基于多随机信号流的密钥生成方案

金 梁 蔡奥林* 黄开枝 钟 州 楼洋明
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：基于随机信号流的密钥生成方案会在合法发送方发送随机信号时泄露部分共享随机源信息导致密钥安全性和可达密钥速率较低。针对此问题，该文提出一种基于多随机信号流的密钥生成方案。首先，发送方利用信道互易性和上行导频估计下行信道，然后发送方在各天线上发送相互独立的随机信号流。由于窃听者难以准确估计所有随机信号流，因此难以窃取接收方每根天线接收到的叠加随机信号，而发送方则可根据估计的下行信道和自身发送的随机信号流计算出接收方各天线的接收信号。因此，可以将接收天线上的叠加随机信号作为共享随机源提取密钥。进一步地，该文还推导了该方案的可达密钥速率和共享随机源的互信息量表达式，并分析了两者间的关系以及对密钥安全性的影响。最后，通过仿真验证了该方案的有效性，仿真结果表明该方案能够有效降低窃听者观察到的共享随机源互信息，从而提升可达密钥速率及密钥安全性。

关键词：物理层安全；多随机信号流；密钥生成；可达密钥速率
中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2019)06-1405-08
DOI: 10.11999/JEIT181040

Secret Key Generation Method Based on Multi-stream Random Signal

JIN Liang CAI Aolin HUANG Kaizhi ZHONG Zhou LOU Yangming
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450002, *China*)

Abstract: The secret key generation method based on random signal may leak part of the common randomness information and reduce the achievable secret key rate when legal transmitter transmits random signal. In response to this problem, the secret key generation method based on multi-stream random signal is proposed. Firstly, the transmitter uses the channel reciprocity and uplink pilot to estimate the downlink channel, then the transmitter transmits mutually independent signal on every antenna. The eavesdropper is difficult to estimate all the random signals. It is difficult to estimate all the random signals for the eavesdropper, so the overlapping signal received by every antenna is difficult to be obtained by the eavesdropper. However, the legal transmitter is able to calculate the signal received by legal receiver by using the downlink channel estimated and the signal transmitted. So, the overlapping signal on every legal antenna can be used to extract secret key as common randomness. Also, the achievable secret key rate expression and the mutual information expression of common randomness are derived, and the relationship between them and the secret key security is analyzed. At last, the effectiveness of this method is verified by the simulation. The simulation results show that this method can reduce the common randomness observed by the eavesdropper to raise the achievable secret key rate and secret key security.

Key words: Physical layer security; Multi-stream random signal; Secret key generation; Achievable secret key rate

1 引言

近年来，无线物理层密钥生成技术利用无线信道的时变性、互易性和空间去相关性的特点生成密钥，为解决无线通信安全问题带来了新的思路[1,2]。

Maurer[3]最早对物理层密钥生成技术进行了研究，给出了可达密钥速率定义，并推导出了其上下界，为密钥生成提供了信息论理论基础。而无线信道十分适合作为Maurer所述的共享随机源用来提取密钥。于是，多种无线物理层密钥生成的方案相继被提出。例如，最常见的利用信号强度的密钥生成方案[4]，也有文献[5]提出了从相位中提取密钥，但是相位信息容易受到噪声干扰。文献[6]认为以上

收稿日期：2018-11-14；改回日期：2019-03-07；网络出版：2019-04-04
*通信作者： 蔡奥林 alcai@stu.xidian.edu.cn
基金项目：国家重点研发计划(2017YFB0801903)，国家自然科学基金(61601514, 61501516, 61521003, 61471396)
Foundation Items: The National Key Research and Development Program of China (2017YFB0801903), The National Natural Science Foundation of China (61601514, 61501516, 61521003, 61471396)

方案并没有充分利用信道的随机性，而多径的时延可以很好地体现信道随机性，于是对利用多径时延提取密钥的方法进行了研究。以上方案均依靠信道的快速变化更新密钥。但是对于“万物互联”的5G物联网场景来说，并非所有的节点都有快速变化的信道。例如，智能家居和智能水表等物联网设备一般情况下是不动的，导致无线信道参数变化十分缓慢，从而密钥生成速率很低。

因此，文献[7–12]通过各种手段增加共享随机源的随机性，以提升密钥生成速率。文献[7]提出利用随机波束成形来模拟信道的波动变化，以弥补信道变化的不足。文献[8]针对多天线系统，随机改变各个天线上的幅度和相位来模拟信道的波动变化。同时，文献[9–10]通过引入节点协作产生干扰增加信道的随机性从而提高密钥速率，但是这种方法需要引入节点进行协作，难免会对资源受限的系统造成负担。以上研究的本质都是增加共享随机源的随机性，但是并没有给出此类密钥生成方法的性能理论分析。因此，文献[11,12]建立了引入随机源并从接收信号中提取密钥的模型，并分析了可达密钥速率，相比于从信道中提取密钥的方案有较大的提升。但是被动窃听者也能通过观察合法用户发送的随机信号窃取部分共享随机源的信息，不仅限制了可达密钥速率也对具体的密钥生成方法实施造成很大困难。

