doi:10.3969/j.issn.1000-436x.2013.07.005

基于最小信息泄漏的线性随机化实现物理层安全传输

李桥龙，金梁
（解放军信息工程大学 信息技术研究所，河南 郑州 450002）

摘 要：为设计实用物理层安全传输机制，给出了线性随机化预处理模型。该模型指出，基于无线信道的特征差异，恰当地设计加性和乘性随机化模块可以为合法用户提供信道优势。从信息理论安全角度论证了加性随机化权值和乘性随机化权值具有最小信息泄漏时应满足的最佳分布。最后提出一种随机子载波参考安全传输机制对乘性随机化权值的优化设计进行了实例化分析。
关键词：物理层安全；线性随机化；信息理论安全；随机子载波参考
中图分类号：TN929.5 文献标识码：A 文章编号：1000-436X(2013)07-0042-07

Linear randomization with lowest information leakage for physical layer secure transmission

LI Qiao-long, JIN Liang
(Institute of Information Technology, PLA Information Engineering University, Zhengzhou 450002 China)

Abstract: Linear randomization pre-processing framework was presented to design feasible ysical layer secure transmission schemes. The framework show that, based on characteristic differentiae of wireless channels, additive and multiplicative randomization modules with suitable design would create channel advantage for legitimate users. In the view point of information theory security, the optimal distributions of the additive randomization weights and the multiplicative randomization weights to induce the lowest information leakage to the eavesdropper were verified. Finally, A random sub-carrier referencing security scheme was proposed as an instantiation analysis for the optimization design of multiplicative randomization weights.
Key words: physical layer security; linear randomization; information theory security; random sub-carrier referencing

1 引言

随着无线通信技术的广泛应用，通信的安全性也愈加受到人们的重视。由于无线传输的开放性和网络拓扑的动态变化，传统加密安全面临着密钥分发与管理的问题。物理层安全技术[1]立足于无线安全问题的诱因，期望从开放的传播环境入手实现安全传输。通过充分利用无线信道的个性化特征区分用户，可以有效抑制窃听者的截获行为，为无线安全带来了全新的解决思路。

作为物理层安全的理论基础，信息理论安全[2]为不同信道模型下的安全传输提供了理论界限。最初的工作由 Wyner 提出 wire-tap 信道模型[3]，并以向合法用户安全传输的最大信息量定义安全容量，用以定量评价系统的安全性能。为保证系统具有可用的安全容量，wire-tap 模型要求合法用户的信道优于窃听者信道，也即窃听信道是合法信道的退化版本。随后安全容量的分析与优化被扩展到了一般的非退化模型[4]、衰落信道[2]以及多天线信道[5]，分析发现信道的衰落特性以及多天线具有的自由度均可以为系统安全提供契机。但是以上安全容量的计算需要预知窃听者的信道信息，这在实际场景中往往无法满足。为设计实用的安全传输机制，基于无线信道差异，可以借助信号处理的方式逐渐为合

收稿日期：2012-03-18；修回日期：2013-01-15
基金项目：国家自然科学基金资助项目（61171108）；国家高技术研究发展计划（“863”计划）基金资助项目（2011AA010604）
Foundation Items: The National Natural Science Foundation of China (61171108)；The National High Technology Research and Development Program of China (863 Program) (2011AA010604)

法用户提供信道优势。

针对多天线系统，S. GOEL 提出在合法信道零空间发送人工噪声以干扰窃听者的接收[6]。零空间发送噪声避免了对合法用户造成影响，从而为其创造了相对的信道优势。未知窃听者信道时，人工噪声仍然可以在零空间全向发送[7]。但是当窃听者的天线数量逐渐增多时，受人工噪声的影响也逐渐减少。相反，X. LI 在文献[8]中通过结合反向同步和阵列随机加权的方式产生干扰，在恶化窃听者信道的同时抑制其可能采取的盲检测能力。实质上该方法同样是在合法用户的零空间施加了乘性噪声。通过随机天线选择[9]代替随机加权可以进一步提高功率利用率，但随机空间受限于天线数量。同样，对于分布式 OFDM 异步协作系统，Z. LI 提出了子载波差分编码的安全机制[10]。在合法用户的导频子载波和数据子载波之间建立随机化权值的参考关系，窃听者由于信道差异无法建立相应的参考关系。但在未能约束窃听者译码方法时，该方法扩展到一般协作场景将面临窃听风险。不同的信道模型下，类似的随机加权方法还有文献[11]和文献[12]。可见，基于无线信道的特征差异，利用随机化处理可以在保证合法用户正常接收的同时抑制窃听者的接收。然而，目前无论是加性人工噪声还是乘性随机加权的安全机制，均缺乏对随机化权值选取的特征刻画。

