5G毫米波通信中的物理层安全预编码

Physical Layer Secure Precoding in 5G Millimeter Wave Communication Systems

摘要：安全预编码是一种信号处理技术，即发送端根据信道状态信息设计预编码矩阵，从而对信号进行预处理。该技术旨在保证合法用户通信质量的前提下，恶化窃听信道，在信息理论意义上实现无线通信系统的安全传输。认为物理层安全技术与移动通信的发展密不可分，利用毫米波信道稀疏特性开发物理层安全预编码技术，有望实现5G通信与安全一体化发展。从长期角度为网络优化部署提供指导，提升网络流量水平，释放流量增长潜力。

关键词：5G；毫米波；物理层；安全通信；预编码

Abstract: Secure precoding is a signal processing technique. Precoding matrix is designed at the transmitter to pre-process signal based on channel state information, aiming to ensure the communication quality for legitimate users and worsen the eavesdroppers' channels. Secure transmission of wireless communication systems is realized in the sense of information theory. The physical layer security technology is inseparable from the development of mobile communication. By developing physical layer security precoding technology with millimeter-wave channel sparse characteristics, it is expected to realize the integrated development of 5G communication and security.

Keywords: 5G; millimeter wave; physical layer; secure communications; precoding

倪云云/NI Yunyun[1]
陈伯庆/CHEN Boqing[1]
李刚/LI Gang[2]
（1.南京邮电大学，中国 南京 210003；
2.中兴通讯股份有限公司，中国 深圳 518057）
(1. Nanjing University of Posts and Telecommunications, Nanjing 210003, China;
2. ZTE Corporation, Shenzhen 518057, China)

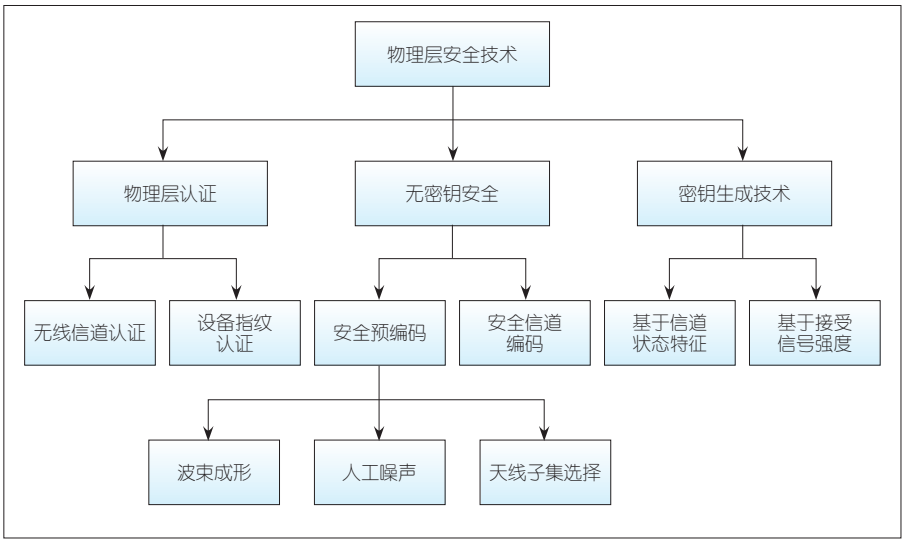
DOI：10.12142/ZTETJ.202104011
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.tn.20210727.1526.005.html
网络出版日期：2021-07-27
收稿日期：2020-09-06

2019年6月6日，中国正式进入了5G商用阶段。5G通信系统采用了大规模多输入多输出（Massive MIMO）、毫米波、非正交多址接入（NOMA）等关键技术[1]，将以超过千兆的比特率以及低于1 ms的延迟，满足大容量、高速率、低延迟的通信需求。5G关键技术的发展不断提升合法用户的性能，但同时这些技术也可能会被窃听者恶意利用，从而影响通信安全。5G通信中，不同场景下的用户对于通信质量的需求各异，例如海量机器类通信（mMTC）、增强移动宽带（eMBB）等场景下的用户对无线业务的需求大相径庭。我们需要针对不同场景下的用户需求，并结合5G新技术和独特的无线信道特性，研究相适的安全通信策略，以满足5G通信中多场景、多等级的弹性安全需求。

相比于传统安全机制，物理层安全（PLS）技术充分利用无线信道的时变性和多样性，以及合法通信双方信道的唯一性和互易性等内生安全特性[2]，保障比特流的安全传输，使比特流不依赖于传统的密钥便有望实现香农于1949年在《保密系统的通信理论》中提出的基于信息论意义上的“完美安全”[3]。传统安全技术主要在上层实施，如数据链路层的认证机制和应用层的加密机制。PLS技术作为上层安全的有力补充，与传统安全机制相辅相成，极大地增强整个通信系统的安全性能。

如图1所示，PLS分为物理层认证、无密钥安全技术和密钥生成技术。物理层认证技术利用无线信道特性区分合法用户和窃听用户，防范入侵者的假冒攻击。无密钥安全技术基于A.D.WYNER提出的窃听信道模型[4]，在已知的信道状态信息（CSI）指导下设计安全预编码矩阵和安全信道编码方案，以实现无密钥安全。安全预编码方案利用CSI设计预编码矩阵，以最大化保密容量为目标设计优化问题并求最优解，实现合法用户的安全通信。安全预编码方案包括波束成形、人工噪声以及天线子集选