针对以上问题，本文结合基于随机信号流的密钥生成机制，针对MIMO系统提出了基于多随机信号流的密钥生成方案。首先，合法发送方利用信道互易性和上行导频估计下行信道，然后发送方在各天线上发送相互独立的随机信号流。由于窃听者难以准确估计合法方发送的所有随机信号流，因此更难窃取合法接收方每根天线收到的叠加随机信号，而发送方则可根据估计的下行信道和自身发送的随机信号流计算出接收方各天线的接收信号。因此，可以将合法接收天线上的叠加随机信号作为共享随机源提取密钥。然后，本文还推导了该方案的可达密钥速率和共享随机源的互信息量表达式，并分析了两者间的关系以及对密钥安全性的影响。最后，通过仿真验证了该方案的有效性，仿真结果表明该方法能够有效降低窃听者观察到的共享随机源互信息，从而提升可达密钥速率，且发送随机信号流数目越多，窃听者能够获取的共享随机源互信息越少，当发送随机信号流数目趋于无穷时，窃听者获取的信息趋近于0，可达密钥速率逼近于共享随机源的互信息量。

2 系统模型

建立如图1所示的多天线系统模型，Alice是合法发送方，配备N_a根天线。Bob是合法接收方，配备N_b根天线。在系统的通信范围内，存在配备N_e根天线的窃听者Eve试图被动窃听。

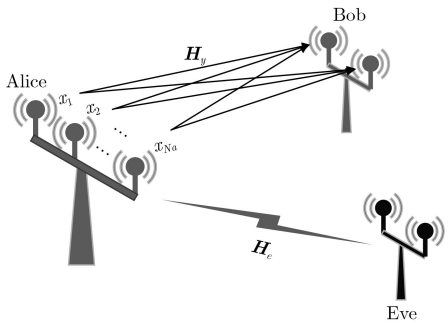

图 1 系统模型

假设所有信道模型都是准静态块衰落信道。Alice与Bob间的信道为$\boldsymbol{H}_y=[\boldsymbol{h}_{y,1}^{\mathrm{T}}\ \boldsymbol{h}_{y,2}^{\mathrm{T}}\cdots\boldsymbol{h}_{y,N_B}^{\mathrm{T}}]^{\mathrm{T}}\in\mathbb{C}^{N_b\times N_a}$，$\boldsymbol{h}_{y,i}=[h_{y,i,1},\ h_{y,i,2},\ \cdots,\ h_{y,i,N_A}]\in\mathbb{C}^{1\times N_a}$，Bob与Eve间的信道为$\boldsymbol{H}_e\in\boldsymbol{C}^{N_e\times N_a}$。$\boldsymbol{H}_y$与$\boldsymbol{H}_e$中元素独立同分布且都是服从均值为0，方差为1的复高斯分布的随机变量。

假设Alice发射随机信号矢量给Bob, Bob和Eve的接收信号为

$$\boldsymbol{Y}=\boldsymbol{H}_y\boldsymbol{X}+\boldsymbol{n}_b \tag{1}$$

$$\boldsymbol{Z}=\boldsymbol{H}_e\boldsymbol{X}+\boldsymbol{n}_e \tag{2}$$

其中，$\boldsymbol{n}_b$是合法接收方天线上的加性高斯白噪声矢量，$\boldsymbol{n}_e$是窃听者天线上的加性高斯白噪声矢量，其中的各元素独立同分布，且方差分别为σ_b^2和σ_e^2。$\boldsymbol{X}=[x_1,x_2,\cdots,x_{N_A}]^{\mathrm{T}}\in\mathbb{C}^{1\times N_a}$为Alice的发送信号矢量。假设发送方各随机信号相互独立，且服从复高斯分布

$$\boldsymbol{K}_{\boldsymbol{XX}}=\mathrm{E}\left(\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}}\right)=\begin{pmatrix}\sigma_1^2 & & & \\ & \sigma_2^2 & & \\ & & \ddots & \\ & & & \sigma_{N_A}^2\end{pmatrix} \tag{3}$$

发送信号总功率满足$P=\sum_{i=1}^{N_a}\sigma_i^2$。发送的多个随机流经过多个不同的信道衰落之后，Bob的每根天线上都接收到N_a个随机信号流的叠加。则接收信号为

$$\begin{aligned}\boldsymbol{Y}&=\begin{bmatrix}h_{y,1,1} & h_{y,1,2} & \cdots & h_{y,1,N_a}\\ h_{y,2,1} & h_{y,2,2} & \cdots & h_{y,2,N_a}\\ \vdots & \vdots & \ddots & \vdots\\ h_{y,N_b,1} & h_{y,N_b,2} & \cdots & h_{y,N_b,N_a}\end{bmatrix}\begin{bmatrix}x_1\\ x_2\\ \vdots\\ x_{N_a}\end{bmatrix}+\boldsymbol{n}_b\\ &=\left[\sum_{j=1}^{N_a}h_{y,1,j}x_j\ \sum_{j=1}^{N_a}h_{y,2,j}x_j\ \cdots\ \sum_{j=1}^{N_a}h_{y,N_B,j}x_j\right]^{\mathrm{T}}+\boldsymbol{n}_b\end{aligned} \tag{4}$$

由于Bob每根天线上的叠加的随机源中具有N_a个随机信号流，针对于Bob的一根天线上的叠加随机源，Eve需要同时准确地估计N_a个随机信号流及相应的信道信息才能够估计这根天线接收到的叠加随机信号，所以难以窃取到Bob每根天线上接收信号，因此可以利用Bob每根天线上的叠加随机源来提取密钥。

