

基于信号对齐的动态人工噪声方法

康小磊¹, 季新生¹, 黄开枝¹, 王 婧²

(1. 国家数字交换系统工程技术研究中心, 河南郑州 450002; 2. 数学工程先进计算实验室, 河南郑州 450000)

摘 要: 传统物理层安全人工噪声方法无法带来合法用户可靠性增强. 针对该问题, 提出一种新型动态人工噪声生成方法, 发送方利用噪声发送时权系数剩下的最后一个的自由度, 来改变合法接收方收到的人工噪声的相位, 使得噪声方向与瞬时信号方向对齐, 以提升合法用户瞬时接收信噪比. 首先给出了具体的实现方法, 然后给出理论上相应的性能分析和复杂度分析. 仿真结果表明在对窃听者造成同等干扰水平下该方法能够有效提升合法用户性能.

关键词: 物理层安全; 动态人工噪声; 信号对齐

中图分类号: TN925 **文献标识码:** A **文章编号:** 0372-2112 (2016)11-2767-06

电子学报 URL: <http://www.ejournal.org.cn> **DOI:** 10.3969/j.issn.0372-2112.2016.11.028

A Dynamic Artificial Noise Signal Alignment Based to Enhance Security

KANG Xiao-lei¹, JI Xin-sheng¹, HUANG Kai-zhi¹, WANG Jing²

(1. China National Digital Switching System Engineering & Technological R&D Center, Zhengzhou, Henan 450002, China;

2. Advanced Computing Laboratory of Mathematics Engineering, Zhengzhou, Henan 450000, China)

Abstract: The classical method based on artificial noise for physical layer security cannot enhance the reliability of the legitimate user. Aiming at this problem, this paper proposes a dynamic method to generate artificial noise and glean benefit from the artificial noise for the legitimate user. The main idea is that the sender pre-generates artificial noise, then analyzing the interference of the noise to the legitimate user, the sender change the phase of received artificial noise of the legal user to align the noise and the desired signal. Analytical and simulation results show that the method proposed significantly improves the performance of legal users when the eavesdropper reached the same level of interference in both methods.

Key words: physical layer security; dynamic artificial noise; signal alignment

1 引言

无线通信因其天然的接入方式使得生活变得愈加方便快捷,但也正是由于这种开放的接入方式,造成通信的安全性受到严峻的挑战.发送方与接收方的通信极易容易遭到窃听.针对防窃听的物理层安全技术近几十年得到了空前的发展.

物理层安全研究最开始的出发点就是通过充分利用无线信道的特性达到安全传输的目的,其中 Wyner^[1]开创了该领域的先河,提出了搭线窃听模型,并从信息论角度证明当窃听者信道是合法信道的退化版本时可以实现非零的安全通信速率.这也为后来的研究建立了主基调:即必须想方设法增强主信道可靠性而同时

恶化干扰窃听信道.现有的研究从多个角度和维度对无线系统的防窃听能力进行了研究,其实质都是利用发送或接收方的冗余资源,以提升合法用户接收性能和恶化窃听用户窃听性能提升保密容量.

现有的物理层安全技术中最简单朴素并且效果显著的方法为人工噪声方法^[2],人工噪声方法的提出,激起了广大研究者们极大的热情,被应用于各种不同的场景,包括 MISO^[3-5]、MIMO^[6]、中继^[7,8]、传感网络^[9]以及认知无线网络^[10]等等,研究了不同资源域上的生成方式^[11].由此还演化出人工干扰、协作干扰种种说法不同但本质思想相同的概念.

人工噪声方法方式的思想就是要利用冗余度来恶化窃听信道,在不影响合法用户接收的同时,造成窃听

收稿日期:2015-04-20;修回日期:2015-09-25;责任编辑:蓝红杰

基金项目:国家自然科学基金(No. 61379006, No. 61401510, No. 61501516, No. 61471396, No. 61521003);国家 863 高技术研究发展计划(No. 2015AA01A708)

信道质量更差,以此拉大合法用户与窃听用户的信道差异,提升保密性能.传统人工噪声方法的最大贡献在于恶化窃听者,当合法用户的信道环境本身就很差时,保密性能的提升受限于合法用户信道,即人工噪声无法增强合法用户可靠性.

