基于极化状态调制的无线通信物理层安全传输技术

李 敏[1], 梁莉莉[1,2], 魏 冬[1,2]

[1]中国科学院信息工程研究所 北京 中国 100093
[2]中国科学院大学 北京 中国 100049

摘要 针对无线通信系统中物理层信息安全风险问题, 提出了一种基于极化状态调制的物理层安全传输技术。在无线通信中, 引入极化状态调制, 在经典的空域、时频域的基础上, 增加了对信号极化域的描述。一方面, 设计高维星座映射方案, 利用信号的幅度、相位和极化状态共同承载信息, 将传统调制技术和极化状态调制有效地结合在一起; 另一方面, 在高维星座映射方案的基础上, 进一步设计基于去极化效应的信道预编码机制, 通过增大 Bob 和 Eve 在极化域的信道差异实现物理层保密传输。安全性分析和仿真实验结果表明, 利用该机制能够提升系统的保密容量, 在接收信噪比为 22dB 时, 窃听者接收到的星座图仍然是十分紊乱的, 无法恢复出有效信息。

关键词 物理层安全; 极化状态调制; 高维星座映射; 去极化效应; 信道预编码
中图法分类号 TN918.91 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2018.09.09

Physical Layer Security Transmission Technology Based on Polarization-Shift Keying in Wireless Communications

LI Min[1], LIANG Lili[1,2], WEI Dong[1,2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]University of Chinese Academy of Sciences, Beijing 100049, China

Abstract Aiming at the physical layer information security risk in the wireless communication system, a physical layer security transmission technology based on polarization shift keying (POLSK) is proposed in this paper. In wireless communications, POLSK is introduced, and the description of the signal in polarization domain is added on the basis of the classical airspace, time and frequency domains. On the one hand, the high-dimensional constellation mapping scheme is designed. Utilize the amplitude, phase, and polarization states of the signal to carry useful information, so that the traditional modulation technology and POLSK can be effectively combined together. On the other hand, based on the high-dimensional constellation mapping scheme, the channel precoding mechanism based on the depolarization effect is further designed to realize the physical layer confidential transmission by increasing the channel difference between Bob and Eve in the polarized domain. Security analysis and simulation and experiment results show that, the mechanism can improve the system's secrecy capacity. When the received signal to noise ratio (SNR) is 22dB, the received constellation is still very chaotic and cannot recover the effective information.

Key words physical layer security; polarization shift keying; high-dimensional constellation mapping; depolarization effect; channel precoding

1 引言

随着无线通信技术的飞速发展, 无线通信业务已深入到人们工作和生活中的各个方面。无线通信链路的开放性和广播性使得通信不受空间的约束, 这是无线通信得以广泛应用的优势, 但同时也导致覆盖范围内的任何人都能够截获接收信号, 存在安全风险[1]。保障信息在物理层上的安全传输可以从根本上防止信息不被第三方窃听, 因此, 物理层安全研究已经成为无线通信安全领域中的一个研究热点。目前, 国内外普遍沿用的物理层安全研究是指基于信息理论的物理层安全理论和技术的研究[2]。

通讯作者: 魏冬, 博士, 副研究员, Email: weidong@iie.ac.cn。
本课题得到国家自然科学基金项目(No. 61501458)资助。
收稿日期: 2017-02-24; 修改日期: 2017-05-02; 定稿日期: 2018-08-20

信息理论安全的概念最早由 Shannon 于 1949 年提出[3], 文中阐述了保密通信的基本原理, 奠定了信息理论安全的基础。Shannon 指出, 当合法接收者与窃听者可以同时接收发送的信号时, 通信系统的安全将无法得到保证, 这个结论建立在窃听者和合法接收者接收到完全相同的信号。然而由于无线信道的随机性和差异性及信道噪声的干扰, 窃听者和合法接收者极有可能接收到发送信号的两个不同副本, 可以利用信道的这种特点去加密信息。在此基础上, Wyner 于 1975 年提出了著名的三点窃听信道模型(wiretap channel)[4], 为无线通信物理层安全的发展做出了巨大贡献。Wyner 指出, 只要窃听者接收到的信号是合法接收者接收信号的退化版本, 则存在一种编码方式可以实现完美保密性通信, 合法用户能够正常接收信号, 而窃听者却无法获取任何与信号相关的有用信息。1978 年 Csiszar 和 Korner 研究了在广播信道下保密信息的传输[5], 并定义了保密容量, 建立了针对无线通信链路的窃听信道模型。文中证明, 只要窃听者接收信息的信道噪声比合法用户的信道噪声大, 则可实现不依赖密钥共享机制的完美保密性通信。同年, Leung 等人进一步研究了高斯信道模型下的保密信息传输[6]。近些年来, 基于信息理论安全的研究集中在多用户、多输入多输出(Multiple Input Multiple Output, MIMO)等无线信道模型[7,8]。信息理论安全研究为物理层安全传输技术的发展奠定了理论基础, 从信息论的角度给出了利用无线通信物理层的特性设计信息安全防护的可能性。