Alice可以根据信道的互易性利用Bob发送的导频信号得到信道信息$\boldsymbol{H}_y$，那么Alice估计到的Bob接收信号为

$$\begin{aligned}\tilde{\boldsymbol{Y}}&=\begin{bmatrix}h_{y,1,1}&h_{y,1,2}&\cdots&h_{y,1,N_a}\\h_{y,2,1}&h_{y,2,2}&\cdots&h_{y,2,N_a}\\\vdots&\vdots&\ddots&\vdots\\h_{y,N_b,1}&h_{y,N_b,2}&\cdots&h_{y,N_b,N_a}\end{bmatrix}\begin{bmatrix}x_1\\x_2\\\vdots\\x_{N_a}\end{bmatrix}\\&=\left[\sum_{j=1}^{N_a}h_{y,1,j}x_j\ \sum_{j=1}^{N_a}h_{y,2,j}x_j\ \cdots\ \sum_{j=1}^{N_a}h_{y,N_B,j}x_j\right]^{\mathrm{T}}\end{aligned}\tag{5}$$

Alice和Bob可分别利用式(5)和式(4)中的随机源来提取密钥，信道参数在整个密钥生成过程中不发生变化，密钥生成过程所用时间为T_0。在文献[12]使用的波束成形方案中，共享随机源$\boldsymbol{y}=[\lambda_1x_1,\lambda_2x_2,\cdots,\lambda_rx_r]^{\mathrm{T}}$，其中$\lambda_i\,(i=1,2,\cdots,r)$是信道矩阵的奇异值，$r$为信道的秩，可见对于其中一个共享随机源，Eve只需要能够估计到一个随机信号流$\lambda_ix_i\ (i=1,2,\cdots,r)$即可。而本文的方案中，Eve获取其中一个共享随机源需要准确估计N_a个随机信号流$h_{y,i,1}x_1,h_{y,i,2}x_2,\cdots,h_{y,i,N_a}x_{N_a}(i=1,2,\cdots,N_b)$。对于Eve来说，从本文的方案中窃取到共享随机源的难度更大一些，所以本文方案有利于密钥的安全性和可达密钥速率的提升。

3　基于多随机信号流的密钥生成方案理论分析

3.1　可达密钥速率分析

可达密钥速率[12]可以作为方案性能的度量指标。可达密钥速率的表达式如式(6)所述。

由文献[13]知，可达密钥速率的下界为

$$\begin{aligned}C_{s,\mathrm{lb}}=\max\Big\{&I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)-I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Z}\right),\\&I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)-I(\boldsymbol{Y};\boldsymbol{Z})\Big\}\end{aligned}\tag{6}$$

根据文献[14]，$\boldsymbol{Z}\to\tilde{\boldsymbol{Y}}\to\boldsymbol{Y}$可以构成马尔可夫链，所以

$$\begin{aligned}I\left(\boldsymbol{Z};\boldsymbol{Y},\tilde{\boldsymbol{Y}}\right)&=I(\boldsymbol{Y};\boldsymbol{Z})+I\left(\boldsymbol{Z};\tilde{\boldsymbol{Y}}\,|\,\boldsymbol{Y}\right)\\&=I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Z}\right)+I\left(\boldsymbol{Z};\boldsymbol{Y}\,|\,\tilde{\boldsymbol{Y}}\right)\end{aligned}\tag{7}$$

由马尔可夫链的无后效性，可知

$$I\left(\boldsymbol{Z};\ \boldsymbol{Y}|\,\tilde{\boldsymbol{Y}}\right)=0\tag{8}$$

且由于$I\left(\boldsymbol{Z};\ \tilde{\boldsymbol{Y}}|\,\boldsymbol{Y}\right)\ge0$，则有

$$I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Z}\right)\ge I(\boldsymbol{Y};\ \boldsymbol{Z})\tag{9}$$

所以

$$\begin{aligned}C_{s,\mathrm{lb}}=\max\Big\{&I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)-I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Z}\right),I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)\\&-I(\boldsymbol{Y};\boldsymbol{Z})\Big\}=I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)-I(\boldsymbol{Y};\boldsymbol{Z})\end{aligned}\tag{10}$$

$$I(\boldsymbol{Y};\boldsymbol{Z})=\log_2\frac{\left|\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\,\sigma_b^2\right|}{\left|\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\,\sigma_b^2-\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\left(\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}+\boldsymbol{I}_e\,\sigma_e^2\right)^{-1}\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}\right|}\tag{11}$$

共享随机源之间的互信息量为

$$I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)=\log_2\left|\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\,\sigma_b^2\right|\tag{12}$$

$$\begin{aligned}C_{s,\mathrm{lb}}=\log_2\Big|&\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\,\sigma_b^2\\&-\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\left(\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}+\boldsymbol{I}_e\,\sigma_e^2\right)^{-1}\\&\cdot\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}\Big|\end{aligned}\tag{13}$$

由文献[13]可知，可达密钥速率的上界为

$$C_{s,\mathrm{ub}}=\min\left\{I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right),I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)\right\}\tag{14}$$

其中，

$$I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right)=h(\boldsymbol{Y},\boldsymbol{Z})-h(\boldsymbol{Z})-h(\boldsymbol{Y}|\,\tilde{\boldsymbol{Y}},\boldsymbol{Z})\tag{15}$$