事实上，随机化预处理可以与窃听者的物理信道形成等效信道。当窃听者无法预知预处理细节时，预处理相当于加性或乘性的信道衰落，导致窃听者接收信号产生信息损失。安全机制设计期望窃听者接收信号信息损失最大化，也即预处理之后泄漏出去的信息最小化，而与信息损失与随机化权值的特性相关。本文从信息安全角度重点刻画具有最小信息泄漏的线性随机化预处理权值特性。对于加性随机化，易于得出具有复高斯分布的加性噪声可以导致信息损失最大化。对于乘性随机化，研究发现在完全未知乘性权值时，经过对数运算乘性随机化可以转化为加性随机化。因此当乘性随机化权值的幅度服从对数高斯分布，而相位服从均匀分布并与幅度保持独立时可以产生最小信息泄漏。为实例化分析乘性随机化权值的优化设计，文中基于文献[10]提出一种随机子载波参考的安全传输机制。下文首先针对信息泄漏给出线性随机化预处理安全模型，接着论证加性和乘性预处理权值的分布特性，最后进行了实例化分析和仿真验证。

2　线性随机化预处理安全传输模型

线性随机化预处理实现安全传输的模型如图 1 所示，由发送方 Alice、合法用户 Bob 以及窃听方 Eve 组成。根据信息理论安全，为了确保或提高系统可用的安全速率，需要为 Bob 创造信道优势并逐渐加大与 Eve 的信道区分[13]。在未知 Eve 信道信息的情况下，只有在发送端对发送信号进行预处理，改变信号所经历的等效信道条件。当 Bob 的等效信道优于 Eve 时，可以为系统提供可用的安全速率。当对发送信号执行线性预处理时，预处理模块可以等效成一个线性系统，包括对信号的加性和乘性操作。人工噪声[6]和随机加权方法[8,10]则分别采用了加性和乘性随机化实现安全传输。当以 $\boldsymbol{w}$ 和 $\boldsymbol{v}$ 分别表示乘性和加性预处理权值矢量时，x 经过预处理之后表示为

$$\boldsymbol{z} = \boldsymbol{w}x + \boldsymbol{v} \tag{1}$$

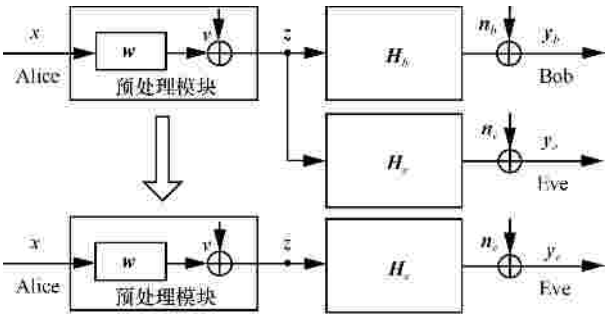

图 1　线性随机化预处理安全传输模型

以 $\boldsymbol{H}_b$ 和 $\boldsymbol{H}_e$ 分别表示 Alice 到 Bob 和到 Eve 的信道矩阵，$\boldsymbol{n}_b$ 与 $\boldsymbol{n}_e$ 分别表示 Bob 和 Eve 信道的高斯噪声。Bob 和 Eve 的接收信号分别为

$$\begin{aligned} \boldsymbol{y}_b &= \boldsymbol{H}_b\boldsymbol{z} + \boldsymbol{n}_b \\ \boldsymbol{y}_e &= \boldsymbol{H}_e\boldsymbol{z} + \boldsymbol{n}_e \end{aligned} \tag{2}$$

预处理模块的设计需要在保证 Bob 正常通信或影响较小的前提下，最大程度地降低 Eve 可获取的信息。随机加权方法还结合了数字相干接收的特点，随机预处理致使 Eve 接收信号随机快变，从而在降低 Eve 等效信道速率的同时增加其接收难度。然而，尽管 Eve 的接收受到抑制，仍然无法确定 Eve 可能获取的信息量。因此，预处理模块的设计原则是基于信道特征差异加大两者的信道区分度。通常 Eve 无法预知预处理模块设计的随机化权值。如图 1 所示，把预处理模块看成线性信道，Eve 的等效信道可以建模成级联信道形式。当 $x \to \boldsymbol{z} \to \boldsymbol{y}_e$ 形成

Markov 链时，根据数据处理定理[14]有如下不等式成立

$$I(\boldsymbol{z};x) \geq I(\boldsymbol{y}_e;x) \tag{3}$$

也即 Eve 获取关于发送信号的信息不会大于预处理之后信息。于是在未知 Eve 信道信息情况下，预处理模块的优化目标是促使发送信号的信息损失最大化，也即信息泄漏最小化。另一方面，随机化预处理需要对 Bob 保持透明，以降低对 Bob 接收的影响。