由于无线通信环境的复杂性, 无线信道具有空间唯一性、随机性和短时互易性等特点[1-2,7]。无线信道的这些特点为基于信道差异的物理层安全技术提供了基础 [8-13]。文献[8-10]利用合法信道特征生成密钥, 与上层密钥加密算法协同实现安全通信。这种方法避免了传统加密算法中复杂的密钥分发和管理, 但算法安全性仍主要依赖于上层加密协议, 实现复杂, 目前尚处于理论研究阶段, 且多针对衰落情况相对简单的窄带系统。另一方面, 无密钥物理层安全传输技术[11-13]则是利用无线信道的空间唯一性、短时互易性等特点, 使合法信道相比窃听信道具有尽可能大的信道优势, 如波束成形[12]和人工噪声[13]的应用。这种方法一般需要已知部分窃听信道信息, 或要求发送端天线数量多于窃听端天线数量, 在实际通信环境中, 无法保证满足这些条件。

基于信道差异的物理层安全技术, 核心是通过利用合法信道和窃听信道的差异, 通过合法信道传输有用信息, 窃听者由于缺少相关信息而无法对其破解, 但该技术本质上并未对信号的调制信息进行直接防护, 窃听者一旦通过增大窃听设备数量等手段获取到通信信号, 仍然可以轻易恢复出物理层信息。

与基于信道差异的物理层安全技术不同, 调制加密技术针对物理层上信号的调制过程直接设计加密算法。低截获概率通信通过采用扩频或跳频等调制技术[14-15], 增大信号被窃听者截获的难度, 从而使调制信息具有很好的隐蔽性和抗干扰性。其中, 跳频通信是指载波信号中心频率在宽频带内按照一定的跳频序列随机跳变, 高随机的频率跳变增大了信号被截获或干扰的难度; 扩频通信则是利用伪随机扩频序列将信息调制成远远大于实际信息带宽需求的宽带通信信号, 将功率谱均匀分布在很宽的频谱范围内, 从而降低信号被截获的概率, 如直接序列码分多址技术的应用。低截获概率技术关注如何降低信号被窃听者截获的概率, 一旦窃听者掌握跳频或扩频序列, 通信安全仍会受到威胁。从无线信道特征的应用角度来看, 低截获概率并没有有效利用到无线信道的特点; 而且, 跳频和扩频技术均需要较大的带宽, 频谱利用率低, 设备成本高。

基于信道差异的物理层安全技术和低截获概率通信技术均是通过增大窃听者截获有用信号的难度的方式, 降低物理层信息泄漏的风险。而基于星座加扰的调制加密技术, 采用直接对符号映射过程进行加密的方式, 扰乱窃听者接收的调制信息。文献[16,17]采用逻辑斯谛映射产生混沌序列控制相位旋转角度, 文献[18]则采用了计数模式下的 AES 加密算法生成流密码生成相位旋转角度。文献[19]利用正交频分复用技术多载波调制的特点, 通过对 IFFT 后的符号置换交织进行时域加扰, 同时扰乱星座点的相位和幅度。受加密序列长度的限制, 星座点加密效果有限, 需要进一步对星座点进行扰乱。文献[17]采用了人工噪声对星座图进一步加扰, 文献[19]引入了信道预补偿, 基于合法信道的幅度和相位特征设计预补偿矩阵, 由于窃听信道与合法信道的不相关性, 窃听者接收星座图是紊乱的, 然而, 在慢衰落信道中, 窃听者仍可以通过盲均衡等技术估计出合法信道信息, 从而消除该影响。

综上所述, 现有的物理层安全传输研究主要可分为两大类, 一类是从利用无线传输媒介的特性出发, 通过增大合法信道和窃听信道的差异性, 设计物理层安全传输算法, 如无线密钥生成技术和无密

钥物理层安全传输技术; 一类从加密调制过程出发, 在传统调制技术的基础上设计调制加密算法, 使窃听者无法截获或破译有效的物理层信号, 如低截获概率通信技术及基于星座加扰的物理层安全传输技术。

可以看出, 现有的物理层安全研究多是利用信道的时频域或空域的特征, 设计物理层加密算法。本文提出一种基于极化状态调制的物理层安全传输技术, 在传统的空域、时频域的基础上, 增加信号极化域的描述, 利用极化域的特点实现物理层安全传输。