式(15)表示在给定随机变量$\boldsymbol{Z}$时的条件互信息。

由于

$$I\left(\boldsymbol{Z};\ \boldsymbol{Y}|\,\tilde{\boldsymbol{Y}}\right)=h(\boldsymbol{Y}|\,\tilde{\boldsymbol{Y}})-h(\boldsymbol{Y}|\,\tilde{\boldsymbol{Y}},\boldsymbol{Z})\tag{16}$$

所以根据式(8)及式(16)，可知

$$h(\boldsymbol{Y}|\,\tilde{\boldsymbol{Y}},\boldsymbol{Z})=h(\boldsymbol{Y}|\,\tilde{\boldsymbol{Y}})=\log_2(\pi e)^{N_b}\tag{17}$$

式(15)可以写为

$$\begin{aligned}I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right)&=\log_2(\pi e)^{N_b+N_e}\left|\mathrm{E}\begin{bmatrix}\boldsymbol{Y}\boldsymbol{Y}^{\mathrm{H}}&\boldsymbol{Y}\boldsymbol{Z}^{\mathrm{H}}\\\boldsymbol{Z}\boldsymbol{Y}^{\mathrm{H}}&\boldsymbol{Z}\boldsymbol{Z}^{\mathrm{H}}\end{bmatrix}\right|\\&\quad-\log_2(\pi e)^{N_e}\left|\mathrm{E}\left[\boldsymbol{Z}\boldsymbol{Z}^{\mathrm{H}}\right]\right|-\log_2(\pi e)^{N_b}\\&=\log_2\Big|\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\,\sigma_b^2\\&\quad-\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\left(\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\right.\\&\quad\left.+\boldsymbol{I}_e\,\sigma_e^2\right)^{-1}\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}\Big|\end{aligned}\tag{18}$$

其中，$\boldsymbol{K}_{\boldsymbol{XX}}$为功率分配矩阵，假设

$$\boldsymbol{K}_{\boldsymbol{XX}}=\boldsymbol{I}_a\frac{P}{N_a} \tag{19}$$

在这里，P是发送方的发送信号功率，N_a是发送方天线的数目。

由式(11)，式(12)，式(18)可知

$$I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)-I(\boldsymbol{Y};\boldsymbol{Z})=I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right) \tag{20}$$

由于互信息量总是非负的[14]，$I(\boldsymbol{Y};\boldsymbol{Z})\ge 0$，所以

$$I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right)\le I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right) \tag{21}$$

因此，

$$\begin{aligned}C_{s,\mathrm{ub}}&=\min\left\{I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right),I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)\right\}\\&=I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}|\boldsymbol{Z}\right)\\&=\log_2\left|\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\sigma_b^2-\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\right.\\&\quad\left.\cdot\left(\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}+\boldsymbol{I}_e\sigma_e^2\right)^{-1}\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}\right|\end{aligned} \tag{22}$$

所以，可达密钥速率具有相同的上下界，且可达密钥速率为

$$\begin{aligned}C_s&=\log_2\left|\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}+\boldsymbol{I}_b\sigma_b^2-\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\right.\\&\quad\left.\cdot\left(\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}+\boldsymbol{I}_e\sigma_e^2\right)^{-1}\boldsymbol{H}_e\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_y^{\mathrm{H}}\right|\end{aligned} \tag{23}$$

3.2 安全性分析

从式(10)，式(20)，式(23)可知：

$$I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right)=C_s+I(\boldsymbol{Y};\boldsymbol{Z}) \tag{24}$$

由于提取密钥时，是从$\tilde{\boldsymbol{Y}}$与$\boldsymbol{Y}$(共享随机源)中提取密钥，而从式(24)可以看出，提取的密钥中总会有部分信息是窃听方能够窃取到的，因此就导致了密钥的不安全性存在[15]。而发送的随机流数目(发送天线数目)越多，窃听者窃取共享随机源互信息的难度越大，$I(\boldsymbol{Y};\boldsymbol{Z})$也会越小。

定理1 假设合法接收方配置有限的N_b根天线，窃听方配置有限的N_e根天线，窃听方位于合法接收方半波长以外。当发送总功率保持不变，发送随机流数目(发送方天线数目)趋近于无穷大的时候，合法方的观测信号与窃听方的观测信号的互信息量为0，即窃听方无法观察到任何共享随机源互信息。

证明： 假设

$$\tilde{\boldsymbol{Z}}=\boldsymbol{H}_e\boldsymbol{X} \tag{25}$$

则窃听方接收信号为

$$\boldsymbol{Z}=\tilde{\boldsymbol{Z}}+\boldsymbol{n}_e \tag{26}$$

其中，$\boldsymbol{n}_e$为窃听方接收天线上的噪声。

$$\begin{aligned}\boldsymbol{R}_{\boldsymbol{Y}\tilde{\boldsymbol{Z}}}&=\lim_{N_a\to\infty}\mathrm{E}\left[\boldsymbol{Y}\tilde{\boldsymbol{Z}}^{\mathrm{H}}\right]\\&=\lim_{N_a\to\infty}\mathrm{E}\left[\boldsymbol{H}_y\boldsymbol{X}\boldsymbol{X}^{\mathrm{H}}\boldsymbol{H}_e^{\mathrm{H}}\right]\\&=\lim_{N_a\to\infty}\boldsymbol{H}_y\boldsymbol{K}_{\boldsymbol{XX}}\boldsymbol{H}_e^{\mathrm{H}}\\&=\lim_{N_a\to\infty}\frac{\boldsymbol{H}_y\boldsymbol{H}_e^{\mathrm{H}}P}{N_a}=\boldsymbol{0}\end{aligned} \tag{27}$$