基金项目：中兴通讯产学研合作项目（2019ZTE01-02-16）；江苏省高等学校自然科学研究项目（19KJB510048）；江苏省研究生科研创新计划（KY-CX17_0781）



▲图1 物理层安全技术框架图

择等。波束成形是通过设计预编码矩阵调节发射天线阵列或其子阵列，将发送信号的能量集中到合法用户方向，以提高合法用户的信道条件，从而增强接收信号质量。人工噪声利用无线信道以及噪声内在的随机性，使得合法用户的信道质量优于窃听者信道，以保证合法用户的信噪比高于窃听者，从而达到安全传输的目的。天线子集选择在保证合法用户正常接收信号的同时，扰乱窃听者星座图，使窃听者无法准确解调信号。而物理层密钥生成技术利用无线传输信道的互易性和唯一性，并根据通信双方随机变化的无线信道生成安全可靠的密钥。物理层安全不需要特定的硬件系统，与上层结构相互独立，易应用于现有的通信系统。物理层安全可以在5G及未来的无线通信领域发挥更大的作用。

1 5G毫米波无线信道特征分析

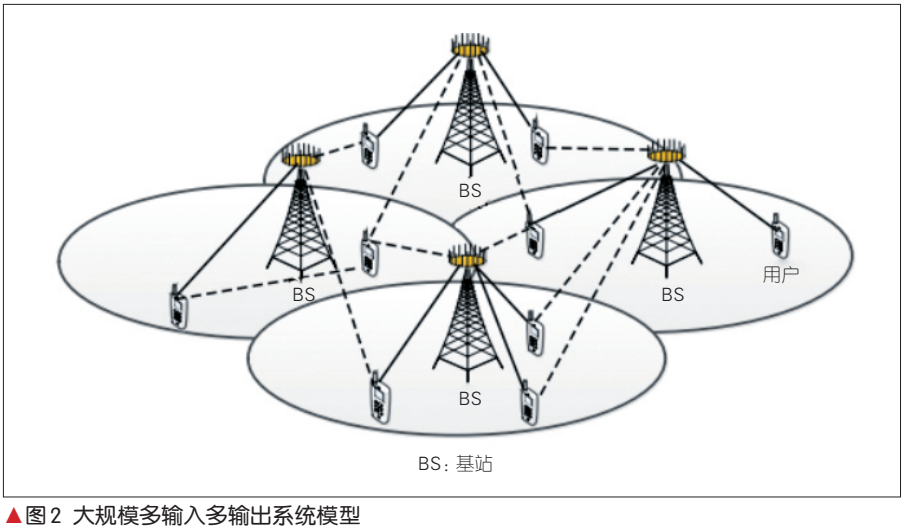
1.1 毫米波频段Massive MIMO信道分析

为了实现最高20 Gbit/s的网速，5G要将带宽提高到1 GHz以上。目前，6 GHz以下已经没有足够的频段了，因此5G使用了毫米波技术。毫米波频段高、频谱资源丰富，具有更高的信道容量。5G通信将在毫米波频段获得较高的通信带宽，并采用基于大规模有源阵列天线的Massive MIMO技术来大幅提升接入网性能。毫米波通信在链路的收发端使用Massive MIMO，所具有的信道容量将远远超越香农公式中基于单输入单输出（SISO）系统所给出的信道容量限制。在Massive MIMO系统中引入波束成形技术，将波束集中到指定位置，不仅可以提高能量效率，还可以减少不同用户之间通信的互相干扰，允许单一基站（BS）接入海量的设备，提升基站容量，实现“万物互联”。

在传统的MIMO系统中，我们通常假设信道为瑞利衰落信道，并使用最小二乘法等进行信道估计，发射导频序列的长度随着MIMO信道矩阵的维度增加而增加。图2的Massive MIMO系统模型实现了水平面的波束成形，还能够利用更多的振子和信道实现垂直面的波束成形。毫米波Massive MIMO系统的信道估计，对计算能力要求更高。这使得导频开销增加，带宽占用更多，系统吞吐量下降。不同于传统的MIMO系统，毫米波Massive MIMO系统可以采用混合波束架构对信道数据进行检测，一条射频链路对应多根天线[5]。大量的毫米波信道测量表明，毫米波信道具有空间域稀疏的特性。利用空时傅里叶变换，毫米波Massive MIMO信道的稀疏性可以在波束域上得以体现。基于毫米波Massive MIMO信道的稀疏性，利用压缩感知等技术可以有效地进行信道估计，并降低导频开销。

1.2 毫米波频段的信道稀疏性分析

毫米波通信频段高、波长短，巨大的路径损耗导致其呈现稀疏散射



▲图2 大规模多输入多输出系统模型

特性。Massive MIMO技术的使用，使得信道矩阵维度增大，因此传统的瑞利信道模型并不适合毫米波信道建模。为此，研究人员提出了针对毫米波无线通信的信道模型——分簇射线（Cluster-Ray）模型[6]。

在毫米波通信中，我们利用分簇射线模型来描述毫米波信道：信道被表示为多个分簇，入射角相似的路径归为同一簇，毫米波信道包括视距（LOS）路径和分簇中的非视距（NLOS）路径。毫米波稀疏性信道如图3所示。

