i(t)$, 可写为

$$\tilde{x}_i(t) = \min_{x_i(t)} \{ \|\tilde{y}_i(t) - v_{b,i} g_{d,i}(t) x_i(t)\|^2 | \tilde{y}_{K_c}(t) \}. \quad (6)$$

当信道噪声较弱时, 按照随机化导频发送准则和 (6) 式可得 $\tilde{x}_i(t) \approx x_i(t)$. 因为 Eve 的信道状态与 Bob 不同, 不但未知导频信号, 而且无法形成独立的并行信道, 所以 Eve 很难从接收的信号中获取信息, 从而有效地防止了其窃听行为. 对于其安全性, 下一节将做较为深入的讨论.

4 算法安全性分析与仿真

安全性威胁可能出现在通信系统的各个环节, 因此对于图 1 所示的数字安全通信模型, 算法安全性的分析分为两个部分: 1) 分析接收端在符号判决之前的信息安全性; 2) 分析判决模块之后的信息安全性.

4.1 符号判决前信息安全性分析

- 随机发送参考算法安全传输速率计算.

在现有的数字通信系统中, 信源通常服从离散分布 (如: BPSK, 16QAM 等系统), 因此本文重点讨论算法在信源服从离散分布情况下的系统安全传输速率 (单位时间内系统可安全传输的信息量). 根

据 (6) 式, 由于 Bob 可根据导频信号进行信息解调, 而 Eve 无法利用导频信号, 且符号判决模块前和均为连续随机变量, 二者与信源所表示的安全速率具体可写为

$$R_s = \max\{I(X; \tilde{X}|\tilde{y}_{B,K_c}) - I(X; Y_E), 0\}, \quad (7)$$

由互信息的定义可得 (7) 式中的 $I(X; \tilde{X}|\tilde{y}_{B,K_c}) = H(\tilde{X}|\tilde{y}_{B,K_c}) - H(\tilde{X}|\tilde{y}_{B,K_c}, X)$, $I(X; Y_E) = H(Y_E) - H(Y_E|X)$. 所以, 为求得 R_s 需要分析各变量的概率分布情况. 本节具体讨论 G_d 的元素服从零均值复循环对称高斯分布时的安全传输速率.

X 为离散复随机向量, 其中除导频信道对应的元素外, 其 $K_B - 1$ 个元素独立同分布, X 共有 S 种取值 $x_{v,i}$, $i = 1, 2, \dots, S$, 概率分布为 $p(x = x_{v,i}) = p_{x_{v,i}}$. 噪声 $\text{element}(\tilde{N}_B)$ 和 $\text{element}(\tilde{N}_E)$ 的实虚部独立同分布, 且 $\tilde{N}_B \sim N(0, \Sigma_{n_B})$, Σ_{n_B} 为对角阵, 其对角线上元素为 $\sigma_{n_B}^2$; $\tilde{N}_E \sim N(0, \Sigma_{n_E})$, Σ_{n_E} 为对角阵, 其对角线上元素为 $\sigma_{n_E}^2$.

为求得文中算法的安全传输速率, 需要对 $H(\tilde{X}|\tilde{y}_{B,K_c})$, $H(\tilde{X}|\tilde{y}_{B,K_c}, X)$, $H(Y_E)$, $H(Y_E|X)$ 进行讨论. 假设 $\tilde{X}$ 在 $\tilde{y}_{B,K_c}$ 先验时的条件概率密度为 $f_{\tilde{X}|\tilde{y}_{B,K_c}}$, 在 $\tilde{y}_{B,K_c}$, X 先验时的条件概率密度为 $f_{\tilde{X}|\tilde{y}_{B,K_c}, X}$, 则

$$H(\tilde{X}|\tilde{y}_{B,K_c}, X) = - \sum_X p_X \int_{\tilde{X}} \int_{\tilde{y}_{B,K_c}} f_{\tilde{X}|\tilde{y}_{B,K_c}, X} \log f_{\tilde{X}|\tilde{y}_{B,K_c}, X} d\tilde{X} d\tilde{y}_{B,K_c}. \quad (8)$$