极化状态是关于信号轨迹与旋向的描述, 是一种矢量特征, 利用极化状态承载信息最初起源于光纤通信系统, 也称为偏振键控调制(Polarization-Shift Keying, POLSK)[20-21]。随着双极化天线的广泛使用, 人们逐渐认识到信号极化特征在无线通信领域中的巨大应用潜力, 开始关注无线通信领域的极化信号处理研究。

在无线通信领域中, 利用极化状态进行多维调制是人们关注的一个重点。宋汉斌从空间电磁场的数学描述出发, 将幅度调制与极化状态调制结合起来, 提出了使用电磁波信号的幅度、辅助极化角与极化相位差异角进行三维调制的理论和方法[22]。文献[23]则从射频功放能效优化的角度出发, 提出了一种极化状态调制与传统幅度-相位调制相结合的调制解调方法。在文献[24]中, 极化状态调制被用来建立隐蔽通信链路, 同时, 该文对比分析了极化状态调制和传统调制技术的频谱效率、频谱相似度等性能。

高维星座是极化状态调制引入的另外一个特点。由于极化状态与三维斯托克斯(Stokes)空间庞加莱球上的极化星座点一一对应, 若在传统基于幅度或相位调制的基础上引入极化状态调制, 可将二维欧氏空间和三维 Stokes 空间结合起来, 传统的二维平面星座则被扩展成高维空间中的星座。文献[21,23]构造了一种基于极化正交振幅调制(Polarization Quadrature Amplitude Modulation, POL-QAM)的高维星座结构, 极化状态分布在庞加莱球面上, 每种极化状态对应一个 4QAM 调制星座空间, 将极化状态和 QAM 结合在了一起。然而, 目前的研究更倾向于分析利用多维调制及高维星座提升系统的传输性能, 缺少针对安全领域的研究。

另外, 由于无线通信环境的多径和富散射等特性使得各极化支路的信号可能互相耦合, 导致水平和垂直极化分量在经过无线信道传播后产生了交叉极化干扰, 两者之间不再严格正交, 极化状态产生失真, 会对合法通信质量产生影响, 该过程也称为去极化效应。为解决该问题, Thomas Pratt 等提出一种自适应发射极化状态的方法, 消除信道极化相关损耗和极化模式色散的影响[25]。文献[26]分析了不同环境中极化相关损耗的分布方式。由于去极化效应与信道密切相关, 不同的无线信道受到的去极化效应也有所不同, 因此, 无线信道去极化效应也可以被用来加密信息。文献[24]即利用去极化效应对合法信道进行了预补偿, 同时恶化了窃听信道接收质量。

本文借鉴了文献[24]的思想, 提出一种基于极化状态调制的物理层安全传输机制, 一方面, 设计高维星座映射方案, 利用信号的标量特征(幅度、相位)和矢量特征(极化状态)共同承载信息, 从而增加了信号极化域的描述; 另一方面, 在高维星座映射方案的基础上, 进一步设计信道预编码矩阵, 增大合法接收者和窃听者在极化域的信道差异实现物理层安全传输。在本文中, 将 QAM 和相移键控(Phase-shift Keying, PSK)调制技术统称为传统调制技术(Traditional Modulation, TM)。

本文后续安排如下: 第二部分提出了基于极化状态调制的物理层安全模型; 第三部分介绍了物理层安全模型中高维星座映射方案的设计方法; 第四部分则分析了如何设计物理层安全模型中的信道预编码和去编码矩阵, 并分析了加入信道预编码前后系统保密容量的变化; 第五部分基于软件无线电平台及 MATLAB 仿真平台对系统的性能进行了测试与分析; 第六部分对论文内容进行了总结与展望。

2 基于极化状态调制的物理层安全模型

整个安全传输系统模型如图 1 所示。发送端 Alice、合法接收端 Bob 和窃听端 Eve 均配置有相同的正交双极化天线用于信号发送和接收, 采用时分双工(Time Division Duplexing, TDD)方式。Alice 和 Bob 之间的信道称为合法信道, 记作 H_{AB}; Alice 和 Eve 之间的信道称为窃听信道, 记作 H_{AE}。在信道相干时间内, 合法通信双方可获得相同的信道信息, 即信道满足短时互易性。当 Eve 与 Alice 或 Bob 的距离相差半个信号波长以上时, H_{AE} 和 H_{AB} 可看作是不相关的[1], 实际窃听信道模型中, 很容易满足该条件, 即信道具有唯一性。

通信过程如下: 合法通信双方首先发送包含有导频序列的通信请求, 获得当前的合法信道信息 H_{AB}, 然后进行安全通信。在 Alice 端, 对传输数据进行高维星座映射, 然后对映射符号进行预编码加权, 预编码矩阵与 H_{AB} 相关。在 Bob 端, 对接收信息