毫米波的高路径损耗导致其信道呈稀疏性，物理信道由到达角（AOA）与离开角（AOD）决定，而MIMO信道矩阵$\boldsymbol{H}$本身并不呈稀疏性。可将MIMO信道矩阵$\boldsymbol{H}$用均匀分布的虚拟AOA和AOD线性来表示：

$$\boldsymbol{H}=\frac{1}{\sqrt{N_r N_t}}\sum_{i=1}^{N_r}\sum_{k=1}^{N_t}\boldsymbol{H}_b(i,k)\boldsymbol{a}_r(i\Delta\varphi_r)\boldsymbol{a}_t^H(k\Delta\varphi_t)=\boldsymbol{U}_r\boldsymbol{H}_b\boldsymbol{U}_t^H, \quad (1)$$

即：

$$\boldsymbol{H}_b=\boldsymbol{U}_r^H\boldsymbol{H}\boldsymbol{U}_t, \quad (2)$$

其中，$\boldsymbol{U}_r$和$\boldsymbol{U}_t$是离散傅里叶变换酉矩阵，它们的列是正交的阵列响应矢量：

$$\boldsymbol{U}_r[:,i]=\frac{1}{\sqrt{N_r}}[\boldsymbol{a}_r(i\Delta\varphi_r)] \quad i\in I(N_r)$$

$$\boldsymbol{U}_t[:,i]=\frac{1}{\sqrt{N_t}}[\boldsymbol{a}_t(i\Delta\varphi_t)] \quad i\in I(N_t)$$

$$I(n)=\{1,2,\cdots,n\}。 \quad (3)$$

相邻虚拟AoD或者AoA的角度间隔分别由基站和移动台的阵列分辨率决定：

$$\Delta\varphi_t=1/N_t$$
$$\Delta\varphi_r=1/N_r。 \quad (4)$$

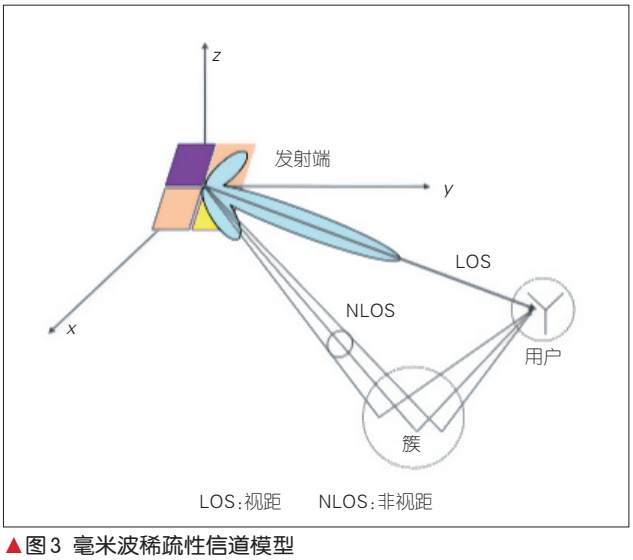
波束空间信道矩阵$\boldsymbol{H}_b$是天线域信道矩阵$\boldsymbol{H}$的酉等价表示，即$\boldsymbol{H}_b$是信道$\boldsymbol{H}$在傅里叶正交集上的投影。经过转换之后可以发现，$\boldsymbol{H}_b$中只有个别元素的值较大，这些元素包含了信道的大部分功率，所以波束空间矩阵$\boldsymbol{H}_b$呈现出明显的稀疏特性。

在毫米波Massive MIMO系统中，基于毫米波信道在角度域上的稀疏性，可利用压缩感知技术进行信道估计，以降低导频开销。

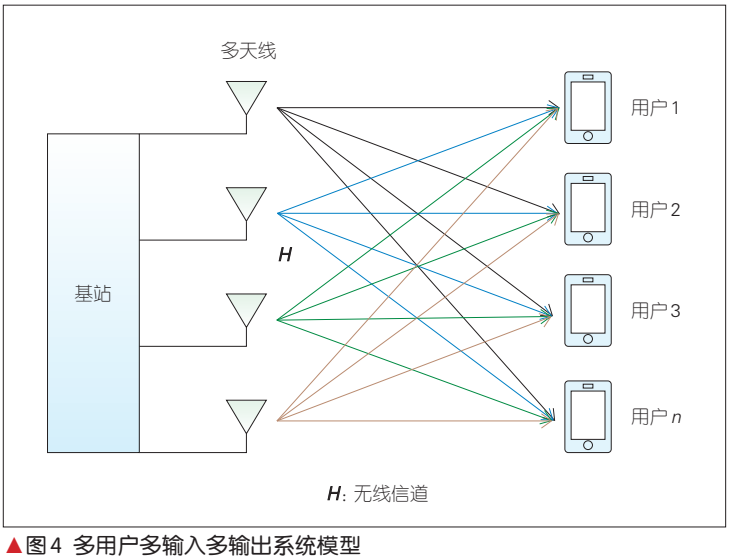
1.3 多用户毫米波MIMO预编码

在多用户MIMO系统中，利用空分复用接入（SDMA）技术可以使系统获取更高的信道容量。毫米波多用户MIMO系统可以在相同的时频资源上与多个用户同时通信，并且发送多个数据流，极大地提升了系统的总频谱效率，而且可以通过高波束成形增益提高传输的可靠性。毫米波多用户MIMO系统通常只需在发射端配置Massive MIMO阵列，因此接收端用户采用传统MIMO多天线即可。这不仅可以充分利用空间资源，提升系统容量，还可以有效地降低成本和复杂度。