由以上推导可知，$\boldsymbol{Y}$与$\tilde{\boldsymbol{Z}}$之间协方差矩阵为零矩阵。$\boldsymbol{Y}$与$\tilde{\boldsymbol{Z}}$间的互信息可由式(28)表示

$$\begin{aligned}I\left(\boldsymbol{Y};\tilde{\boldsymbol{Z}}\right)&=\log_2\left|\frac{\boldsymbol{R}_{\tilde{\boldsymbol{Z}}}}{\boldsymbol{R}_{\tilde{\boldsymbol{Z}}}-\boldsymbol{R}_{\tilde{\boldsymbol{Z}}\boldsymbol{Y}}\boldsymbol{R}_{\boldsymbol{Y}}^{-1}\boldsymbol{R}_{\boldsymbol{Y}\tilde{\boldsymbol{Z}}}}\right|\\&=0\end{aligned} \tag{28}$$

其中，$\boldsymbol{R}_{\tilde{\boldsymbol{Z}}}$, $\boldsymbol{R}_{\boldsymbol{Y}}$为方差矩阵，$\boldsymbol{R}_{\tilde{\boldsymbol{Z}}\boldsymbol{Y}}$, $\boldsymbol{R}_{\boldsymbol{Y}\tilde{\boldsymbol{Z}}}$为协方差矩阵。

$\boldsymbol{Y}\to\tilde{\boldsymbol{Z}}\to\boldsymbol{Z}$可构成马尔可夫链，所以

$$I(\boldsymbol{Y};\boldsymbol{Z})\le I\left(\boldsymbol{Y};\tilde{\boldsymbol{Z}}\right) \tag{29}$$

由于互信息是大于等于0的，所以

$$I(\boldsymbol{Y};\boldsymbol{Z})=0 \tag{30}$$

由式(28)和式(30)可以知道，不管窃听信道噪声多小，窃听方都无法获取到任何共享随机源互信息。证毕

所以

$$C_s=I\left(\tilde{\boldsymbol{Y}};\boldsymbol{Y}\right) \tag{31}$$

4 基于多随机信号流的密钥生成

基于多随机信号流的密钥生成方案分为4个阶段：生成共享随机源、共享随机源量化、密钥协商、隐私放大。

4.1 生成共享随机源

假设Bob发送足够长的导频信号给Alice，使Alice能够精准地估计到下行信道的信息。然后Alice在各天线上发送相互独立的复高斯随机信号给Bob。在这一步完成之后，Alice和Bob分别获得了式(5)和式(4)中的随机源。

4.2 共享随机源量化

通过确定量化门限将连续信号量化为离散信号。目前常用的量化方案有：均匀量化，等概率量化[16]，MMSE量化[17]等。为了能够使量化后的信息熵达到最大，一般采用等概率量化。先将变量值域划分为β个量化区间，使样本落入每个量化区间的概率相等。将相位和幅度分别进行量化。幅度的分布是瑞利分布，可以根据幅度的分布划分等概区间并进行量化。而相位的分布是均匀分布，因此可以直接将相位均匀划分为β个量化区间。Alice计算得

到量化门限信息发送给Bob，由于Eve无法确定自己观察到的连续信号的概率分布与Bob是否一致，因此无法利用Alice的量化信息进行等概率量化。

4.3 密钥协商

Alice与Bob密钥协商过程较为常用的是Cascade协议[18]。Alice利用双方约定好的纠错码随机选取一个码字$C(n)$(n为编码前信息序列)，然后将分组后保密序列q_A与其进行异或运算之后得到s发送出去(这里s经过信道编码之后发送出去，并且假设接收方能够无误地解码)。而Bob利用接收到的序列s与自己的序列q_B进行异或得到$C(n)\oplus e$ (e=$q_A\oplus q_B$)，进行译码纠错得到Alice随机选取的码字$C(n)$。然后Bob可以根据此码字$C(n)$和s进行异或运算即可得到协商后的序列。具体的方案可以采用低密度奇偶校验码(Low Density Parity Check code, LDPC)[19]或者极化码[20]来实现。本文采用低密度奇偶校验码进行协商实验。

4.4 隐私放大

由于窃听者观测到部分合法用户共享随机源信息，在协商过后，合法用户与窃听者间的比特不一致率(Bit Mismatch Ratio, BMR)会低于0.5，所以需要利用隐私放大来提升两者间的BMR，隐私放大一般用Hash函数来实现[21]。对于Hash函数的输入长度一般需要根据窃听方与合法用户之间的BMR来确定[20]，从而保证生成密钥的安全性。为了能够方便比较出不同方案不同发送总功率下隐私放大后的性能，需要设置相同的输入长度。Hash函数采用SHA256算法，按照输入长度隐私放大即可得到密钥。

5 仿真分析

为了能够验证理论值，可以使用文献[22]中提到的利用Copula熵估计1维随机变量间互信息的方法。为了能够估算条件互信息，定义式(32)

$$I(X_1;X_2;\cdots;X_k)\triangleq\int\cdots\int p(X_1,X_2,\cdots,X_k)\cdot\log_2\frac{p(X_1,X_2,\cdots,X_k)}{\prod_{i=1}^{k}p(X_i)}\mathrm{d}_{X_1}\mathrm{d}_{X_2}\cdots\mathrm{d}_{X_k}\quad(32)$$