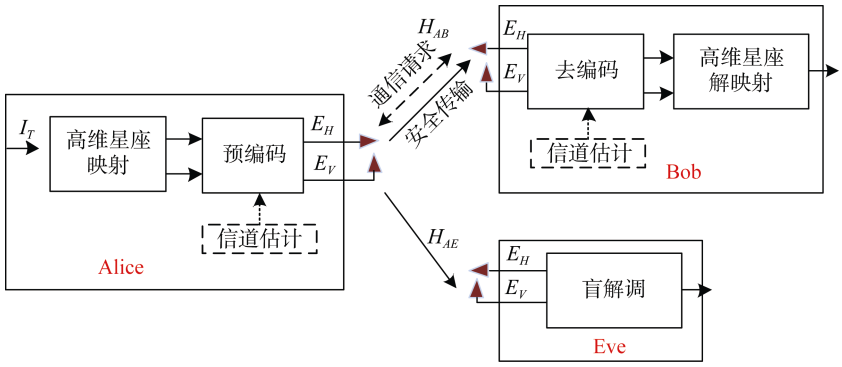


图 1　安全传输系统模型

Figure 1　The model of secure communication system

进行去编码, 然后进行高维星座解映射, 即可恢复出原始信息。然而, 由于窃听信道和合法信道是不相关的, 窃听端无法获得 H_{AB}, 获得的星座图受到了严重扰乱, 窃听者无法恢复出正常信息, 从而保障无线通信的物理层安全传输。

3　高维星座映射方案

本节设计了一种高维星座映射方案, 通过对发送信息进行高维星座映射, 引入信号极化域的描述。

在传统调制技术的基础上引入极化状态调制, 此时, 信号的幅度 A_k、相位 ϕ_k 和极化状态 P_k 共同承载着发送信息。幅度和相位由传统调制过程控制, 极化状态由极化状态调制过程控制。若由 M_T 阶传统调制(PSK 或 QAM)和 M_P 阶 POLSK 调制构成 M 阶基于高维星座映射的调制技术(Multilevel Constellation Modulation, MCM), 则各调制阶数满足 $M_T \times M_P = M$。高维星座映射方案如图 2 所示。

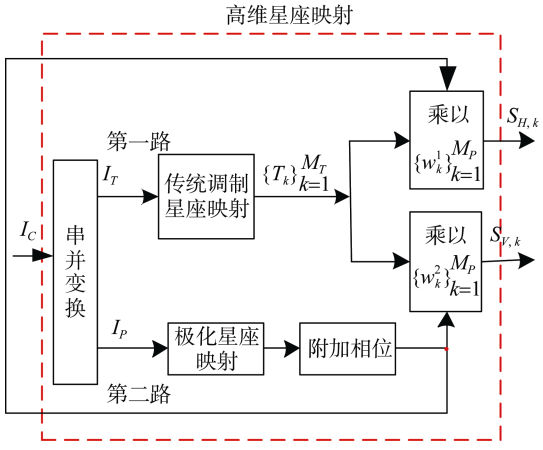


图 2　高维星座映射方案

Figure 2　The constellation mapping method

首先, 将经过信源和信道编码后的二进制序列 I_C 进行串并变换, 得到比特序列对 (I_T, I_P), 其中, I_T 包含 $\log_2(M_T)$ 个比特, I_P 包含 $\log_2(M_P)$ 个比特。

然后, 将 I_T 和 I_P 分成两路分别进行符号映射。I_T 进行 M_T 阶的传统调制符号映射, 当 M_T>8 时进行 QAM 映射, 否则进行 PSK 映射, 得到传统调制符号 T_k; I_P 被映射为三维 Stokes 空间中 M_P 阶的极化星座点, 并经过附加相位模块, 得到水平极化和垂直极化加权因子 w_k^1 和 w_k^2; 将水平和垂直加权因子分别与 T_k 相乘, 即得到高维映射后的符号 S_k。附加相位模块是为了能够更自由地设计极化星座点, 更好地构建各极化支路的星座结构。

传统调制符号 T_k、加权因子 w_k^1 和 w_k^2 及符号 S_k 的 Jones 矢量表示形式如下:

$$T_k = A_k e^{j\phi_k}$$
$$\begin{bmatrix} w_k^1 \\ w_k^2 \end{bmatrix} = e^{j\Delta\varphi_k} \begin{bmatrix} \cos\delta_k \\ \sin\delta_k e^{j\gamma_k} \end{bmatrix} \tag{1}$$
$$S_k = \begin{bmatrix} A_k e^{j(\phi_k+\Delta\varphi_k)} \cos\delta_k \\ A_k e^{j(\phi_k+\Delta\varphi_k)} \sin\delta_k e^{j\gamma_k} \end{bmatrix}$$