图4为多用户MIMO系统模型。MIMO系统能够充分利用空间自由度，基站端有多根天线用于信号传输，却不要求接收端有多天线。发送端发射信号后经过预编码矩阵处理，将信号发送给接收端，接收端进行信号解调并获取有效信息。多用户MIMO系统中的预编码方案可以按照干扰信号处理的方式分为基于干扰抑制和基于干扰抵消的预编码方案。通过发射端的预编码处理，可以有效地消除多用户间的干扰，提升系统保密容量；还可以减少接收端的解调难度，解决移动端的功耗和体积问题。



▲图3 毫米波稀疏性信道模型



▲图4 多用户多输入多输出系统模型

2 毫米波安全预编码

2.1 经典窃听信道模型

1975年，A.D.WYNER提出了窃听信道模型。在该模型中，假设窃听信道为退化的合法信道，从而保证非负的保密能力。在合法信道质量优于窃听信道时，总存在一种编码方式，使得合法接收端在正确解调的情况下，实现信息的安全传输[7]；而当窃听信道质量优于合法信道时，则需要引入人工噪声技术，恶化窃听信道质量，保证数据安全传输。

图5为多输入多输出多天线窃听（MIMOME）信道模型[4]，合法发送方Alice端配置N_t根天线，合法接受者Bob配置N_r根天线，窃听者Eve配置N_e根天线。Alice需要发送保密信息x给Bob，因此Bob和Eve的接收信号分别为：

$$\begin{aligned} \boldsymbol{y}_b &= \boldsymbol{H}\boldsymbol{x} + \boldsymbol{n}_b \\ \boldsymbol{y}_e &= \boldsymbol{G}\boldsymbol{x} + \boldsymbol{n}_e \end{aligned} \quad 。 \tag{5}$$

$\boldsymbol{H} \in \mathbb{C}^{N_r \times N_t}$表示Alice到Bob间的合法信道矩阵，$\boldsymbol{G} \in \mathbb{C}^{N_e \times N_t}$表示Alice到Eve之间的窃听信道矩阵。$\boldsymbol{x} \in \mathbb{C}^{N_t \times 1}$表示Alice发送的信号，其中协方差矩阵为$E\{\boldsymbol{x}\boldsymbol{x}^H\} = \boldsymbol{Q}_x$，$Tr(\boldsymbol{Q}_x) \leqslant P_t$，$P_t$是总发送功率；$\boldsymbol{n}_b \in \mathbb{C}^{N_r \times 1}$和$\boldsymbol{n}_e \in \mathbb{C}^{N_e \times 1}$分别表示Bob和Eve的零均值加性复高斯噪声向量，协方差矩阵分别是$\sigma_b^2\boldsymbol{I}$和$\sigma_e^2\boldsymbol{I}$。

假设Alice已知信道矩阵$\boldsymbol{HG}$的理想CSI，并且存在$\sigma_b^2 = \sigma_e^2 = 1$。根据香农公式，出合法信道与窃听信道的信道容量可以表示为：

$$\begin{aligned} C_b &= \log_2 \det(\boldsymbol{I} + \boldsymbol{H}\boldsymbol{Q}_x\boldsymbol{H}^H)_{N_r \leqslant N_t} \\ C_e &= \log_2 \det(\boldsymbol{I} + \boldsymbol{G}\boldsymbol{Q}_x\boldsymbol{G}^H)_{N_r \leqslant N_t} \end{aligned} \quad 。 \tag{6}$$

系统的保密容量可以用主信道的信道容量减去窃听信道的信道容量来实现，为了保密容量的非负性，则有：

$$C_s = \begin{cases} C_b - C_e, & C_b > C_e \\ 0, & C_b \leqslant C_e \end{cases} 。 \tag{7}$$

MIMOME窃听信道的保密容量可以表示为：

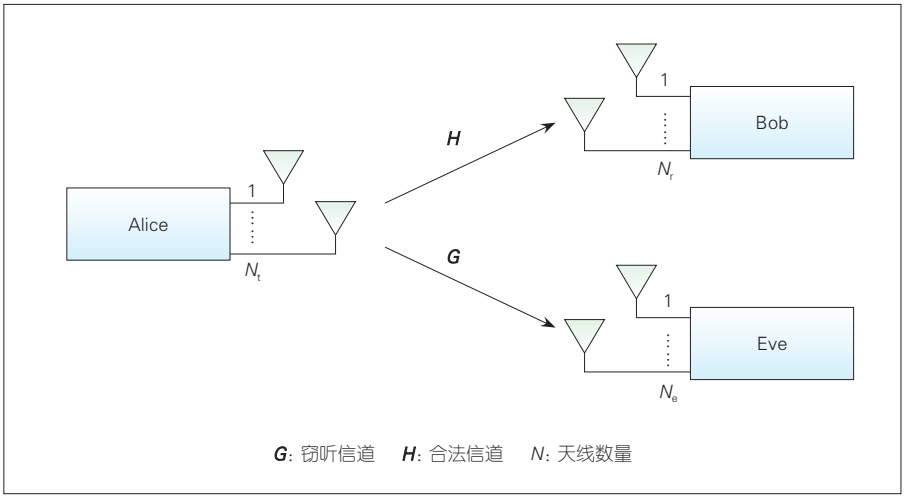
$$C_s(P_t) = \max_{\boldsymbol{Q}_x \geqslant 0, Tr(\boldsymbol{Q}_x) \leqslant P_t} \log_2(\det(\boldsymbol{I} + \boldsymbol{H}\boldsymbol{Q}_x\boldsymbol{H}^H)) - \log_2(\det(\boldsymbol{I} + \boldsymbol{G}\boldsymbol{Q}_x\boldsymbol{G}^H)) 。 \tag{8}$$