3 具有最小信息泄露的随机化预处理

依据随机化预处理安全传输模型，随机化权值的优化目标是预处理之后的信号具有最小信息泄漏。下面分别论证具有最小信息泄漏的加性和乘性随机化预处理权值的特性。

随机化预处理为了实现在抑制 Eve 接收的同时对 Bob 保持透明，安全传输系统需要具有信道资源的冗余度。因此，x 与 z 之间通常形成多维信道（具体表现为多天线、多个正交子载波所产生的多维子信道）。在此考虑多维并行独立的子信道的预处理设计，此时可以简化成一维信道。

3.1 加性随机化预处理

当单独考虑加性随机化预处理时，式(1)可以重新写成

$$z = x + v \tag{4}$$

当 x 与 v 保持相互独立时，x 与 z 之间的互信息可以表示为

$$\begin{aligned} I(z;x) &= h(z) - h(z \mid x) \\ &= h(z) - h(x+v \mid x) \\ &= h(z) - h(v) \end{aligned} \tag{5}$$

因此，在发送功率有限的情况下，为了最小化 $I(z;x)$，需要 $h(v)$ 最大化。v 应是复高斯噪声，即有 $v \sim \mathrm{CN}(0, s_v^2)$。式（5）可重写为

$$I(z;x) \leq \ln\left(1 + \frac{s_x^2}{s_v^2}\right) \tag{6}$$

等号成立的条件是输入信号 x 服从高斯分布 $x \sim \mathrm{CN}(0, s_x^2)$。以上结论反映了 AWGN 信道下的互信息的特性，对于给定的发送信源，存在一种最差的信道使得信道输出的信息量最小，即互信息是信道传递概率的 U 型凸函数。因此，为使 Eve 获取最少的信息量，应使预处理之后等效成最差的传输信道。

3.2 乘性随机化预处理

同样，当单独考虑乘性随机化预处理时，式（1）可以重新写成

$$z = wx \tag{7}$$

当 w 和 x 相互独立并且 Eve 无法预知 w 信息时，乘性随机化等效成信道衰落，将会降低 Eve 获取关于 x 的信息。为分析 w 的分布特性，在 w 和 x 均是非零随机变量时，对式（7）两边取自然对数变换。根据复数域的自然对数运算的定义，当 $x = a + \mathrm{j}b = A_x \mathrm{e}^{\mathrm{j}?_x}$，其中，$A_x$ 和 $?_x$ 分别为 x 的幅度和相位，有 $\ln x = \ln A_x + \mathrm{j}?_x$。于是式（7）可以重写为

$$\begin{aligned} \ln z &= \ln(wx) = \ln w + \ln x \\ &= \ln A_w + \mathrm{j}?_w + \ln A_x + \mathrm{j}?_x \end{aligned} \tag{8}$$

其中，A_w 和 $?_w$ 分别为 w 的幅度和相位。通过对数变换可以把乘性随机化等效成幅度和相位的加性随机化。为刻画 w 的分布特性以使 $I(z;x)$最小化，有如下定理成立。

定理 1 假定 $w = A_w \mathrm{e}^{\mathrm{j}?_w}$ 是非零随机变量，对发送信号 x 随机化预处理 $z = wx$，当 w 的幅度 A_w 满足对数高斯分布，而相位 $?_w$ 在[- p, p]内均匀分布并且与 A_w 保持相互独立时，$I(z;x)$满足如下不等式

$$I(z;x) \leq \frac{1}{2}\ln\left(1 + \frac{s_{A_x}^2}{s_{A_w}^2}\right) \tag{9}$$

其中，$s_{A_w}^2$ 和 $s_{A_x}^2$ 分别是 $\ln A_w$ 和 $\ln A_x$ 的功率约束。

为证明定理 1，首先考虑对数转化过程中互信息的变化。引理 1 说明了复数域随机变量的对数操作可以保持互信息不变。为叙述简便，以小写 x 表示相应随机变量 X 的随机实现，约定积分区间为相应随机变量的定义域。

引理 1 给定 W 和 X 是非零且相互独立的复随机变量，对等式 $Y = WX$ 两边取自然对数得到 $\ln Y = \ln W + \ln X$，在此令 $\ln Y = U$、$\ln W = K$ 及 $\ln X = V$，则 $I(Y;X) = I(U;V)$。