可以利用式(33)将条件互信息做出以下变化

$$\begin{aligned}&I(X_1,X_2,\cdots,X_m;Y_1,Y_2,\cdots,Y_n|Z_1,Z_2,\cdots,Z_l)\\&=I(X_1;X_2;\cdots;X_m;Y_1;Y_2;\cdots;Y_n;Z_1;Z_2;\cdots;Z_l)\\&\quad-I(X_1;X_2;\cdots;X_m;Z_1;Z_2;\cdots;Z_l)\\&\quad-I(Y_1;Y_2;\cdots;Y_n;Z_1;Z_2;\cdots;Z_l)\\&\quad+I(Z_1;Z_2;\cdots;Z_l)\end{aligned}\quad(33)$$

接下来利用式(33)来对理论值进行仿真验证。

5.1 密钥安全性及可达密钥速率仿真

以下所有实验每个发送总功率点取10000组信道参数，每组信道参数取2000个采样点，假设每个采样点周期为T。假设在准静态块衰落的信道模型下，在密钥生成周期内信道参数不发生变化。信道参数服从均值为0，方差为1的复高斯分布。

首先针对在3.2小节中的安全性分析进行仿真，发送功率为20 dBm，接收方有2根天线，σ_b^2=1, σ_e^2=1。

可以看到图2中仿真验证了安全性分析：合法发送方天线数目越多，发送的随机信号流数目就越多，窃听者就越难以获取接收方天线上的叠加随机源，合法接收方与窃听者之间的互信息量就越少。这也就意味着，窃听者与合法接收方之间的互信息量可以随着发送随机信号流数目的增加逐渐减小甚至变为0。由于在实际仿真中无法设置发送天线数目为无穷大，为了方便分析，设置天线数目为64来对此进行验证。这里假设接收方和窃听方都是单天线，σ_b^2=1。从图3可知，σ_e^2=0.01和σ_e^2=0.001时，窃听者与合法接收者之间的互信息量都为0，所以窃听者不能够获取到共享随机源互信息的任何信息，这时合法用户可达密钥速率是等于共享随机源的互信息量的。

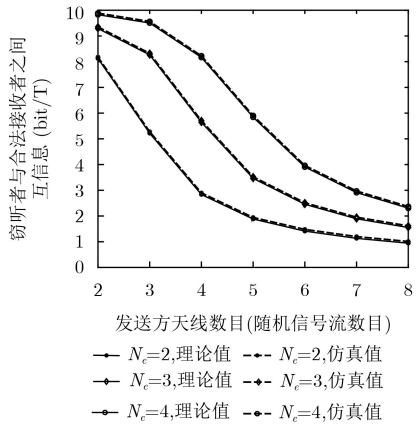

图 2 窃听方与合法方间互信息

然后分析可达密钥速率随发送天线的变化规律。设置发送功率为20 dBm, σ_b^2=1, σ_e^2=1, 图4设置合法接收方为2根天线，图5实验设置发送方5根天线，合法接收方2根天线并与文献[12]中的波束成形方案进行比较。

从图4中可知，本文所提多随机流方案优于波束成形方案。并且在发送方天线数目逐渐增加时，多随机流方案中可达密钥速率随窃听方天线数目增加而下降的幅度越来越小。因为在增加发送方天线数目的时候，多随机流方案发送的随机流数目也在

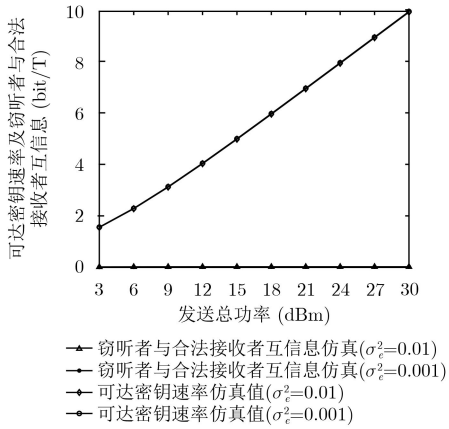

图 3 可达密钥速率及窃听者与合法方间互信息(N_a=64)

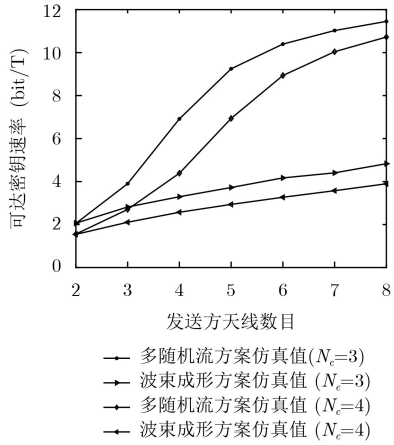

图 4 可达密钥速率随发送天线数目的变化

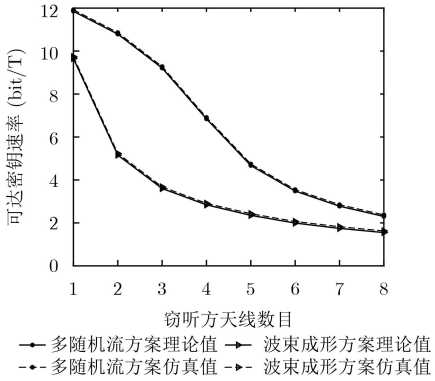

图 5 可达密钥速率随窃听方天线数目的变化

增加，窃听者也就更加难以正确估计合法接收方每根天线上的接收信号，所以窃听者能够窃取到的共享随机源信息也就越少(这点在图2中也可以看出)，而可达密钥速率也逐渐增加。从图5可看到窃听方天线数目增加时，两种方案的可达密钥速率都会下降，而多随机流方案依然是优于波束成形方案。因为在相同的窃听天线数目下，多随机流方案中的窃听方准确获取合法用户所有发送随机信号流的难度依然要大于波束成形方案。