2.2 数模混合预编码

无线通信中的安全问题可以转化为通信资源的分配和挖掘问题，安全能力的增强来自于通信能力的提升和通信资源的有效利用。为了挖掘空间自由度，并且能更有效地利用发送端能量，移动通信采用MIMO系统来提高物理层链路性能。5G通信中Massive MIMO技术带来的天线阵列增益可以弥补毫米波传输过程中的高路径损耗。

传统的MIMO系统通常采用数字预编码方案，在基带使用预编码矩阵对信号进行预处理。这要求每根天线单元有单独的射频（RF）链路，包括放大器、滤波器和模数转换器（ADC）/数模转换器（DAC）等器件，为系统带来空间复用及分集增益。在数字预编码方案中，信号的幅度和相位可以灵活设置，从而提升通信效率。但在Massive MIMO系统中，使用全数字预编码方案会产生高昂的硬件成本和功耗，因此在5G通信中的预编码方案设计里，我们一般不考虑采用全数字预编码方案。模拟预编码技术指使用预编码矩阵在RF端改变信号的相位，并通过低成本、低功耗的移相器完成相位的控制，因此从经济效益的角度考虑，模拟预编码方案更受欢迎。但由于缺乏对幅度的控制，模拟预编码的性能比数字预编码差。为了在获得天线增益的同时减少成本支出，可通过少量的射频链连接基带预编码与射频预编码，采用数模混合架构进行无线信道的数据发射与检测[8]。

图6为典型的毫米波混合通信系统模型，系统中有N_s个数据流，发送端与接收端配备了N_t、N_r根天线。发送端数据经基带数字预编码$\boldsymbol{F}_{\mathrm{BB}}$进行预处理后，通过$N_t^{\mathrm{RF}}$个射频链路转换至射频端。RF链路满足$N_s \leqslant N_t^{\mathrm{RF}} \leqslant N_t$，每个RF链路通过$N_t$个移相器连接至天线，并通过移相器对信号进行模拟预编码。在此硬件架构下，发送端采用$N_t^{\mathrm{RF}} \times N_s$的基带预编码矩阵



▲图5 窃听信道模型

$\boldsymbol{F}_{\mathrm{BB}}$和$N_t \times N_t^{\mathrm{RF}}$的RF预编码矩阵$\boldsymbol{F}_{\mathrm{RF}}$。RF预编码矩阵$\boldsymbol{F}_{\mathrm{RF}}$的元素幅度相同，系统总发射功率通过$\boldsymbol{F}_{\mathrm{BB}}$进行限制，使得$\| \boldsymbol{F}_{\mathrm{RF}}\boldsymbol{F}_{\mathrm{BB}}\|_F^2 = N_s$。

考虑一个窄带慢衰落传播信道，则接收端信号为：

$$\boldsymbol{y} = \sqrt{\rho}\,\boldsymbol{H}\boldsymbol{F}_{\mathrm{RF}}\boldsymbol{F}_{\mathrm{BB}}\boldsymbol{s} + \boldsymbol{n}。 \tag{9}$$

$\boldsymbol{H}$为$N_r \times N_t$的信道矩阵，ρ代表平均接收功率，经接收端处理过后的信号可表示为：

$$\tilde{\boldsymbol{y}} = \sqrt{\rho}\,\boldsymbol{W}_{\mathrm{BB}}^H\boldsymbol{W}_{\mathrm{PF}}^H\boldsymbol{H}\boldsymbol{F}_{\mathrm{PF}}\boldsymbol{F}_{\mathrm{BB}}\boldsymbol{s} + \boldsymbol{W}_{\mathrm{BB}}^H\boldsymbol{W}_{\mathrm{PF}}^H\boldsymbol{n}, \tag{10}$$

其中，$\boldsymbol{W}_{\mathrm{RF}}$是大小为$N_r \times N_r^{\mathrm{RF}}$的射频组合矩阵，$\boldsymbol{W}_{\mathrm{BB}}$是大小为$N_r^{\mathrm{RF}} \times N_s$的基带组合矩阵。与射频预编码矩阵相同，$\boldsymbol{W}_{\mathrm{RF}}$通过移相器实现并且元素幅度相同。假设传输的符号为高斯符号，系统的频谱效率为[9]：

$$R = \log_2\left(\left|\boldsymbol{I}_{N_1} + \frac{\rho}{N_s}\boldsymbol{R}_n^{-1}\boldsymbol{W}_{\mathrm{BB}}^H\boldsymbol{W}_{\mathrm{RF}}^H\boldsymbol{H}\boldsymbol{F}_{\mathrm{RF}}\boldsymbol{F}_{\mathrm{BB}} \times \boldsymbol{F}_{\mathrm{BB}}^H\boldsymbol{F}_{\mathrm{RF}}^H\boldsymbol{H}^H\boldsymbol{W}_{\mathrm{RF}}\boldsymbol{W}_{\mathrm{BB}}\right|\right), \tag{11}$$