为证明引理 1，首先给出差熵的 2 个性质。

性质 1 给定 X 是非零复随机变量，令 $Y = wX$ 且 w 是非零的复常数，则 $h(Y) = h(X) + 2\ln|w|$。

证明 令 $w = A_w \mathrm{e}^{\mathrm{j}?_w}$，有 $\ln w = \ln A_w + \mathrm{j}?_w$。假定随机变量 X 和 Y 的概率密度函数分别为 $p_X(x)$ 和 $p_Y(y)$，则 $p_Y(y) = \frac{1}{|w|^2} p_X\left(\frac{y}{w}\right)$。$Y$ 的差熵为

$$\begin{aligned} h(Y) &= -\int p_Y(y)\ln p_Y(y)\mathrm{d}y \\ &= -\int \frac{1}{|w|^2}p_X\left(\frac{y}{w}\right)\ln\frac{1}{|w|^2}p_X\left(\frac{y}{w}\right)\mathrm{d}y \\ &= -\int p_X(x)\ln\frac{1}{|w|^2}p_X(x)\mathrm{d}x \\ &= \ln|w|^2 - \int p_X(x)\ln p_X(x)\mathrm{d}x \\ &= \ln|w|^2 + h(X) \end{aligned} \tag{10}$$

性质 2　给定 Y 是非零复随机变量，其对数运算 $U=\ln Y$，则 $h(Y)=2\mathrm{E}[\ln A_y]+h(U)$。

证明　令 $Y=A_y\mathrm{e}^{\mathrm{j}?_y}$，有 $\ln Y=\ln A_y+\mathrm{j}?_y$。假定 U 和 Y 的概率密度函数分别为 $p_U(u)$ 和 $p_Y(y)$，则 $p_Y(y)=\frac{1}{|y|^2}p_U(\ln y)$。$Y$ 的差熵为

$$\begin{aligned} h(Y) &= -\int p_Y(y)\ln p_Y(y)\mathrm{d}y \\ &= -\int \frac{1}{|y|^2}p_U(\ln y)\ln\frac{1}{|y|^2}p_U(\ln y)\mathrm{d}y \\ &= \int \frac{1}{|y|^2}p_U(\ln y)\ln|y|^2\,\mathrm{d}y - \\ &\quad \int \frac{1}{|y|^2}p_U(\ln y)\ln p_U(\ln y)\mathrm{d}y \\ &= \int \ln|y|^2\ p_U(u)du - \int p_U(u)\ln p_U(u)\mathrm{d}u \\ &= \mathrm{E}[\ln|y|^2]+h(U) \end{aligned} \tag{11}$$

证明(引理 1)　假定 X 的概率密度函数为 $p_X(x)$，首先考虑 Y 与 X 之间的互信息

$$\begin{aligned} I(Y;X) &= h(Y)-h(Y|X) \\ &= h(Y)-\int h(Y|X=x)p_X(x)\mathrm{d}x \\ &= h(Y)-\int h(xW)p_X(x)\mathrm{d}x \end{aligned} \tag{12}$$

根据差熵的性质 1，当 x 固定，而 W 为随机变量时，有 $h(xW)=h(W)+\ln|x|^2$，于是式(12)可以继续写成

$$\begin{aligned} I(Y;X) &= h(Y)-\int[h(W)+\ln|x|^2]p_X(x)\mathrm{d}x \\ &= h(Y)-h(W)-\int \ln|x|^2\ p_X(x)\mathrm{d}x \\ &= h(Y)-h(W)-2\mathrm{E}[\ln|x|] \end{aligned} \tag{13}$$

给定 $U=\ln Y=\ln A_y+\mathrm{j}?_y$ 和 $K=\ln W=\ln A_w+\mathrm{j}?_w$ 根据差熵的性质 2，有 $h(Y)=2\mathrm{E}[\ln A_y]+h(U)$ 和 $h(W)=2\mathrm{E}[\ln A_w]+h(K)$ 成立，式（13）写成

$$\begin{aligned} I(Y;X) &= 2\mathrm{E}[\ln A_y]+h(U)- \\ &\quad 2\mathrm{E}[\ln A_w]-h(K)-2\mathrm{E}[\ln A_x] \\ &= h(U)-h(K) \\ &= h(U)-h(K+V|V) \\ &= h(U)-h(U|V) \end{aligned} \tag{14}$$

因此有 $I(U;V)=I(Y;X)$ 成立。

证明(定理 1)　根据引理 1，乘性随机化预处理经过对数运算后可以等效成加性随机化预处理，并且保持了原有的互信息不变。于是对于等式 $\ln z=\ln w+\ln x$，为使 $I(z;x)$ 最小化，应使 $\ln w$ 为高斯噪声。因此，$\ln w=\ln A_w+\mathrm{j}?_w$ 的实部和虚部应保持相互独立，并且 w 的幅度 A_w 满足对数高斯分布，即 $\ln A_w\sim\mathrm{N}(0,s^2_{A_w})$，而相位 $?_w$ 在[- p, p]内均匀分布。从而有 $I(z;x)$ 满足式（9）。