下面分析可达密钥速率随发送总功率的变化规律。设置发送天线数目为3。这里假设接收方和窃听方都是单天线，σ_b^2=1, σ_e^2=1。

从图6可以看出，波束成形方案中，可达密钥速率会随着发送总功率的逐渐增加而趋近于平稳。而多随机流方案中可达密钥速率会随着发送总功率增加而增加。并且由于多随机流方案中共享随机源的互信息量与可达密钥速率大小较为接近，所以窃听者窃取到的密钥信息较少，窃听者获取到与合法方相同密钥的概率也会降低。所以可达密钥速率占据共享随机源互信息的比例越大，密钥也会越安全[15]。这一点也可以通过最终生成的密钥的BMR来进行验证。

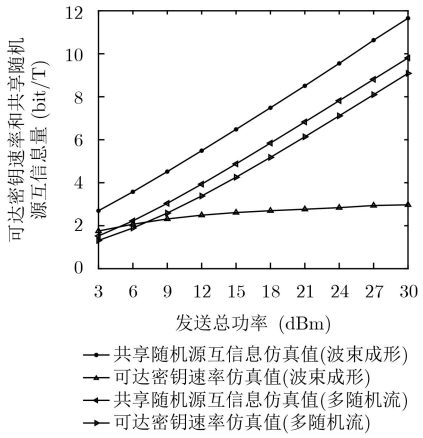

图 6 可达密钥速率和共享随机源互信息量随发送总功率的变化

下面通过进行量化、协商和隐私放大实验来比较两种方案的实际性能。

5.2 量化、协商及隐私放大仿真

(1) 量化：对图6中采取的样点实行4.2节量化算法进行1 bit量化。

(2) 协商：采用码长2000的低密度奇偶校验码[19](LDPC)进行协商仿真实验。

(3) 隐私放大：一般用Hash函数来实现。这里具体算法采用SHA256算法。

可以得到每个发送总功率点的平均量化BMR如图7、图8所示。

从图7中可知，两种方案的合法用户间BMR都会随着发送总功率逐渐降低；从图8中可知，多随机流方案中合法用户与窃听者间BMR随着发送总功率增加而降低的幅度更小。因为在发送总功率逐渐增加过程中，对于多随机流方案来说，窃听者能够观察到的信息增多，但与合法信号之间差异性也变大，所以合法用户与窃听者间的BMR稳定在0.5。

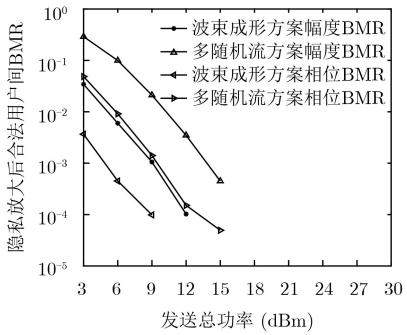

图 7 隐私放大后合法用户间BMR

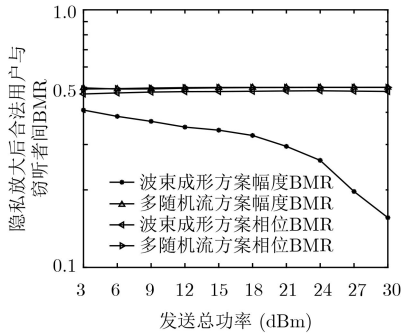

图 8 隐私放大后合法用户与窃听者BMR

6　结束语

本文针对基于随机信号流的密钥生成方案会因为窃听者的存在导致部分共享随机源信息泄露且可达密钥速率较低的问题，提出了一种基于多随机信号流的密钥生成方案。本文方案通过发送方发送多随机信号流，并将接收天线上的叠加随机源作为共享随机源，降低窃听者观察到的共享随机源互信息，从而提高可达密钥速率和密钥安全性。仿真结果表明本文方案能够有效提高可达密钥速率和密钥安全性，并且发送随机流数目越多，窃听者能够窃听到的共享随机源互信息越少，密钥安全性越高，如果发送随机流数目趋于无穷，窃听者窃取的信息会趋近于0。

参 考 文 献

[1] LIU Yiliang, CHEN H H, and WANG Liangmin. Physical layer security for next generation wireless networks: Theories, technologies, and challenges[J]. *IEEE Communications Surveys & Tutorials*, 2017, 19(1): 347–376. doi: 10.1109/COMST.2016.2598968.

[2] YANG Enhui and WU Xinwen. Information-theoretically secure key generation and management[C]. 2017 IEEE International Symposium on Information Theory, Aachen, Germany, 2017: 1529–1533. doi: 10.1109/ISIT.2017.8006785.

[3] MAURER U M. Secret key agreement by public discussion from common information[J]. *IEEE Transactions on Information Theory*, 1993, 39(3): 733–742. doi: 10.1109/18.256484.