其中，$\boldsymbol{R}_n$是经过组合器后的噪声协方差。

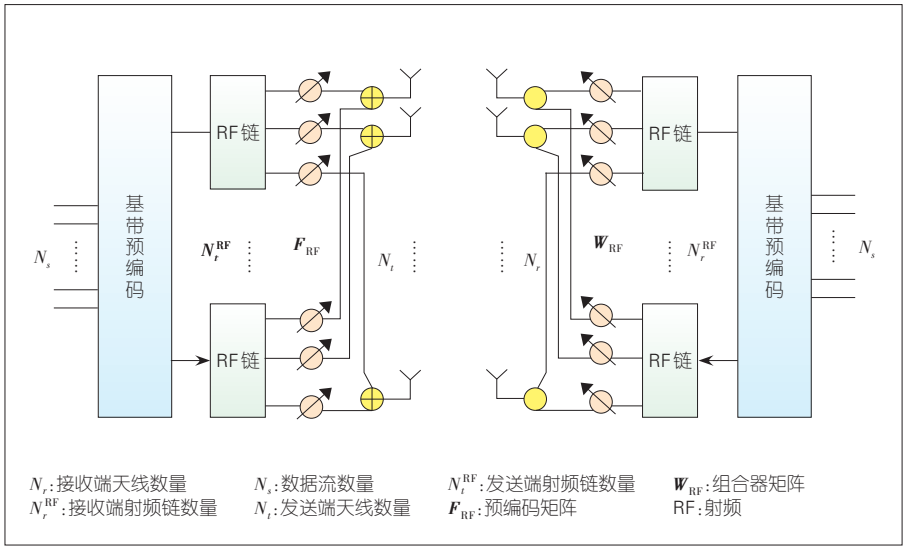
2.3 波束成形

波束成形是一种经典的多天线技术，通过调整发送天线权重系数，使天线主瓣对准合法接收用户，从而减少信号泄露。波束成形提高合法用户的信噪比，并降低潜在窃听者的信噪比，提升系统安全容量。

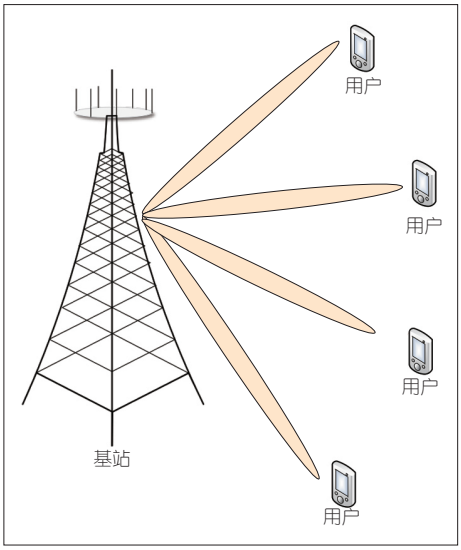
图7为Massive MIMO系统。Massive MIMO系统中的天线阵列为实现定向波束而部署，它可以利用波阵面相干叠加原理在指定方向增强波束，在其他位置削弱波束强度，从而增加信道容量。

文献[10]研究了毫米波MIMOME系统的数模混合预编码，在已知窃听者CSI的情况下，提出模拟预编码器和组合器的联合设计以防止信息泄露，并基于等效基带信道计算数字预编码器和组合器以最大化安全速率。文献[11]提出，在毫米波MISO系统中，可以使用离散角域信道模型来分析信道路径，以获得目标用户和窃听者间公共信道路径数目的概率分布函数，推导出最大比传输（MRT）连接概率的闭合表达式，并分析主动和被动窃听者场景下的保密中断概率。在MISOSE系统中，文献[12]提出，使用相控阵传输结构，并利用复平面中的多边构造解决星座合成问题，以符号速率改变传输权重向量，从而在接收端获得预期的相位，并在窃听者处产生随机性。额外的随机相位旋转添加至发送权重向量中，在不显著降低接收端符号检测的可靠性的前提下，给窃听者造成干扰。同样，在MISOSE系统中，文献[13]创建了由传统相控阵和可编程功率放大器组成的可编程加权相控阵（PWPA）结构，在此基础上提出反置天线子空间传输技术和优化加权天线子空间传输技术，利用天线阵列的幅值权重扰乱非预期方向的星座图，并在非预期方向产生人工噪声。PWPA增加了攻击者向量估计的难度，从而提升系统的安全性能。

在随机几何架构中的毫米波/微波异构网中，文献[14]基于随机阻塞模型和固定视距模型，分析节点位置和阻塞模型的不确定性，描述保密中断概率和条件链接概率，推导出LOS和NLOS下的条件保密中断概率的上下限，利用阻塞提升系统保密性能。在窃听者随机分布的场景中，文献[15]结合毫米波信道特性，推导随机



▲图6 毫米波通信系统模型



▲图7 大规模多输入多输出系统

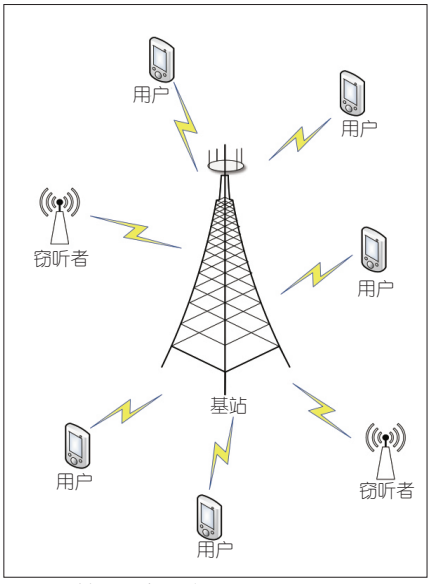
阻塞和保密中断概率的闭合表达式，并分析不同参数对保密性能的影响。

合理的波束成形方案可将主波束对准合法用户，提高了信噪比，优化了数据传输速率。同时，还可以限制窃听者的接收信号功率，弱化其窃听能力。但是，波束成形方案需要知道窃听信道状态信息或者其他反馈信息，这在现实中往往很难实现。