其实从信号本身来看,干扰并不一定对信号起有害作用,这种有害只能算是统计平均意义上的有害.针对瞬时信号,从电磁波角度出发,如果某一瞬时干扰恰好与信号具有相同的波峰波谷(类似于共振)时,它反而能够增强期望信号强度.那么当发送方或者接收方已知这种瞬时干扰,就可能对其进行控制并加以利用.这种思想已经被 Christos Masouros 等人^[12]在 MIMO 多用户预编码中有所研究.

借助上述思想,我们在设计人工噪声时不用考虑必须让人工噪声位于合法用户零空间的约束,而是首先随机满维度生成人工噪声,在此基础上发送方通过信道状态、已生成的人工噪声以及此时要发送的符号,预测用户在瞬时接收符号上受到的人工噪声,并通过最后一个维度的相位变化来对齐人工噪声和瞬时信号,以达到对瞬时接收信噪比的提升.仿真结果表明,在对窃听者造成同等干扰水平情况下该方法能够使合法用户获得 1.75 dB 的性能提升.

命名规则及符号说明如下: Alice 代表发送方, Bob 代表合法用户,窃听者用 Eve 表示, $(\cdot)^{-1}$, $(\cdot)^T$ 以及 $(\cdot)^H$ 分别代表矩阵求逆、转置以及共轭转置, $[\cdot]^+$ 代表 $\max\{\cdot, 0\}$, $h, \mathbf{h}, \mathbf{H}$ 分别代表变量、向量和矩阵, \mathbf{I}_M 表示对角元素全为 1 的 $M \times M$ 矩阵.

2 系统模型及问题描述

考虑如图 1 所示的 MISOSE 窃听模型,发送方多天线 N_t ,合法用户与窃听方均为单天线的窄带系统.发送方 Alice 到合法用户 Bob 的信道为 $\mathbf{h}_{AB} = \{h_{11}, h_{11}, \dots, h_{n1}\}$,其中 h_{ni} 表示从 Alice 第 n 根天线到 Bob 的信道参数,服从均值为 0,方差为 1 循环复高斯分布,并且各天线间的信道参数相互独立.发送方可以通过反向训练序列获取合法用户信道状态信息,但是假

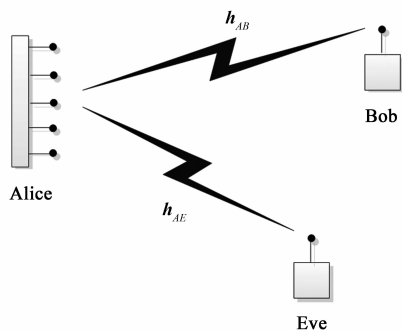


图 1 系统模型

设窃听者是未认证的系统用户,只存在被动窃听的行为,因此其信道状态信息 \mathbf{h}_{AE} 对于 Alice 是未知*.

经典人工噪声方法即设计如下的发送信号:

$$\mathbf{x} = \mathbf{u}s + \mathbf{Wz} \quad (1)$$

即信号由两部分组成:期望信号 $\mathbf{u}s$ 与人工噪声 \mathbf{Wz} , \mathbf{u} 为期望信号预编码向量, s 为期望传输的有用信号, \mathbf{W} 为人工噪声预编码矩阵, \mathbf{z} 为人工噪声向量. 其中 $E\{|s|^2\} = p_s = (1 - \vartheta)P_0$ 为期望信号功率, ϑ 为功率分配因子;人工噪声信号功率为 $E\{|\mathbf{z}|^2\} = p_z = \vartheta P_0$. 假设发送方到合法用户的信道状态为 \mathbf{H} ,那么 \mathbf{W} 必须满足 $\mathbf{H}\mathbf{W} = \mathbf{0}$,即人工噪声位于合法用户零空间,这样就可以保证人工噪声不会干扰合法用户,而用户的预编码最优值即让每一根天线发送值在合法用户处同相叠加: $\mathbf{H}_{AB}\mathbf{u} = \|\mathbf{H}_{AB}\|$.

经过上述处理,我们可以得出合法用户与窃听者的接收信噪比分别为:

$$\gamma_B = \frac{\|\mathbf{H}_{AB}\|^2 (1 - \vartheta) p}{\sigma^2} \quad (2)$$

$$\gamma_E = \frac{\|\mathbf{H}_{AE}\mathbf{u}\|^2 (1 - \vartheta) p}{\|\mathbf{H}_{AE}\mathbf{W}\|^2 \vartheta p + \sigma^2} \quad (3)$$

从上式可以看出,当功率分配因子一定,那么人工噪声对合法用户的信噪比不带来任何增益,只是对窃听用户起到抑制作用.当合法用户信道质量较差,即 $\|\mathbf{H}_{AB}\|$ 较小时,合法用户接收信噪比较差,那么两个用户之间的差异就无法通过人工噪声来拉大.