根据定理 1 给出的结论及证明过程可以得出，当发送信号经历时变衰落信道，而 Eve 又无法预知衰落权值时，乘性衰落会造成发送信号的信息损失。而当乘性衰落满足定理 1 给定的条件时，信息损失将会最大化，即发送信号遭受最差的传输信道。此外，由式（9）可知，w 对发送信号的影响等价于 $\ln A_w$ 对 $\ln x$ 的影响。因此在 w 选定最佳分布时，$\ln A_w$ 的功率 $s^2_{A_w}$ 并不是 w 产生的直接发送功率。根据对数高斯分布函数定义[15]，A_w 的概率密度函数为（假定其均值为零）

$$f(A_w)=\frac{1}{A_w\sqrt{2\pi s^2}}\mathrm{e}^{\frac{-(\ln A_w)^2}{2s^2}} \tag{15}$$

其中，$s^2=s^2_{A_w}$ 为对数高斯分布的尺度参数。A_w 的均值和方差则分别为：$\mathrm{e}^{s^2/2}$ 和 $(\mathrm{e}^{s^2}-1)\mathrm{e}^{s^2}$。当产生功率 $(\mathrm{e}^{s^2}-1)\mathrm{e}^{s^2}$ 的对数高斯分布 A_w，实际只有功率 $s^2=s^2_{A_w}$ 的等效高斯噪声对 Eve 的接收造成影响。因此，最佳分布的乘性随机化处理对 A_w 的功率具有对数压缩效果。

为对上述论证进行实例化分析，下面基于文献[10]子载波参考安全传输机制进行一般化扩展，分析指出扩展后其中可能存在的安全隐患，并提出随机子载波参考安全传输机制。最后仿真分析了乘性随机化预处理权值的优化设计。

4　实例分析——随机子载波参考安全传输机制

针对分布式 OFDM 异步协作系统，Z. LI 等人

提出子载波参考的安全传输机制[10]。由于安全机制关注的重点在于随机化预处理对安全性的贡献，因而在此对该机制的应用条件进行一般化扩展，即暂不考虑原文中节点的定时错误对安全性的影响。所有可用的 N 个子载波等分成 P 组数据子载波和 P 组导频子载波，每组具有 $\lfloor N/2P \rfloor = JG$ 个子载波（J 为中继节点数，于是每个中继节点在每组中可以拥有 G 个子载波）。每个子载波只被一个节点占用，其他节点在该子载波上不发送信号。子载波参考安全传输机制在导频和数据子载波之间，按如下约束建立随机化预处理权值的参考关系

$$w_i^j h_{b,i}^j = w_{N-i-1}^j h_{b,N-i-1}^j,$$
$$i \in \{(p-1)JG + (j-1)G + (0,1,\cdots,G-1)\} \quad (16)$$

其中，w_i^j 和 w_{N-i-1}^j 分别是中继节点 j 为数据子载波 i 和导频子载波 $N-i-1$ 设定的随机化预处理权值，$h_{b,i}^j$ 和 $h_{b,N-i-1}^j$ 分别为 Bob 相应子载波的频域信道响应。Bob 基于导频子载波可以顺利完成差分译码。由于信道的差异性，Eve 的子载波之间并不满足以上参考关系

$$w_i^j h_{e,i}^j \neq w_{N-i-1}^j h_{e,N-i-1}^j,$$
$$i \in \{(p-1)JG + (j-1)G + (0,1,\cdots,G-1)\} \quad (17)$$

Eve 无法进行差分译码。此外，当 w_i^j 随机改变时，Eve 接收信号表现为随机快变，从而抑制了 Eve 对发送信号的盲估计。

但是在未知 Eve 任何信息时，无法限制 Eve 可能采用的译码方法。由式(16)分析发现当信道保持慢时变时，尽管 w_i^j 和 w_{N-i-1}^j 在每个 OFDM 符号中随机选择，但是比值 $w_i^j / w_{N-i-1}^j = h_{b,N-i-1}^j / h_{b,i}^j$ 保持慢时变。因此，Eve 不一定执行差分译码，而是依据导频与数据子载波的比值执行对发送信号的估计。Eve 接收的信号可以表示为

$$\begin{cases} y_{e,i}^j = h_{e,i}^j w_i^j \cdot x_i^j + n_{e,i}, \\ i \in \{(p-1)JG + (j-1)G + (0,1,\cdots,G-1)\} \\ y_{e,N-i-1}^j = h_{b,N-i-1}^j w_{N-i-1}^j \cdot 1 + n_{e,N-i-1} \end{cases} \quad (18)$$

其中，$y_{e,i}^j$ 和 $y_{e,N-i-1}^j$ 分别是 Eve 在子载波 i 上接收到由中继节点 j 发送的数据和导频。当处于高 SNR 时，Eve 可以消除 w_i^j 的影响。

$$\bar{y}_{e,i}^j = \frac{y_{e,i}^j}{y_{e,N-i-1}^j} = \frac{h_{e,i}^j w_i^j \cdot x_i^j + n_{e,i}}{h_{b,N-i-1}^j w_{N-i-1}^j \cdot 1 + n_{e,N-i-1}}$$
$$\cong \frac{h_{e,i}^j h_{b,N-i-1}^j \cdot x_i^j}{h_{b,N-i-1}^j h_{b,i}^j} @ \bar{h}_{e,i}^j x_i^j \quad (19)$$