[4] ZHU Xiaojun, XU Fengyuan, NOVAK E, *et al*. Using wireless link dynamics to extract a secret key in vehicular scenarios[J]. *IEEE Transactions on Mobile Computing*, 2017, 16(7): 2065–2078. doi: 10.1109/TMC.2016.2557784.

[5] HASSANA A A, STARKB W E, HERSHEYC J E, *et al*. Cryptographic key agreement for mobile radio[J]. *Digital Signal Processing*, 1996, 6(4): 207–212. doi: 10.1006/dspr.1996.0023.

[6] KITAURA A, SUMI T, TACHIBANA K, *et al*. A Scheme of private key agreement based on delay profiles in uwb systems[C]. 2006 IEEE Sarnoff Symposium, Princeton, USA, 2006: 1–6. doi: 10.1109/SARNOF.2006.4534731.

[7] MADISEH M G, NEVILLE S W, and MCGUIRE M L. Applying beamforming to address temporal correlation in wireless channel characterization-based secret key generation[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(4): 1278–1287. doi: 10.1109/TIFS.2012.2195176.

[8] HUANG Pengfei and WANG Xudong. Fast secret key generation in static wireless networks: A virtual channel approach[C]. 2013 Proceedings IEEE INFOCOM, Turin, Italy, 2013: 2292–2300. doi: 10.1109/INFCOM.2013.6567033.

[9] CHEN Dajiang, QIN Zhen, MAO Xufei, *et al*. SmokeGrenade: An efficient key generation protocol with artificial interference[J]. *IEEE Transactions on Information Forensics and Security*, 2013, 8(11): 1731–1745. doi: 10.1109/TIFS.2013.2278834.

[10] GOLLAKOTA S and KATABI D. Physical layer wireless security made fast and channel independent[C]. 2011 Proceedings IEEE INFOCOM, Shanghai, China, 2011: 1125–1133. doi: 10.1109/INFCOM.2011.5934889.

[11] LI Guyue, HU Aiqun, ZHANG Junqing, *et al*. Security analysis of a novel artificial randomness approach for fast key generation[C]. 2017 IEEE Global Communications Conference, Singapore, 2017: 1–6. doi: 10.1109/GLOCOM.2017.8254029.

[12] LOU Yangming, JIN Liang, ZHONG Zhou, *et al*. Secret key generation scheme based on MIMO received signal spaces[J]. *Scientia Sinica Informationis*, 2017, 47(3): 362–373. doi: 10.1360/N112016-00001.

[13] ZHANG Junqing, DUONG T Q, MARSHALL A, *et al*. Key generation from wireless channels: A review[J]. *IEEE Access*, 2016, 4: 614–626. doi: 10.1109/ACCESS.2016.2521718.

[14] COVER T and THOMAS J. Elements of information theory[M]. Boston: John Wiley &Sons, 2012: 33–34.

[15] PASOLINI G and DARDARI D. Secret key generation in

correlated multi-dimensional Gaussian channels[C]. 2014 IEEE International Conference on Communications, Sydney, Australia, 2014: 2171–2177. doi: 10.1109/ICC.2014.6883645.

[16] YE Chunxuan, REZNIK A, and SHAH Y. Extracting secrecy from jointly Gaussian random variables[C]. 2006 IEEE International Symposium on Information Theory, Seattle, USA, 2006: 2593–2597. doi: 10.1109/ISIT.2006.262101.

[17] ROE G. Quantizing for minimum distortion (Corresp.)[J]. *IEEE Transactions on Information Theory*, 1964, 10(4): 384–385. doi: 10.1109/TIT.1964.1053693.

[18] ZHAN Furui, YAO Nianmin, GAO Zhenguo, *et al*. Efficient key generation leveraging wireless channel reciprocity for MANETs[J]. *Journal of Network and Computer Applications*, 2018, 103: 18–28. doi: 10.1016/j.jnca.2017.11.014.

[19] WONG C W, WONG T F, and SHEA J M. Secret-Sharing LDPC codes for the BPSK-constrained Gaussian wiretap channel[J]. *IEEE Transactions on Information Forensics and Security*, 2011, 6(3): 551–564. doi: 10.1109/TIFS.2011.2139208.

[20] ZHANG Shengjun, JIN Liang, LOU Yangming, *et al*. Secret key generation based on two-way randomness for TDD-SISO system[J]. *China Communications*, 2018, 15(7): 202–216. doi: 10.1109/CC.2018.8424614.

[21] BENNETT C H, BRASSARD G, CREPEAU C, *et al*. Generalized privacy amplification[J]. *IEEE Transactions on Information Theory*, 1995, 41(6): 1915–1923. doi: 10.1109/18.476316.

[22] ZENG X and DURRANI T S. Estimation of mutual information using copula density function[J]. *Electronics Letters*, 2011, 47(8): 493–494. doi: 10.1049/el.2011.0778.

金 梁：男，1969年生，教授，博士生导师，研究方向为移动通信技术、阵列信号处理、物理层安全.

蔡奥林：男，1993年生，硕士，研究方向为移动通信、物理层安全.

黄开枝：女，1973年生，教授，博士生导师，研究方向为宽带移动通信与异构无线网络安全、无线物理层安全.

钟 州：男，1982年生，讲师，研究方向为移动通信、物理层安全.

楼洋明：男，1991年生，助理研究员，硕士，研究方向为信息论、物理层安全.