3 基于信号对齐的动态人工噪声生成方法

3.1 动态人工噪声生成方法基本原理

文献[12]在研究多用户 MIMO 预编码的过程中,发现了当多用户调制方式为 BPSK 或 QPSK 时,如果发送方已知多用户信号对其他用户的干扰时,可以分析这些干扰瞬时对期望用户的影响,具体我们可以从图 2 说明:

假设用户信号 QPSK 调制,信道无噪并且信道估计准确,则用户接收星座如图 2 所示,在某个符号接收的瞬时,假设该用户受到其他用户期望信号的干扰,如果此瞬时的干扰与期望信号同相位,并且幅度方向一致(同正同负),那么该瞬时的干扰能够增强 QPSK 解调的软判决,对信号起到了增强的作用,归为有益干扰,用户接收到的星座就偏差在图 2 的阴影部分而不是星座点的坐标上;如果期望信号与干扰信号不满足上述约束,那么星座点坐标则落在了阴影之外,增加了解调判决的难度,归为有害干扰.

* 为了专注于方法本身,与传统人工噪声机制一样,我们假设不存在码间干扰.更加实际的情况将会作为未来的工作进一步展开研究.

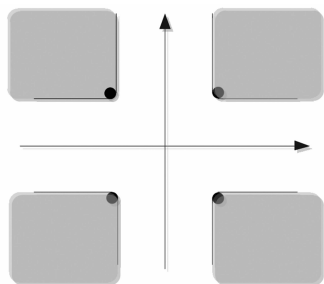


图2 有益干扰和有害干扰示意图

文献[12]正是基于该思想提出了两种动态的线性预编码技术,即动态的信道翻转(SCI)和动态的规整化信道翻转(SRCI),通过这两种手段将部分有害干扰消除而有益干扰保留,以提升每一用户的信噪比。

3.2 动态人工噪声生成方法

借鉴于上述多用户 MIMO 动态线性预编码的思想,我们可以看到,在传统的人工噪声生成上,由于人工噪声由发送方生成,同时发送方也已知合法信道,所以可以预测出其产生的人工噪声到合法用户处形成什么样的影响^{*}。所以我们同样可以对其加以区分,利用最后一个自由度将人工噪声与瞬时信号对齐,以达到增强信号的目的。

基于上述分析,我们设计发送方的信号为

$$\mathbf{x} = \mathbf{w}_s s + \alpha \mathbf{z} \quad (4)$$

其中 α 为归一化因子: $\alpha = 1 / \sqrt{\text{trace}(\|\mathbf{z}\|^2)}$ 。为了简化分析,我们假设期望信号采用 BPSK 调制,信号的判决只依赖调制符号的实部。期望信号最优的预编码设计保留跟传统方式一样,即波束成形或称为点聚焦:

$$\mathbf{w}_s = \frac{\mathbf{h}_{AB}^*}{\|\mathbf{h}_{AB}\|} \quad (5)$$

在每一发送符号内,由于人工噪声的生成是已知的,那么设计如下的干扰分析式:

$$\mathbf{h}_{AB} \mathbf{z}_{(t)} \triangleq s(t) \quad (6)$$

其中 $\mathbf{z}_{(t)}$ 表示 t 时刻生成的人工噪声, \triangleq 表示两端取相同正负符号, $s(t)$ 表示当前 t 时刻发送的有用符号。由于每一发送符号 s 是已知的,因此我们首先随机生成 $N_t - 1$ 维复高斯随机向量 $\mathbf{z}_{(t)}(i), i = 1, 2, \dots, N_t - 1$, 最后一个自由度 z_{N_t} 通过公式(6)确定。值得注意的是,满足上式的 z_{N_t} 具有无穷多解,只需要在无穷多解中随机选取即可,此外还可以看出,该方法生成的人工噪声与信道和发送信号相关,如果信道慢衰落或者比较稳定,那么窃听者有可能会从接收信号中破解信道 \mathbf{h}_{AB} , 那么该方案将会失效。