其中，$\cong$ 为高 SNR 近似。因此当 Bob 和 Eve 的信道慢时变，Eve 可以对 $\bar{h}_{e,i}^j$ 进行盲估计[16]。对于一般化扩展后的机制，产生以上安全隐患的原因是数据与导频子载波之间的参考关系保持相对固定。为此提出随机子载波参考机制，如图 2 所示。

Alice 通过配置有单天线的 J 个信任中继向 Bob 传递私密信息。假定系统为时分双工互易系统，中继节点基于反向导频获取与 Bob 之间的信道信息。中继网络不存在簇节点，即节点之间无法进行信息共享。同样把 N 个子载波分成导频和数据子载波组。但是对于每个数据子载波 i，Alice 随机选择一个中继节点 j 转发数据。被选中的节点同时设定子载波 $i+1$ 为导频子载波，并在子载波 i 和 $i+1$ 之间构建随机化权值 (w_i^j, w_{i+1}^j) 的参考关系。

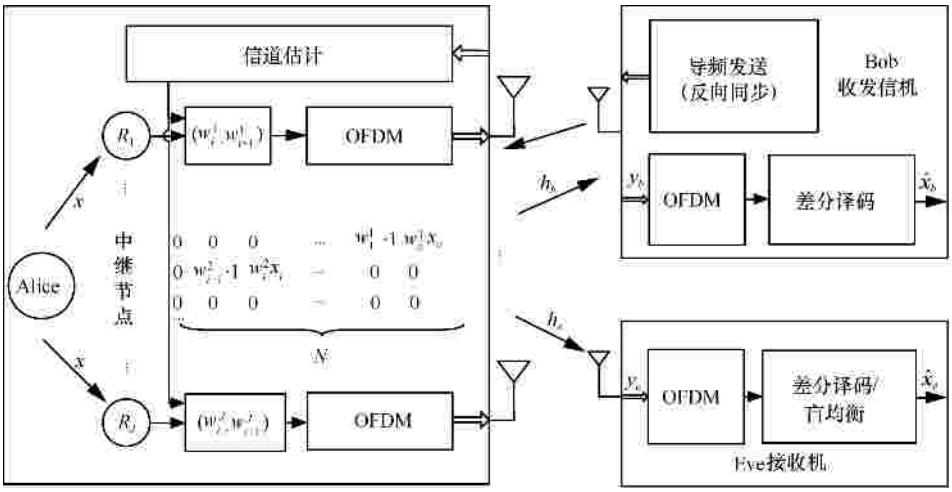

图 2 随机子载波参考安全传输机制结构

$$w_i^j h_{b,i}^j = w_{i+1}^j h_{b,i+1}^j,$$
$$\{i = 2n < N-1 \,|\, n \in N\},\ 1 \le j \le J \qquad (20)$$

在相邻的子载波之间形成数据和导频的权值参考关系，Bob 同样可以进行差分译码。但是每个数据子载波由 Alice 随机选择中继节点，导致每个 OFDM 符号中的子载波参考关系随机变化。Eve 接收的信号不具有式（20）的参考关系，并且式（19）中随机权值的比值在不同符号之间同样表现为随机变化，因此 Eve 无法采取类似的盲检测方法进行估计[16]。

然而，无论是固定的子载波参考还是随机子载波参考机制，随机权值的设计是保障安全的关键。为最大程度降低 Eve 可能获取的信息，根据线性随机化安全传输模型，不同子载波上的随机化权值应促使发送信息预处理之后泄漏最小化。考虑到不同子载波之间的正交性，数据子载波组可以看成是多维独立并行子信道。每个数据子载波的随机权值可以任意选取，依据定理 1 给出的相关结论，恰当地选取每个数据子载波上的随机化预处理权值可以使得预处理之后的信息损失最大化。因此，每个被选中的中继节点 j 为子载波 i 设定的 w_i^j 的幅度 $A_{w_i^j}$ 应服从对数高斯分布，而相位 $?_{w_i^j}$ 应在[- p, p]内独立均匀产生。随机子载波参数安全传输机制的完整发送过程如图 3 所示。

for i =0 : 2 : N- 1

Alice 随机选择中继节点 $j(1 \le j \le J)$ ；

中继节点 j 依据式（15）分布为子载波 i 产生 $A_{w_i^j}$ ，在[- p, p]中独立均匀产生相位 $q_{w_i^j}$ ；

中继节点 j 按下式为子载波 i+1 设定 w_{i+1}^j ，

$w_i^j h_{b,i}^j = w_{i+1}^j h_{b,i+1}^j$，$w_i^j = A_{w_i^j} \mathrm{e}^{\mathrm{j}q_{w_i^j}}$ ；