Eve 端的接收信号 Y_E 在 X 先验情况下, 根据 (3) 式可知 $Y_E|X \sim N(\mu_{Y_E|X}, \Sigma_{Y_E|X})$, 其中 $\Sigma_{Y_E|X} = H_E \Sigma_{G_X|X} (H_E)^\dagger + \Sigma_{\tilde{N}_E}$, $\mu_{Y_E|X} = 0$. 因此可得 [9]

$$H(Y_E|X) = - \sum_X p_X \int_{Y_E} f_{Y_E|X} \log f_{Y_E|X} dY_E = \sum_X p_X \log[\det(\pi e \Sigma_{Y_E|X}(X))], \quad (9)$$

其中 $\mu_{Y_E|X}$ 和 $\Sigma_{Y_E|X}$ 为 X 的函数. $H(\tilde{X}|\tilde{y}_{B,K_c})$, $H(Y_E)$ 由 (10), (11) 式给出,

$$H(\tilde{X}|\tilde{y}_{B,K_c}) = - [\sum_X p_X f_{\tilde{X}, \tilde{y}_{B,K_c}, X}] \log [\sum_X p_X f_{\tilde{X}, \tilde{y}_{B,K_c}, X}] d\tilde{X} d\tilde{y}_{B,K_c}, \quad (10)$$

$$H(Y_E) = - \int_{Y_E} [\sum_X p_X f_{Y_E|X}] \log [\sum_X p_X f_{Y_E|X}] dY_E, \quad (11)$$

将 (8)~(11) 代入到 (7) 式可得系统在符号判决前的安全传输速率.

• 恒模信源的安全传输速率.

当信源为离散的恒模信号时, 多天线系统的随机发送参考物理层安全传输算法可从根本上防止 Eve 接收信息, 即算法可以有效保证信号的相位信息安全, 具体描述为如下定理 1.

定理 1 当信源为等概分布的恒模离散信号时, 系统的安全传输速率等于 Alice 和 Bob 之间的互信息, 此时 Eve 接收的信息量.

证明 由于信源为等概分布的恒模信号, 因此对于 X 的 S 种取值 $x_{v,i}$, $i = 1, 2, \dots, S$, 令模 $|x_{v,i}| = A_x$ 为恒定值, 相位 $\angle(x_{v,i}) = \phi_{x,i}$. 概率分布为 $p(x = x_{v,i}) = p(x = x_{v,k}) = p_x$, 其中 $i \neq k$.

对于 Bob 端, 根据 (8) 式和 (10) 式可知, 当概率密度满足 $f_{\tilde{X}|\tilde{y}_{B,K_c}, X} \neq f_{\tilde{X}|\tilde{y}_{B,K_c}}$ 时, $I(X; \tilde{X}|\tilde{y}_{B,K_c}) > 0$, Bob 端可以接收到信息; 对于 Eve 端, 当概率密度满足 $f_{Y_E|X} = f_{Y_E}$ 时, $I(X; Y_E) = 0$, Eve 端无法接收到信息. 当前述两条件均满足时, 由 (7) 式可知系统的安全传输速率只与 Bob 接收到的信息有关. 因此只需证明在定理 1 的条件下, $f_{\tilde{X}|\tilde{y}_{B,K_c}, X} \neq f_{\tilde{X}|\tilde{y}_{B,K_c}}$, 且 $f_{Y_E|X} = f_{Y_E}$.