同理,当用户信号为 QPSK 调制时,干扰分析矩阵则为如下实部与虚部的分开形式:

$$\begin{aligned} \text{real}(\mathbf{h}_{AB} \mathbf{z}_{(t)}) &\triangleq \text{real}(s(t)) \\ \text{imag}(\mathbf{h}_{AB} \mathbf{z}_{(t)}) &\triangleq \text{imag}(s(t)) \end{aligned} \quad (7)$$

其中 $\text{real}(\cdot)$ 与 $\text{imag}(\cdot)$ 分别表示取实部和虚部运算。综上,结合本文提出的基于信号对齐的人工噪声生成方法, BPSK 或 QPSK 调制系统的物理层安全算法设计如下:

(1) 在发送信号之前合法用户发送反向导频, Alice 估计并获取信道状态信息;

(2) 当发送第 t 时刻的符号时按照公式(5)设计期望信号;

(3) 发送方随机生成 $N_t - 1$ 维人工噪声向量 $\mathbf{z}_{(t)}(i), i = 1, 2, \dots, N_t - 1$;

(4) 按照公式(6)(BPSK)或(7)(QPSK)生成干扰分析公式, 求出 $\mathbf{z}_{(t)}(N_t - 1)$, 并确定归一化因子 α ;

(5) 按照公式(4)设计合成第 t 时刻发送向量。

上述动态人工噪声实现框图如图3所示。由于本文方法中是通过合法用户发送反向导频, 因此可以合理地假设窃听者 Eve 无法获取合法信道 \mathbf{h}_{AB} 。通过上述算法设计, 合法用户接收端收到的信号为:

$$y_B = \mathbf{h}_{AB} \mathbf{x} + n_B \quad (8)$$

那么有:

$$y_B = \|\mathbf{h}_{AB}\| s + \alpha \mathbf{h}_{AB} \mathbf{z} + n_B = \|\mathbf{h}_{AB}\| s + \beta s + n_B \quad (9)$$

其中 $\beta = \alpha \|\text{real}(\mathbf{h}_{AB} \mathbf{z})\|$, 每一符号动态变化。而窃听者收到的信号为:

$$y_E = \mathbf{h}_{AE} \mathbf{w}_s s + \alpha \mathbf{h}_{AE} \mathbf{z} + n_E \quad (10)$$

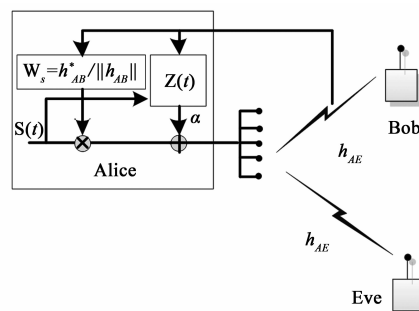


图3 动态人工噪声设计框图

4 性能分析

4.1 合法用户性能增益分析

对比于文献[1]公式(4)可见, 我们的新方法能够使得人工噪声对合法用户每一符号产生增益 βs 。而窃听者同样受到人工噪声干扰。下面我们定量分析这种新型人工噪声所能带来的增益究竟有多少。

由于本文方法是基于 PSK 调制, 不属于高斯信号, 因此无法从保密容量的理论上刻画本方法的安全性, 但是我们可以通过接收信噪比或者误码率来衡量两者之间的差异。由于每一符号的人工噪声编码矩阵都在

* 虽然这里的人工噪声没有调制过程, 但是也正是由于这种人工噪声的随机性, 能够满足任何调制方式而不仅仅局限于 PSK 调制。

改变,而且处理是瞬时的,因此每一符号的接收信噪比都可能不同,瞬时的接收信噪比可以从公式(9)中获得:

$$\gamma_B(i) = \frac{|s(i)|^2(H_{AB}(i)^2 + \alpha(i)^2\beta^2)}{\sigma(i)^2} \quad (11)$$

不过更有实际意义的是平均意义上的接收信噪比,所以我们对每一符号上的接收信噪比做平均,本文方法下的平均接收信噪比为:

$$\begin{aligned} \bar{\gamma}_B &= \frac{\frac{1}{N} \sum_{i=1}^N (|s(i)|^2 (\|H_{AB}(i)\|^2 + \alpha(i)^2 \|\beta\|^2))}{\frac{1}{N} \sum_{i=1}^N \sigma(i)^2} \\ &= \frac{E\{s\} \{E\{\|H_{AB}\|^2\} + E\{\alpha^2\} E\{\beta^2\}\}}{\sigma^2} \end{aligned} \quad (12)$$