2.4 人工噪声

人工噪声技术指基站端在传输信号的同时牺牲一部分发送功率，生成额外的干扰信号。将人工噪声对准合法信道的零空间，该干扰信号仅作用于窃听者，从而可以降低窃听者的信噪比，恶化窃听信道质量，同时不会影响合法用户间的通信。

图8为5G通信中的单基站多用户模型。在单基站多用户通信过程中，基站端与合法用户间进行正常的信号传输。基站端可以分出部分功率，向窃听者发射人工噪声干扰信号。利用CSI设计人工噪声矩阵，并将其投影到合法用户的零空间，可以干扰窃听信道条件，降低窃听者信噪比，从而使得保密容量非负，减少信号泄露。



▲图8 单基站多用户模型

文献[11]研究了MISO毫米波系统的物理层安全，用空间可分解路径来表示离散角信道模型，并推导出人工噪声方法连接概率的闭合表达式。在保密中断概率的约束下，最大化保密吞吐量，并获得人工噪声与信号间的功率分配参数。文献[16]研究毫米波车联网通信，通过混合波束成形将信号发送给接收方，向目标方向发射人工噪声。相比于传统向所有非预期方向发射人工噪声的方法，该方案可以避免向非窃听方向发送噪声。

在毫米波MIMOSE系统中，在窃听者CSI未知的情况下，文献[17]研究基于人工噪声的混合波束成形方案。该方案可在中断窃听者接收信息的同时，将接收端的服务质量维持在预期水平。

文献[18]研究了毫米波系统慢衰落信道的安全传输，并在假设发送端已知部分窃听CSI的情况下，提出了基于合法用户和窃听者路径方向的人工噪声传输策略。通过开关传输方案，并在保密速率的约束下，最小化保密中断概率，同时推导了传输信号与人工噪声间最优功率分配的闭合表达式。

基于人工噪声的安全传输技术，并通过生成干扰信号来扰乱窃听信道，可使得合法用户信道质量优于窃听信道质量，从而实现物理层安全通信。人工噪声技术适用于频分双工（FDD）和时分双工（TDD）系统，其方案设计需要了解精确的合法户CSI，从而消除对合法用户的干扰。若人工噪声方案设计不当，可能会降低合法接收端的性能，甚至导致接收信号峰均比增大。

2.5 天线子集选择

天线子集选择是在保证合法用户正确解调信号的前提下，扰乱窃听者星座图，使其接收信号的幅度相位发生随机旋转并产生畸变，无法正确解调信号，从而降低接收信号的信噪比。

文献[19]提出，如果发送端能获得合法接收端和窃听者的CSI，则可以选择安全容量最大的一根天线来传输信号；如果仅知道合法接收端的CSI，则可以选择使合法信道容量最大的天线来传输信号。文献[20]提出一种基于点对点通信系统的低复杂度定向调制技术。通过驱动阵列中的一部分天线以符号速率调制辐射方向图，在所需方向上投射出清晰的星座图，并在其他方向上生成随机星座图。文中，我们给出两种天线选择算法：随机天线子集选择与模拟退火天线子集选择。随机天线子集选择不会影响合法用户方向接收器的符号解调，但会随机化旁瓣方向窃听者的接收信号幅度和相位。而基于模拟退火的天线子集选择优化算法，可以克服随机天线子集选择中旁瓣较大的问题，减少能量泄漏。文献[16]提出一种用于车联网毫米波通信系统的物理层安全方案。在单射频链路天线阵系统中，该方案能够随机选择天线子集进行模拟预编码。同时，该方案可以将信息符号发送到目标接收器，剩余的所有天线向非目标方向发送噪声。系统中没有闲置天线，窃听者无法消除旁瓣失真。

天线子集选择通过控制天线的开-关来扰乱窃听者星座图，但对合法用户并没有影响。此方案需要以符号速率控制开关，实现困难。

3 结束语

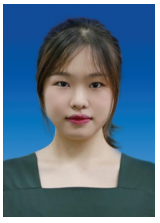
传统基于密码学的加密机制已经无法满足5G通信时代下日益增长的安全需求。PLS技术采用信号处理

和编码技术来增强5G移动通信系统的保密性，而不依赖于密钥的计算复杂度。安全预编码技术利用无线信道的内生安全属性，实现基于用户位置的安全传输。利用波束成形、人工降噪和天线子集选择等安全预编码方案，能够拉大合法用户与窃听者的信道容量差距，从而提高5G移动通信系统的保密性能。PLS技术与移动通信的发展密不可分，利用毫米波信道稀疏特性开发物理层安全预编码技术，有望实现5G通信与安全一体化发展。