其中, $\Delta\varphi_k$ 为附加相位, $-\pi \leqslant \Delta\varphi_k < \pi$; (δ_k, γ_k) 为极化状态描述子, $0 \leqslant \delta_k \leqslant \pi/2$, $-\pi \leqslant \gamma_k < \pi$, δ_k 为矢量电磁波的辅助极化角, γ_k 为矢量电磁波的极化相位差异角。若 $\|E_{kH}\|$ ($\|E_{kV}\|$)、φ_{kH} (φ_{kV})分别为水平(垂直)极化支路信号中第 k 个符号的幅值和相位, 则有

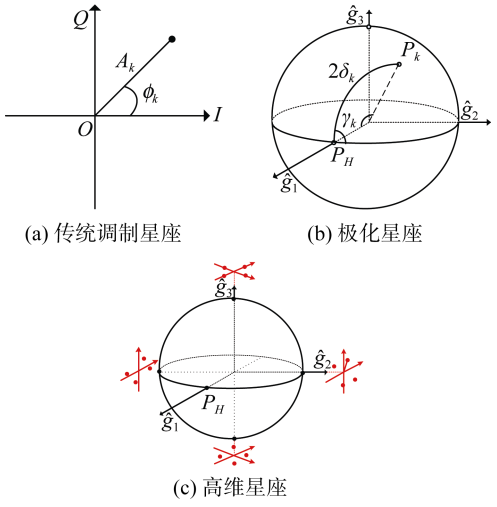
$$\delta_k = a\tan\left(\frac{\|E_{kV}\|}{\|E_{kH}\|}\right) \tag{2}$$
$$\gamma_k = \varphi_{kV} - \varphi_{kH}$$

最后, 对符号 S_k 进行成形滤波, 得到基带 MCM 调制信号, 其 Jones 矢量可表示为

$$S(t)=\begin{bmatrix}S_H(t)\\S_V(t)\end{bmatrix}=\sum_k A_k e^{j(\phi_k+\Delta\varphi_k)}\begin{bmatrix}\cos\delta_k\\\sin\delta_k e^{j\gamma_k}\end{bmatrix}g(t-kT) \tag{3}$$

其中，$S_H(t)$ 和 $S_V(t)$ 分别表示水平和垂直极化分量，$g(t)$ 为单位阶跃函数，T 为符号周期。

为了直观地理解高维星座映射过程，本文分析了上述映射过程的星座结构变化情况。经过传统调制符号映射后，Jones 矢量为 $\left[A_k e^{j\phi_k}, A_k e^{j\phi_k}\right]$。此时，水平极化支路和垂直极化支路的调制符号是相同的，星座点分别分布在二维欧氏空间中，如图 3(a)所示；同时，由极化加权因子 $\left[w_k^1, w_k^2\right]^{\mathrm{T}}$ 决定的极化星座点分布在三维的 Stoke 空间中的 Poincare 球上，如图 3(b)所示；然后，利用极化加权因子对传统调制符号进行加权，此时，Jones 矢量变为 $\left[A_k\cos\delta_k e^{j(\phi_k+\Delta\varphi_k)}, A_k\sin\delta_k e^{j(\phi_k+\gamma_k+\Delta\varphi_k)}\right]$，通过这种方式，将传统调制和极化状态调制结合在了一起，形成了高维星座图，如图 3(c)所示。需要注意的是，引入附加相位，会改变各极化支路的符号状态，但不会对信号的极化状态产生影响，因为极化状态是由水平和垂直极化支路的符号幅度比和相位差共同决定的矢量特征。



(a) 传统调制星座　(b) 极化星座

(c) 高维星座

图 3　高维星座模型

Figure 3　The constellation model

可见，经过高维星座映射，传统调制技术和 POLSK 技术有效地结合在了一起，形成了高维星座空间，所有的极化状态星座点分布在 Poincare 球面上，每一个极化状态星座点与一个二维欧氏空间连接，而且这些欧氏空间相互没有重叠交叉。即便是两个相同位置上的传统调制星座点，它们也可能位于两个不同的二维欧氏空间中而连接着两个不同的极化状态星座点。因此，星座图设计的灵活度大大增加。

相应地，为了能够从接收到的信号中恢复出原始发送序列，在合法接收端设计高维星座解映射方案如下:

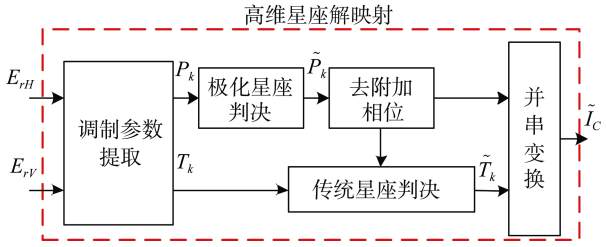


图 4　高维星座解映射方案

Figure 4　The constellation inverse mapping method

首先，接收到的基带水平极化和垂直极化支路分别记为 E_{kH} 和 E_{kV}，对应的 Jones 矢量可表示为

$$\begin{bmatrix}E_{kH}\\E_{kV}\end{bmatrix}=A_k\begin{bmatrix}\cos\delta_k e^{j(\phi_k+\Delta\varphi_k)}\\\sin\delta_k e^{j(\phi_k+\gamma_k+\Delta\varphi_k)}\end{bmatrix}+\begin{bmatrix}n_{kH}\\n_{kV}\end{bmatrix} \tag{4}$$

上式中，$\begin{bmatrix}n_{kH}\\n_{kV}\end{bmatrix}$ 为加性高斯白噪声。

通过 Stokes 矢量提取参数的方法恢复出极化调制状态 P_k 和传统调制状态 T_k。

$$\begin{aligned}A_k&=\sqrt{g_{k0}}=\sqrt{\|E_{rH}\|^2+\|E_{rV}\|^2}\\g_{k1}&=\frac{1}{g_{k0}}\left(\|E_{rH}\|^2-\|E_{rV}\|\right)^2\\g_{k2}&=\frac{1}{g_{k0}}\left(E_{rH}E_{rV}^*+E_{rV}E_{rH}^*\right)\\g_{k3}&=\frac{j}{g_{k0}}\left(-E_{rH}E_{rV}^*+E_{rV}E_{rH}^*\right)\end{aligned} \tag{5}$$

其中，$\left(g_{k0},g_{k1},g_{k2},g_{k3}\right)$ 为极化状态 P_k 对应的四个 Stokes 参数，g_{k0} 表征了信号功率，与极化状态描述子相对应，关系如下[20]:

$$\begin{aligned}g_{k0}&=\|E_{KH}\|^2+\|E_{KV}\|^2\\g_{k1}&=\|E_{KH}\|^2-\|E_{KV}\|^2\\g_{k2}&=2\|E_{KH}E_{KV}\|\cos(\gamma_k)\\g_{k3}&=2\|E_{KH}E_{KV}\|\sin(\gamma_k)\end{aligned} \tag{6}$$

根据式(6)可恢复出极化调制状态 P_k。根据 g_{k1}、g_{k2} 和 g_{k3} 可以确定极化辅助角 δ_k、极化相位差异角

γ_k 及附加相位 $\Delta\varphi_k$，在水平和垂直支路分别去除附加相位影响，结合 E_{rH} 和 E_{rV} 即可恢复出调制相位 ϕ_k，从而恢复出传统调制状态 T_k。

然后，利用最大似然准则(Maximum Likelihood, ML)分别对极化状态和传统调制状态进行判决。

$$\begin{aligned}\tilde{P}_k &= \arg \min_{P_i(1\leqslant i\leqslant M_p)} dis\{P_i, P_k\} \\ \tilde{T}_k &= \arg \min_{T_i(1\leqslant i\leqslant M_T)} dis\{T_i, T_k\}\end{aligned} \tag{7}$$

其中，$dis\{X_i, X_k\}$ 表示接收符号与调制星座点的欧氏距离。

最后，将恢复的两路信息进行并串变换，依据高维映射规则进行逆映射，恢复出原信息序列 $\tilde{I}_c$。

本文涉及 6 种传统调制星座结构，包括 BPSK、QPSK、8PSK、16QAM、32QAM、64QAM，其中，QAM 为方型结构。涉及的 POLSK 技术包括 2-POLSK、4-POLSK circle、4-POLSK tetrahedron 和 8-POLSK cube 四种规则的结构，示例如图 5[20]:

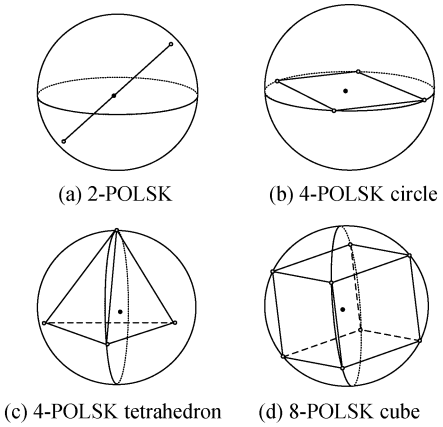


图 5 M-POLSK 星座图

Figure 5 The M-POLSK constellation

在本文中，采用虚拟极化发射原理产生发射信号的极化状态[27]，并利用一个正交双极化天线发送，避免了复杂的极化状态控制电路，利用数字信号处理的方式实现高维星座映射解映射过程，对传统调制技术具有很好的兼容性，实现简单。经过高维星座映射后，极化状态调制和传统调制相结合，信号的矢量特征(极化状态)和标量特征(幅度、相位)共同承载信息，打破了传统调制技术原始信息与调制信息的一一映射关系，可以对抗只针对传统标量特征的简单攻击。