本文假设信道服从期望为0,方差为1的循环对称复高斯分布,所以: $E\{\|H_{AB}\|^2\} = E\{\text{sum}(\text{var}(h)^2)\} = N_t$; 期望信号是归一化的 BPSK 信号,因此有 $E\{s\} = 1$. 对于 $E\{\|z\|^2\}$, 从上文可知, z 是与期望信号对齐的人工噪声向量, 所以有 $E\{\|z\|^2\} = N_t E\{\|z\|^2\} = N_t$, 进而可以得出功率归一化因子: $E\{\alpha^2\} = (1/\sqrt{N_t})^2 = 1/N_t$; 噪声 z 的设计满足均值为零, 方差为1的循环复高斯变量, 由于 BPSK 只与实部有关, 因此有用噪声部分的功率也只能利用 50%. 所以 $E\{\|\text{real}(z)\|^2\} = N_t/2$. 综上, 我们可以获得平均每接收符号的信噪比为:

$$\bar{\gamma}_B = \frac{N_t + \frac{1}{2}N_t}{\sigma^2} = \frac{3N_t}{2\sigma^2} \quad (13)$$

传统方法当人工噪声置于合法用户零空间时, 平均接收信噪比为: $\gamma_B = \frac{N_t}{\sigma^2}$, 那么理论上本文方法能够使合法用户获得 $\bar{\gamma}_B/\gamma_B = 3/2 \approx 1.76$ (dB) 的性能提升, 同理我们也可分析得出当 QPSK 调制时能获得的提升为 $\bar{\gamma}_B/\gamma_B = 5/4 \approx 0.96$ (dB).

4.2 复杂度分析

为了研究本方法的复杂度, 表1给出了我们方法与传统零空间人工噪声方法的复杂度对比. 其中 N_f 表示帧大小, 即假设在 N_f 个符号持续时间内, 信道估计次数为 N , N 大小表征信道变化快慢. 我们通过一帧内所消耗的运算数的量级来比较本文方法与零空间人工噪声方法的复杂度. 从表中可以看出, 本文方法由于不需要进行大量矩阵分解, 所以会减少很大一部分关于信道变换的运算量, 除此之外, 零空间的方案需要每符号都要进行正交基与随机产生的人工噪声向量进行矩阵的乘积运算, 而本方案只需要简单的解方程过程即可, 综上, 本文方法在复杂度量级上远低于经典方案.

表1 方案复杂度对比

零空间人工噪声	运算量	动态人工噪声	运算量
信道 SVD 分解求解零空间正交基	$N * O(N_t^3)$	信道 SVD 分解求解零空间正交基	0
构造零空间噪声	$N_f * O[N_t(N_t - 1)]$	构造动态噪声	$N_f * O(2N_t)$
计算尺度因子	0	计算尺度因子	$N_f * O(N_t)$
合计	$N * O(N_t^3) + N_f * O(N_t^2)$	合计	$N_f * O(3N_t)$

5 数值结果及分析

仿真条件如下: 发送总功率为2, 期望信号与噪声信号功率配比为1:1, 设定信噪比为[0 5 10 15 20] dB (对应噪声功率为[1 0.3162 0.1 0.0316 0.01]), 随机生成10000个符号, 假设信道每100个符号变一次(块长度为100), 并且信道服从循环复高斯分布, 均值为0, 方差为1, 随机生成; 窃听者信道未知, 所以窃听信道也随机生成, 重复试验1000次统计平均.

首先我们从星座图上观察, 零空间人工噪声与动态人工噪声下的合法用户(左)与窃听者(右)的接收信号星座分别如图4、5所示. 显而易见地, 相对于零空间人工噪声, 本文方法下合法用户的星座点判决距离变大, 而对于窃听者, 两者效果持平.