参考文献

[1] POPOVSKI P, TRILLINGSGAARD K F, SIMEONE O, et al. 5G wireless network slicing for eMBB, URLLC, and mMTC: a communication–theoretic view [J]. IEEE access, 2018, (6): 55765–55779. DOI: 10.1109/ACCESS.2018.2872781
[2] BLOCH M, BARROS J. Physical–layer security: from information theory to security engineering [M]. Cambridge, British: Cambridge University Press, 2011
[3] SHANNON C E. Communication theory of secrecy systems [J]. Bell system technical journal, 1949, 28(4): 656–715. DOI: 10.1002/j.1538–7305.1949.tb00928.x
[4] WYNER A D. The wire–tap channel [J]. Bell system technical journal, 1975, 54(8): 1355–1387. DOI: 10.1002/j. 1538–7305.1975.tb02040.x
[5] BOGALE T E, LE L B. Massive MIMO and mmWave for 5G wireless HetNet: Potential benefits and challenges [J]. IEEE vehicular technology magazine, 2016, 11(1): 64–75. DOI:10.1109/MVT.2015.2496240
[6] AYACH O E, RAJAGOPAL S, ABU–SURRA S, et al. Spatially sparse precoding in millimeter wave MIMO systems [EB/OL]. [2021–06–05]. https://arxiv.org/abs/1305.2460
[7] CSISZAR I, KORNER. Broadcast channels with confidential messages [J]. IEEE transactions on information theory, 1978, 24(3):339–348. DOI: 10.1109/TIT.1978.1055892
[8] KIM C, SON J, KIM T, et al. On the hybrid beamforming with shared array antenna for mmWave MIMO–OFDM systems [C]//2014 IEEE Wireless Communications and Networking Conference (WCNC). Istanbul, Turkey: IEEE, 2014: 335–340. DOI: 10.1109/WCNC.2014.6951990
[9] ALKHATEEB A, AYACH OEL, LEUS G, et al. Channel estimation and hybrid precoding for millimeter wave cellular systems [J]. IEEE journal of selected topics in signal processing, 2014, 8(5): 831–846. DOI: 10.1109/jstsp.2014.2334278
[10] TIAN X W, LI M, WANG Z H, et al. Hybrid precoder and combiner design for secure transmission in mmWave MIMO systems [C]//GLOBECOM 2017 – 2017 IEEE Global Communications Conference. Singapore, Singapore: IEEE, 2017: 1–6. DOI: 10.1109/GLOCOM.2017.8254019
[11] JU Y, WANG H M, ZHENG T X, et al. Safeguarding millimeter wave communications against randomly located eavesdroppers [J]. IEEE transactions on wireless communications, 2018, 17(4): 2675–2689. DOI:10.1109/twc.2018.2800747
[12] ZHANG X J, XIA X G, HE Z S, et al. Phased–array transmission for secure mmWave wireless communication via polygon construction [J]. IEEE transactions on signal processing, 2020, 68: 327–342. DOI: 10.1109/TSP.2019.2944751
[13] HONG Y Q, JING X J, GAO H. Programmable weight phased–array transmission for secure millimeter–wave wireless communications [J]. IEEE journal of selected topics in signal processing, 2018, 12(2): 399–413. DOI:10.1109/JSTSP.2018.2822048
[14] VUPPALA S, BISWAS S, RATNARAJAH T. An analysis on secure communication in millimeter/micro–wave hybrid networks [J]. IEEE transactions on communications, 2016, 64(8): 3507–3519. DOI:10.1109/TCOMM.2016.2587287
[15] YANG W W, TAO L W, SUN X L, et al. Secure on–off transmission in mmWave systems with randomly distributed eavesdroppers [J]. IEEE access, 2019, (7): 32681–32692. DOI:10.1109/ACCESS.2019.2898180
[16] ELTAYEB M E, CHOI J, AL–NAFFOURI T Y, et al. Enhancing secrecy with multiantenna transmission in millimeter wave vehicular communication systems [J]. IEEE transactions on vehicular technology, 2017, 66(9): 8139–8151. DOI:10.1109/TVT.2017.2681965
[17] JU Y, WANG H M, ZHENG T X, et al. Secure transmission with artificial noise in millimeter wave systems [J]. IEEE transactions on communications, 2017, 65(5): 2114–2127. DOI: 10.1109/TCOMM.2017.2672661
[18] TIAN X W, LIU Q, WANG Z H, et al. Secure hybrid beamformers design in mmWave MIMO wiretap systems [EB/OL]. [2021–06–21]. https://ui. adsabs. harvard. edu/abs/2020ISysJ..14..548T/abstract
[19] ZOU Y L, ZHU J, WANG X B, et al. Improving physical–layer security in wireless communications using diversity techniques [J]. IEEE network, 2015, 29(1): 42–48. DOI: 10.1109/MNET.2015.7018202
[20] VALLIAPPAN N, LOZANO A, HEATH R W. Antenna subset modulation for secure millimeter–wave wireless communication [J]. IEEE transactions on communications, 2013, 61(8): 3231–3245. DOI:10.1109/TCOMM.2013.061013.120459

作 者 简 介



倪云云，南京邮电大学物联网学院在读硕士研究生；主要研究领域为物理层安全预编码技术、机器学习等。

陈伯庆，南京邮电大学计算机学院在读博士研究生；主要研究领域为毫米波通信系统物理层安全技术；申请发明专利2项。

李刚，中兴通讯股份有限公司高级工程师、5G研发总工，深圳市国家级领军人才；从事CDMA/WiMAX/LTE/Pre5G/5G等产品的技术方案设计、架构设计和研发管理工作；发表论文5篇，申请发明专利15项。