根据 (3) 式, 发送端首先利用对角阵 G_d 对 X 进行线性变换. 令 $Y_d = G_d X$, 其元素 $y_{d,i} = g_{d,i} x_i$, 且幅度为 $|y_{d,i}| = A_{y_{d,i}}$, 相位为 $\angle(y_{d,i}) = \phi_{y_{d,i}}$. 因为 G_d 的元素服从复高斯分布, 所以其幅度 $A_{g_{d,i}}$ 服从 Rayleigh 分布, 其相位 $\phi_{g_{d,i}}$ 服从均匀分布. 又因为 $|x_{v,i}| = A_x$ 为恒定值且其相位等概分布, 所以 $f_{g_{d,i} x_i | x_i} = f_{g_{d,i} A_x | x_i} = f_{g_{d,i} A_x}$. 因此有 $f_{G_d X | X} = f_{G_d A_X}$ 成立, 其中 A_X 表示由 A_x 构成的常数向量. 进一步结合 (3) 式可知, Eve 接收信号的概率分布满足

$$f_{Y_E | X} = f_{H_E G_d X + N_E | X} = f_{H_E G_d A_X + N_E} = f_{Y_E}. \quad (12)$$

在 Bob 端, 对于第 i 个接收元素有

$$f_{\tilde{x}_i | x_i, \tilde{y}_{B, K_c}} = f_{v_{b,i} g_i x_i + \tilde{n}_B | x_i, \tilde{y}_{B, K_c}} = f_{v_{b,i} g_i x_i + \tilde{n}_B, x_i, \tilde{y}_{B, K_c}} / f_{x_i \tilde{y}_{B, K_c}}. \quad (13)$$

当噪声趋于零时, 根据 (13) 式可得 $f_{\tilde{x}_i | x_i, \tilde{y}_{B, K_c}} = f_{x_i \tilde{y}_{B, K_c}} / f_{x_i \tilde{y}_{B, K_c}} = 1 \neq f_{\tilde{x}_i | \tilde{y}_{B, K_c}}$, 因此 $f_{\tilde{X} | \tilde{y}_{B, K_c}, X} \neq f_{\tilde{X} | \tilde{y}_{B, K_c}}$, 由于 (12) 和 (13) 式成立, 根据前述分析, 定理 1 得证.

4.2 符号判决后信息安全性分析及仿真

符号判决模块后 $\hat{X}_B$ 和 $\hat{X}_E$ 均为离散随机变量, 相对于 (9) 式, 此时的安全传输速率为

$$R_s = \max\{I(X; \hat{X}_B | \tilde{y}_{B, K_c}) - I(X; \hat{X}_E), 0\}, \quad (14)$$

其中的互信息 $I(X; \hat{X}_B | \tilde{y}_{B, K_c})$ 和 $I(X; \hat{X}_E)$ 取决于信道转移概率, 所以在离散型信息的传输过程中, 信道转移概率 (误码率) 与安全传输速率通常具有一致性.

定理 2 当信源为相位均匀分布、幅度恒模的离散随机变量时 (如传统的调相系统), 其硬判决后系统的安全传输速率等于信道转移概率信息熵之差, $R_s = H(\hat{x}_e | x) - H(\hat{x}_b | x)$, 并且其取值范围为 $0 \leq R_s \leq \log S$.

证明 根据互信息定义, 具有一般意义地将除导频信道外的第 i 个并行信道的输入信号为 $x_i = x$, Bob 端硬判决输出信号记为 $\hat{x}_i = \hat{x}_b$, Eve 端硬判决输出信号记为 $\hat{x}_i = \hat{x}_e$. 由 (14) 式可知 $R_s = I(x; \hat{x}_b | \tilde{y}_{B, K_c}) - I(x; \hat{x}_e)$, 由于先验条件 $\tilde{y}_{B, K_c}$ 存在于 Bob 的整个解调判决过程, 为便于表达式简洁, 将 $\tilde{y}_{B, K_c}$ 省去可得

$$R_s = I(x; \hat{x}_b) - I(x; \hat{x}_e) = H(\hat{x}_b) - H(\hat{x}_b | x) - H(\hat{x}_e) + H(\hat{x}_e | x), \quad (15)$$

因为 $H(\hat{x}_b) = -\sum_{j=1}^S p(\hat{x}_b = x_{v,j}) \log p(\hat{x}_b = x_{v,j})$, $H(\hat{x}_b | x) = -1/S \sum_{i=1}^S \sum_{j=1}^S p(\hat{x}_b = x_{v,j} / x = x_{v,i}) \log p(\hat{x}_b = x_{v,j} / x = x_{v,i})$.