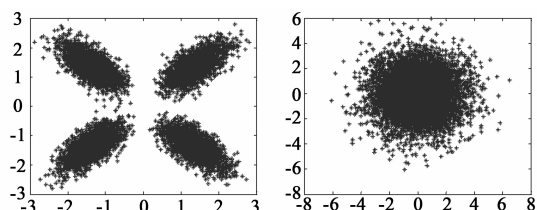


图4 零空间人工噪声下Bob和Eve星座(QPSK)

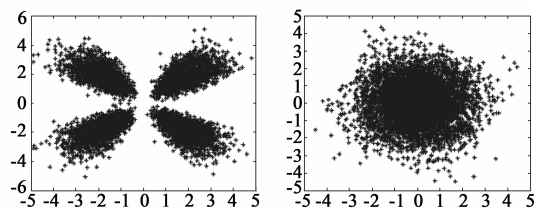


图5 动态人工噪声下Bob与Eve星座(QPSK)

BPSK 系统的误符号率(SER)性能仿真如图6所示, 从图中可以看出, 传统人工噪声方法和本文的动态人工噪声方法下, 窃听者的性能几乎持平, 都几乎达到了无法正确解调, 但是, 本文方法下合法用户的SER性能显著地优于传统方法. 可以看出在相同SER下本文方法平均比传统方法高1.75左右dB, 与我们在4.2节中理论分析的结果一致.

系统吞吐量随输出信噪比关系如图7所示, 本文方法下吞吐量性能有所提升, 从侧面反映了接收可靠性

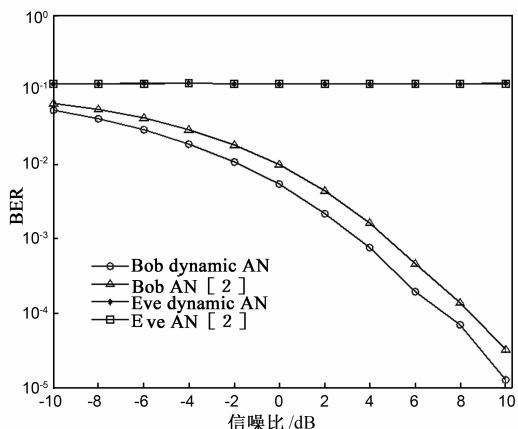


图6 SER性能

得到了增强,此外还可以看出,BPSK 提升的增益大于 QPSK. 从理论上讲,随着调制阶数的增加,本文方法所能获得的增益是逐渐变小的,这与本文的干扰分析矩阵和判决准则设计有关系,本文并没有去寻求最优的方案,只是提出一种朴素的思想,因此对于高阶调制来讲,性能提升将受到限制,这也是后续工作的深入方向之一;图 8 给出了接收信噪比与发送方天线数的定量关系:随着天线数的增多,信噪比稳步提升,当天线数较小时,仿真值与理论值吻合;当天线数持续增大,仿真值低于理论值,但是逼近理论限.