然而，无线信道的去极化效应会造成极化状态的偏移与失真，从而影响合法通信的传输性能。而且，MCM 与传统调制技术面临同样的问题，如果窃听端采用相同的正交双极化天线接收，在平稳衰落信道中，窃听者仍可以通过通信盲均衡等技术手段对信道进行估计与均衡，进而恢复出星座图，系统仍然面临安全风险。为解决该问题，本文提出一种基于信道预编码的物理层安全传输技术，利用信道的去极化效应，设计信道预编码矩阵，对高维星座图进行扰乱，实现高维调制信息的安全防护。

4 信道预编码方案

4.1 去极化效应

通过引入极化域，信道模型由传统的单输入单输出变为双输入双输出，如下图所示[24]:

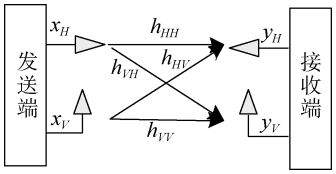


图 6 信道模型

Figure 6 The channel model

在图 6 中，合法通信双方均采用正交双极化天线，x_H 和 x_V 分别表示水平、垂直极化天线发射的信号；y_H 和 y_V 分别表示水平、垂直极化天线接收的信号。设信道矩阵为 H_C，可以得到

$$H_C = \begin{bmatrix} h_{HH} & h_{HV} \\ h_{VH} & h_{VV} \end{bmatrix} \tag{8}$$

其中，$h_{ij}(i, j = H, V)$ 为发射天线 j 到接收天线 i 的信道衰落系数。

利用奇异值分解，H_C 可以分解为

$$H_C = U_C \Sigma_C V_C^{*} = U_C \begin{bmatrix} \sqrt{\lambda_{C,1}} & 0 \\ 0 & \sqrt{\lambda_{C,2}} \end{bmatrix} V_C^{*} \tag{9}$$

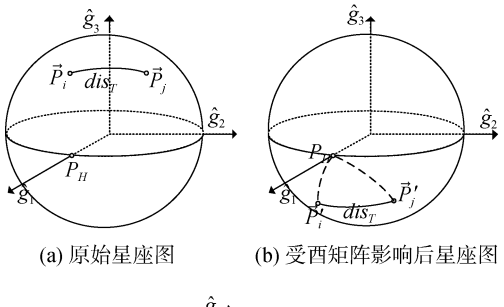
其中，U_C 和 V_C 为 2×2 的酉矩阵，$(\bullet)^{*}$ 表示矩阵的共轭转置；Σ_C 为对角矩阵；$\lambda_{C,1}$ 和 $\lambda_{C,2}$ 为矩阵 $H_C H_C^{*}$ 的特征值，且满足 $\lambda_{C,1} \geq \lambda_{C,2} > 0$。

无线信道去极化效应会造成极化星座失真，结合图 7，对其进行具体分析。

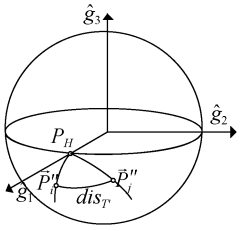
假设 P_i 和 P_j 为单位 Poincare 球面上相邻的两个星座点，其星座点距离为 dis_T，如图 7(a)所示。

酉矩阵的作用会使得所有的极化星座点在 Poincare 球面上产生相同的旋转，即极化星座结构在球面上整体发生了刚性旋转，星座结构和每个星座点的功率都保持不变，这样极化星座点承载的信息

也不会丢失, 如图 7(b)所示。



(a) 原始星座图 (b) 受酉矩阵影响后星座图



(c) 受对角阵影响后星座图

图 7 去极化效应对极化星座产生的影响

Figure 7 The impact to polarization constellation from depolarized effect

而对角阵 Σ_C 对不同的极化星座点可能产生不同的影响, 具体与星座点的位置有关。受 Σ_C 的影响, 水平和垂直极化分量间的相位差保持不变, 而幅度比由 $\tan\delta$ 缩小为 $\sqrt{\lambda_{C,2}/\lambda_{C,1}}\tan\delta$, 对极化星座进行归一化, 表现在单位 Poincare 球上幅度比的缩小会造成极化星座点向水平极化状态 P_H 收缩, 如图 7(c)所示, 此时, 每个极化星座点承载的信息将有所损失。