当信源为相位均匀分布、幅度恒模的离散随机变量时, 文中的算法使得概率 $p(\hat{x}_b = x_{v,j}) = 1/S$, 即所有判决值的概率相同. 所以 $H(\hat{x}_b) = \log S$. 同理有 $H(\hat{x}_e) = \log S$ 因此 $R_s = I(x; \hat{x}_b) - I(x; \hat{x}_e) = H(\hat{x}_e | x) - H(\hat{x}_b | x)$. 再证明 R_s 的取值范围, 若主信道转移概率满足

$$\text{当 } j = i, p(\hat{x}_b = x_{v,j} / x = x_{v,i}) = 1; \text{ 当 } j \neq i, p(\hat{x}_b = x_{v,j} / x = x_{v,i}) = 0, \quad (16)$$

则 $I(x; \hat{x}_b) = H(\hat{x}_b) - H(\hat{x}_b | x) = \log S$, 此时为 $I(x; \hat{x}_b)$ 的最大值. 若信道转移概率满足

$$\text{对于 } \forall i, j, p(\hat{x}_b = x_{v,j} / x = x_{v,i}) = 1/S, \quad (17)$$

图 2 QPSK 调制方式下, 两种算法的接收端星座图

Figure 2 The constellation of received QPSK signal two algorithms. (a) Bob's constellation with random reference algorithm; (b) Eve's constellation with random reference algorithm; (c) Bob's constellation with additive artificial noise algorithm; (d) Eve's constellation with additive artificial noise algorithm

则 $I(x; \hat{x}_b) = H(\hat{x}_b) - H(\hat{x}_b|x) = 0$, 此时为 $I(x; \hat{x}_b)$ 的最小值. 依据定理 1 可知 $I(x; \hat{x}_e) = 0$, 可得 $R_s = I(x; \hat{x}_b)$. 因此有 $0 \leq R_s \leq \log S$, 定理 2 得证.

定理 2 及其证明过程表明接收信道的转移概率信息熵的差等于安全传输速率. 由于转移概率等价于信号的误码率, 因此可以利用误码率之差来刻画系统的安全性 (安全传输速率) [10]. 即当 Bob 端的误码率趋于零, 而 Eve 端误码率趋于均匀化时, 信道的转移概率信息熵最大, 此时可达到最大的系统安全传输速率. 利用误码率之差描述系统的安全性更为便捷.

仿真中设置多天线系统中发送端 Alice 的天线数为 3 根, Bob 和 Eve 的接收天线数均为 2 根. 在 Bob、Eve 均未知信道状态的条件下, 为便于对比分析误码率性能, 令 Alice 端的多根发射天线同时发送相同信息. 其中信道状态矩阵 H_B, H_E 分别为

$$H_B = 10^{-4} \cdot \begin{bmatrix} 4e^{2.15j} & 4e^{-1.71j} & 12e^{1.90j} \\ 2e^{-2.86j} & 4e^{-1.17j} & 4e^{2.42j} \end{bmatrix}, \quad H_E = 10^{-4} \cdot \begin{bmatrix} 10e^{0.51j} & 4e^{-2.13j} & 9e^{1.01j} \\ 6e^{0.41} & 11e^{-2.07j} & 2e^{0.20j} \end{bmatrix}.$$

图 2 所示为调制方式为 QPSK 时, 分别采用随机发送参考算法与现有加性人工噪声算法在接收端的星座图. 令发射总功率为 P , 随机导频信道的发射功率为 P_1 , 加性人工噪声对应的发射功率为 P_2 , 这两部分功率均是为实现安全通信所损耗的功率. 仿真中设置发射总功率 $P = 1.8 \text{ mW}$, $P_1 = P_2 = 0.7 \text{ mW}$, $\sigma_{nE}^2 = \sigma_{nB}^2 = 0.6 \cdot 10^{-4} \text{ mW}$. 从图 2(a) 和 (c) 中可以看出, 在存在相同的功率损耗情况下, 两种算法在 Bob 端的星座图一致, 均具有较好的接收质量, 但相比之下, 图 2(a) 所示的星座点更为发