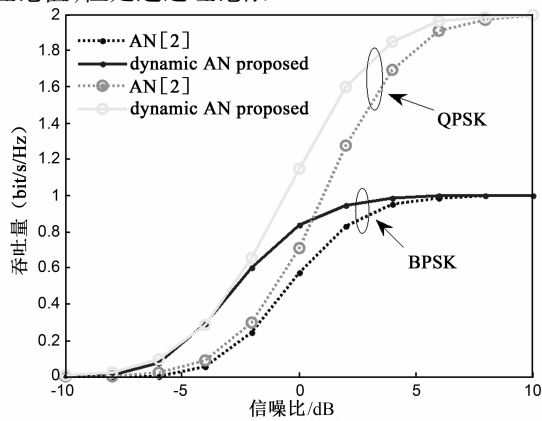


图7 吞吐量变化

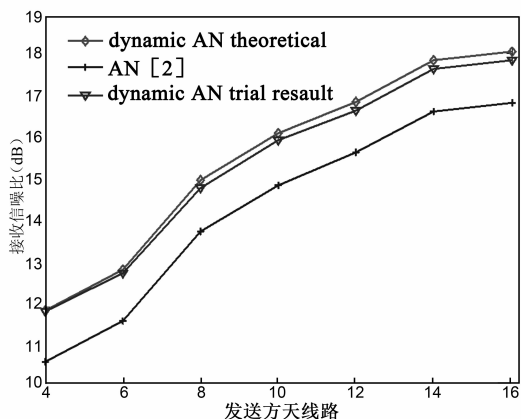


图 8 接收信噪比随天线数变化

6 结束语

本文针对物理层安全中传统人工噪声方法无法提升合法用户可靠性问题,提出了一种基于信号对齐的人工噪声生成方法,在设计人工噪声时不用考虑必须让人工噪声位于合法用户零空间的约束,而是首先随机满维度生成人工噪声,在此基础上发送方通过信道状态、已生成的人工噪声以及此时要发送的符号,预测用户在瞬时接收符号上受到的人工噪声,并通过最后一个维度的相位变化来对齐人工噪声和瞬时信号,以达到对瞬时接收信噪比的提升.同时给出了基于本文人工噪声生成方法下的物理层安全算法,此外还给出理论上的性能分析,仿真结果进一步证实了该方法的有效性.不过受限于信道,该方案在信道慢变时将受到严峻挑战.将该方法推广到 MIMOME 系统以及探究存在信道估计错误时的方案性能可靠性可作为进一步研究工作.

参考文献

- [1] Wyner A D. The wire-tap channel[J]. Bell Syst Tech J, 1975,54(8):1355-1387.
- [2] Goel S, Negi R. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008,7(6):2180-2189.
- [3] Li J, Petropulu A P. On ergodic secrecy rate for gaussian mISO wiretap channels[J]. IEEE Transactions on Wireless Communications, 2011,10(4):1176-1187.
- [4] Xiong Q, Gong Y, Liang Y, et al. Achieving secrecy of MI-SO fading wiretap channels via jamming and precoding with imperfect channel state information[J]. IEEE Wireless Communications Letters, 2014,3(4):357-360.
- [5] Khisti A, Wornell, Gregory W. Secure transmission with multiple antennas—part i: the misome wiretap channel[J]. IEEE Transactions on Information Theory, 2010,56(7):3088-3104.
- [6] 罗文宇,金梁,黄开枝,等. γ 约束均方误差下的无线信道加密方法[J]. 电子学报,2012,40(7):1289-1297. Luo Wenyu, Jin Liang, Huang Kaizhi, et al. A wireless channel encryption method with γ mean square error[J]. Acta Electronica Sinica, 2012, 40 (7): 1289 - 1297. (in Chinese)
- [7] Dong L, Han Z, Petropulu A P, et al. Improving wireless physical layer security via cooperating relays [J]. IEEE Transactions on Signal Processing, 2010, 58 (3): 1875 - 1888.
- [8] 吴亚峰,赵睿,贺玉成,等. 基于有限反馈的非可信中继系统的物理层安全性能分析[J]. 电子学报,2015,43(11):2247-2254.

- Wu Yafeng, Zhao Rui, He Yucheng, et al. Performance analysis of physical layer security of untrusted relay system based on limited feedback [J]. Acta Electronica Sinica, 2015, 43(11): 2247 – 2254. (in Chinese)
- [9] Ding Z, Ma Z, Fan P. Asymptotic Studies for the Impact of Antenna Selection on Secure Two-Way Relaying Communications with Artificial Noise [J]. IEEE Transactions on Wireless Communications, 2014, 13(4): 2189 – 2204.
- [10] He Y, Evans J, Subhrakanti D. Secrecy rate maximization for cooperative overlay cognitive radio networks with artificial noise [A]. 2014 IEEE International Conference on Communications (ICC) [C]. Sydney, NSW: IEEE, 2014. 1663 – 1669.
- [11] Tomoki A, Shunta A, Takahiko S. Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems [A]. 2014 International Conference on Communications (ICC) [C]. Sydney, NSW: IEEE, 2014. 807 – 813.
- [12] Christos M, Emad A. Dynamic linear precoding for the exploitation of known interference in MIMO broadcast systems [J]. IEEE Transactions on Wireless Communications, 2009, 8(3): 1396 – 1405.

作者简介



康小磊 男, 1986 年生于陕西咸阳. 国家数字交换系统工程技术研究中心博士生. 研究方向为无线物理层安全、D2D 通信.
E-mail: yiranniao001@163.com.cn



季新生 (通信作者) 男, 1968 年生于江苏如东. 国家数字交换系统工程技术研究中心教授, 博士生导师. 研究方向为未来无线通信新技术.
E-mail: jxs@mail.ndsc.com.cn

黄开枝 女, 1974 年生于安徽滁州, 国家数字交换系统工程技术研究中心教授, 博士生导师. 研究方向为无线安全组网技术.

王婧 女, 1985 年生于河南郑州, 数学工程先进计算实验室讲师. 研究方向为网络安全、计算机技术与应用.