中继节点 $m(1 \le m \le J, m \ne j)$ 设定 $w_i^m = w_{i+1}^m = 0$ ；

end

中继节点 j 发送 OFDM 符号：$[w_0^j x_0, w_1^j \cdot 1, \mathrm{L}, \ w_{N-2}^j x_{N-2}, w_{N-1}^j \cdot 1]$

图 3　随机子载波参考安全机制

5　仿真分析

本节首先仿真验证随机子载波参考机制的安全性，并基于此分析最佳分布乘性随机化权值设计。假定系统配置 $J = 4$ 个中继节点，每个 OFDM 符号包括 128 个子载波并分享 1MHz 带宽，从而符号间隔时间 128 μs，循环前缀时长设定为 32 μs。假定 L 阶信道模型可以表示为 $h(t) = \sum_{l=1}^{L} a_l d(t - t_l)$，$a_l$ 为信道抽头增益并满足复高斯分布，t_l 是相应的路径时延，归一化 $\sum_{l=1}^{L} \mathrm{E}[a_l a_l^{\mathrm{H}}] = 1$。每个中继节点与 Bob 和与 Eve 之间的信道独立产生并保持恒定。在给定 $\mathrm{E}|x|^2 = 1$ 时，系统的总体平均发送功率满足 $\sum_{j=1}^{J} \sum_{i=0}^{N-1} s_{w_i^j}^2 \le P_t$，其中，$s_{w_i^j}^2$ 为 w_i^j 的功率，实际每个 OFDM 符号只会随机产生 N 个有效权值 w_i^j。

为便于比较，对从文献[10]中一般化扩展后的子载波参考安全传输机制进行了同样条件的仿真，并设定分组数 $P = 4$。图 4 和图 5 分别给出了频率选择性信道（$L = 3$）和平坦信道（$L = 1$）下的性能对比。从图中可以看出，由于缺乏数据和导频子载波之间的权值参考关系，当采用差分译码时，Eve 在 2 种安全机制下均具有很高的误码率，无法恢复发送的信息。然而，当 Eve 基于数据与导频子载波的比值对发送信号进行盲估计时，在扩展后的子载波参考安全传输机制中误码率逐渐下降，Eve 从而可以恢复部分信息。尽管盲估计性能受到信道选择性衰落和噪声的影响，Eve 仍可以逐渐改善接收环境以提高信噪比。但这种盲估计的方法对于随机子载波参考安全传输机制却是无效的，因为数据与导频子载波之间由于中继节点的选择并不存在稳定的参考关系。