图 3 两种算法的误码性能对比图

Figure 3 The constellation of received QPSK signal two algorithms. (a) The BER of the random reference algorithm; (b) the BER of the additive artificial noise algorithm

散. 这是由于随机发送参考算法采用 (5) 式进行解调, 其解调效果受信道加性噪声 $\tilde{n}_{B,i}(t)$ 和接收信号空间的残余噪声 $\tilde{n}_{B,K_c}(t)$ 两部分共同影响; 而加性人工噪声只受信道加性噪声影响, 所以在 Bob 端其性能略好于随机发送参考算法. 对比图 2 (b) 和 (d) 可以看出采用随机发送参考算法时, Eve 端的星座图紊乱程度较为均匀, 无法辨识出其星座点, 进一步印证了定理 1 中 Eve 端接收的信息量为零的结论. 而采用加性人工噪声算法时, 其星座点可大致进行辨识. 这是由于该算法是在 Bob 信道状态矩阵的零空间方向引入人工噪声, 而在其主方向传输信号. 由于二者信道状态不正交, 主方向的信号会在 Eve 的信道状态方向上有所体现, 即 Eve 接收的信号等于 Bob 期望接收的信号与加性噪声之和. 所以可初步表明随机发送参考算法的安全性好于加性人工噪声算法.

图 3 为当信道噪声 $\sigma_{n_E}^2 = \sigma_{n_B}^2 = 3.8 \cdot 10^{-4}$ mW, 信息发射功率 $P - P_1 = 0.8$ mW 时, 2 种算法在 BPSK, QPSK, 8PSK, 16QAM 四种调制方式下, 接收端的误码率性能对比图. 图 3(a) 中表明, 对于随机发送参考算法的信号, 在 Bob 端均具有较低的误码率. 当发送端导频功率 (随机化功率) P_1 较低时, Bob 端的抗噪声能力比较弱, 误码率接近 0.1; 与 Bob 相比较, 图中 Eve 的误码率高, 对于具有 S 个星座点的调制方式, 其误码率稳定于 $1/S$. 图 3(b) 是加性人工噪声算法的误码率曲线, 算法同样可以保证 Bob 接收信号具有较低的误码率; 与图 3(a) 相比, 加性人工噪声在 Eve 造成的误码率逐步增高, 只有当随机化功率较大时, 误码率才逼近 $1/S$. 因此随机发送参考算法的安全性比加性人工噪声算法好.

图 4 为两种算法的误码率之差的对比图, 可以发现随着星座点增多, 随机发送参考造成的误码率之差增大, 同时依照定理 2 可知, 其可以安全传输的信息量也变大; 加性人工噪声则只有当发送端的随机化功率增大到一定程度, 其误码率性能之差才可以稳定在较高水平.

图 5 所示的是两种算法的安全传输速率仿真结果, 仿真参数设置与图 3 相同. 可以看出随机发送参考算法的安全传输速率高于加性人工噪声方法. 随机发送参考算法的优势在于即使发射端随机化功率较低, 也可以获得较高的安全传输速率, 尤其对于 16QAM 调制方式, 两种算法的安全传输速率差异更大. 另外, 对比图 3 和图 5 可知, 安全传输速率的所描述的算法性能与误码率所描述的算法性能总体上一致.