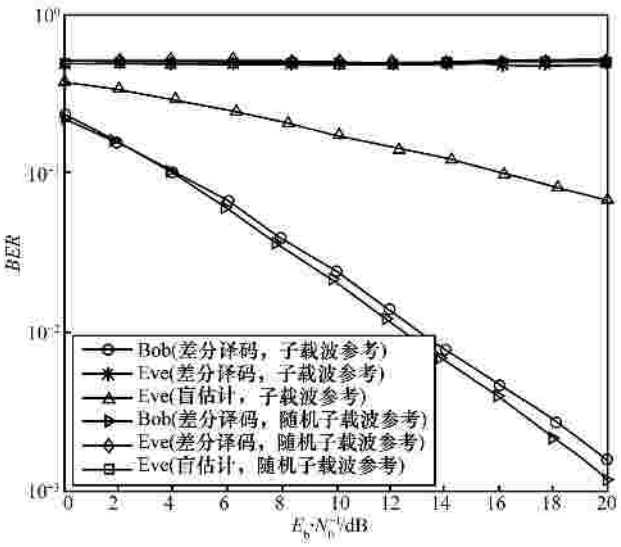

图 4　选择性信道下的安全机制性能对比

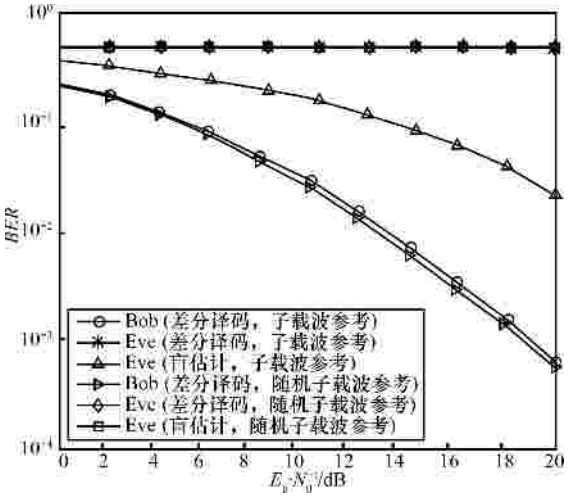

图 5 平坦信道下的安全机制性能对比

虽然上述结果表明随机子载波参考机制可以有效抑制 Eve 的窃听行为，但在未知 Eve 信道信息时仍然无法确定 Eve 获取的信息量。随机化权值的优化目标是期望 Eve 可能获取的信息最小化。针对随机子载波参考安全机制，图 6 给出了乘性随机化权值分别以复高斯分布和以定理 1 给定的最佳分布产生时的性能。可以看出，不同分布形成的随机化权值，Eve 均具有较高的误码率，但是最佳分布的随机化权值却可以降低预处理之后的信息泄露。此外，对于 Bob 的接收，由于对数高斯分布对发送功率的压缩效果，从而区别于复高斯分布时接收性能。值得指出的是，误码率的衡量不仅受到信道速率的约束还依赖于所采取的译码方法。

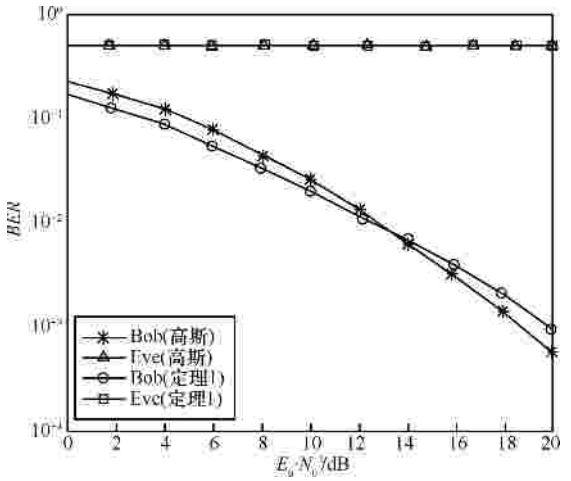

图 6 不同分布乘性随机化预处理值下安全机制性能对比

6 结束语

特定的随机化信号处理可以为合法用户提供信道优势，从而抑制窃听者的有效截获。本文给出了线性随机化预处理安全传输模型，包括加性和乘性预处理并把预处理模块建模成级联信道。本文重点论证了随机化权值的最佳分布特性。为最大程度降低窃听者获取的信息，加性随机化权值应服从复高斯分布，而乘性随机化权值的幅度服从对数高斯分布并具有独立均匀分布的相位。最后提出随机子载波参考安全机制对乘性权值的优化设计进行了仿真验证。但是上述论证均假定了随机化矢量的元素保持相互独立，这是最为基础的特性分析，尤其是对数操作对乘性权值的转化，可以为实际随机化权值的设计提供参考。为避免对合法用户造成影响，往往需要在权值矢量的元素之间构造相关约束，此时的权值分布是后续工作的重点。正如文中指出，物理层安全技术目前还主要集中于不同信道模型下的信息理论安全研究，但安全容量的计算需要窃听者的信道信息。当窃听者为系统用户（如小区用户）时，可以用以防止不同用户之间的信息窃听，故需要考虑网络场景下的安全理论分析。然而更为通用的场景则是存在被动窃听和主动攻击情况（如军事通信），因此实用的安全机制亟待研究。

参考文献：

[1] SHIU Y S, CHANG S Y, WU H C. Physical layer security in wireless networks: a tutorial[J]. IEEE Wireless Communications, 2011, 18(2): 66-74.

[2] LIANG Y, POOR H V, SHAMAI (SHITZ) S. Information theoretic security[J]. Foundations and Trends in Communications and Information Theory, 2008, 5(4/5): 355-580.

[3] WYNER D. The wire-tap channel[J]. Bell System Technical Journal, 1975, 54(8): 1355-1387.

[4] CSISZÁR I, KÖRNER J. Broadcast channels with confident l messages[J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[5] BUSTIN R, LIU R, POOR H V. An MMSE approach to the secrecy capacity of the MIMO Gaussian wiretap channel[J]. EURASIP Journal Wireless Communication Network-special Issue on Wireless Physical Layer Security, 2009,(7).

[6] GOEL S, NEGI R. Guaranteeing secrecy using artificial noise[J]. IEEE Transactions on Wireless Communication, 2008, 7(6): 2180- 2189.

[7] SWINDLEHURST A L. Fixed SINR solutions for the MIMO wiretap channel[A]. Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Taipei, China, 2009.

[8] LI X, HWU J, RATAZZI E P. Using antenna array redundancy and channel diversity for secure wireless transmissions[J]. Journal on Communication, 2007, 2(3): 24-32.

[9] 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[J]. 西安交通大学学报. 2010,44(6):62-66.

（下转第 58 页）