5 结论

文中提出随机发送参考算法来保障物理层的信息传输安全. 该算法通过在多天线系统中加入随

图 4 两种算法的误码率之差对比图

Figure 4 The BER difference results of two algorithms. (a) The BER of the random reference algorithm; (b) the BER of the additive artificial noise algorithm

图 5 两种算法的安全传输速率对比图

Figure 5 The transmission rates of two algorithms. (a) The security rate of the random reference algorithm; (b) the security rate of the additive artificial noise algorithm

机化的导频, 使得除 Bob 外的其它窃听者无法正常接收信息, 即将信道的差异性转化为信号质量的差异, 使信道安全传输速率得到增大. 为了分析算法性能, 文中对符号判决前后的安全性进行讨论, 推导出了符号判决前安全传输速率的计算公式, 并通过定理 1 证明随机发送参考方法可有效保证信号相位信息的安全传输. 在符号判决后, 文中分析表明系统的安全性可以通过误码率进行体现. 最终的仿真也表明随机发送参考算法的安全性高于现有的加性人工噪声方法.

参考文献

- 1 Gao Q N, Jiang Z B, Wang J G. The analysis of a novel secure MIMO communication system. In: Proceedings of IEEE 13th International Conference on Communication Technology, Jinan, 2011. 714-718
- 2 Chen W, McNeal M, Hong L. Cross-layered design of security scheme for cooperative MIMO sensor networks. In: Proceedings of IEEE International Conference on Wireless Information Technology and Systems, Honolulu, 2010. 1-4

- 3 Csiszár I, Kóner J. Broadcast channels with confidential messages. *IEEE Trans Inform Theory*, 1978, 24: 339–348
- 4 Islam M R, Tanni F Y, Itha S A, et al. Secrecy capacity analysis in a cooperative MIMO based wireless sensor network. In: *Proceedings of 14th International Conference on Computer and Information Technology*, Dhaka, 2011. 595–600
- 5 Mu P C, Yin Q Y, Wang W J. A physical layer encryption method of using antenna arrays for wireless communication security. *Acad J Xi'an Jiaotong Univ*, 2010, 44: 62–66[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. *西安交通大学学报*, 2010, 44: 62–66]
- 6 Li X H, Hwu J, Ratazzi E P. Array redundancy and diversity for wireless transmissions with low probability of interception. In: *Proceedings of the IEEE International Conference on Acoustics Speech and Signal Processing*, Toulouse, 2006. 4–8
- 7 Zhou X Y, Mckay M R. Secure transmission with artificial noise over fading channels: achievable rate and optimal power allocation. *IEEE Trans Veh Technol*, 2010, 59: 3831–3842
- 8 Goel S, Negi R. Guaranteeing secrecy using artificial noise. *IEEE Trans Wirel Commun*, 2008, 7: 2180–2189
- 9 Telatar E. Capacity of multi-antenna Gaussian channels. *Trans Telecomm*, 1999, 10: 585–595
- 10 Wyner A D. The wire-tap channel. *Bell Syst Tech J*, 1975, 54: 1355–1387

The physical layer security algorithm of MIMO system based on random reference

JI Jiang*, LIU Lu, JIN Liang & HUANG KaiZhi

National Digital Switching System Engineering and Technological Center, Zhengzhou 450002, China

*E-mail: jijinjiang@sohu.com.cn

Abstract To transmit the information in secret with MIMO (multi-input multi-output) system, the security scheme based on the random reference is presented. In this scheme, the independent parallel channels are obtained by doing singular value decomposition. Then, the random pilot is sent to one of these channels, which encrypts the information carried on other parallel channels. Because of the discrepancy from the main channel, with the eavesdropping channel, the eavesdropper cannot decompose the independent random pilot channel to recover the information sent by transmitter. By the theoretical analysis and the simulation about the security after symbol decision module, we get a conclusion that, comparing with the existing artificial noise scheme, the random reference algorithm can be safer.

Keywords wireless communication, MIMO system, physical layer security, pilot, random reference

JI Jiang received the B.S. degree and the M.S. degree in Communication Engineering from the PLA Information Engineering University, China, in 2005 and 2008 respectively. Now he is a Ph.D. student in National Digital Switching System Engineering and Technological Research Center, Zhengzhou, China. His main research interests include mobile communications security, MIMO systems and UWB systems.