无线信道的去极化效应会使得本文提出的高维星座图产生畸变, 从而影响系统的误码性能。

4.2 基于去极化效应的信道预编码方案

考虑到, 无线信道具有短时互易性和唯一性, 本文利用无线信道的去极化效应设计信道预编码矩阵, 建立等效信道模型, 增大合法信道和窃听信道在极化域的差异, 从而保障无线通信的信息安全。

基于信道预编码的等效信道模型如图 8 所示, X 为 Alice 发送信号; C_P 和 D_P 分别是预编码和去解码模块, 与合法信道共同等效形成稳定信道, 便于 Bob 接收信息, 而与窃听信道共同等效成随机快变的信道, 恶化 Eve 接收质量。

模型中, Bob 和 Eve 接收信号分别可以表示为

$$\begin{aligned} Y_B &= D_P H_{AB} C_P X + D_P N_B = H_{AB}{}' X + N_B{}' \\ Y_E &= H_{AE} C_P X + N_E = H_{AE}{}' X + N_E \end{aligned} \tag{10}$$

其中, N_B 和 N_E 分别为合法信道和窃听信道中的加性噪声。

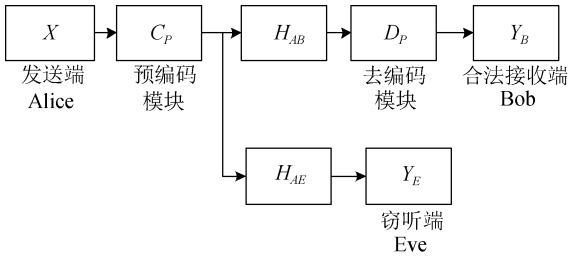


图 8 基于去极化效应的等效信道模型

Figure 8 The model of the depolarized channel

在发送端设置预编码矩阵 C_P, 如下:

$$\begin{aligned} C_P &= V_{AB}\begin{bmatrix} \dfrac{1}{\sqrt{\lambda_{AB,1}}} & 0 \\ 0 & \dfrac{1}{\sqrt{\lambda_{AB,2}}} \end{bmatrix}\left(U_{AB}{}^*\right)^n \begin{bmatrix} (-1)^m & 0 \\ 0 & 1 \end{bmatrix} \\ H_{AB} &= U_{AB}\begin{bmatrix} \sqrt{\lambda_{AB,1}} & 0 \\ 0 & \sqrt{\lambda_{AB,2}} \end{bmatrix} V_{AB} \end{aligned} \tag{11}$$

其中, m 为 0 或 1, n 为整数, 且满足 $-N+1 \leqslant n \leqslant N$。$U_{AB}$ 和 V_{AB} 为合法信道矩阵 H_{AB} 奇异值分解得到的酉矩阵, $\lambda_{AB,1}$ 和 $\lambda_{AB,2}$ 为矩阵 $H_{AB}H_{AB}{}^*$ 的特征值。加权矩阵的选择由合法通信双方共享的伪随机序列决定。

相应地, 在接收端设置去编码矩阵, 如下:

$$D_P = \begin{bmatrix} (-1)^m & 0 \\ 0 & 1 \end{bmatrix}\left(U_{AB}\right)^{n-1} \tag{12}$$

这样, 合法信道即可等效为

$$H'_{AB} = D_P H_{AB} C_P = I \tag{13}$$

由于 D_P 为单位酉矩阵, 不影响噪声的统计特性, 式(10)中 $N_B{}'$ 与 N_B 可看作是一类噪声信号。

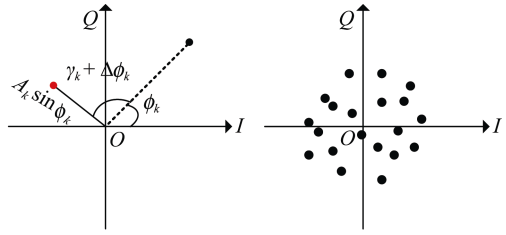
另一方面, 窃听信道可等效为

$$\begin{aligned} H'_{AE} &= H_{AE} C_P \\ &= H_{AE} V_{AB}\begin{bmatrix} \dfrac{1}{\sqrt{\lambda_{AB,1}}} & 0 \\ 0 & \dfrac{1}{\sqrt{\lambda_{AB,2}}} \end{bmatrix}\left(U_{AB}{}^*\right)^n \begin{bmatrix} (-1)^m & 0 \\ 0 & 1 \end{bmatrix} \end{aligned} \tag{14}$$

由于合法信道和窃听信道是不相关的, 窃听者接收到的信号除了受到自身信道的去极化效应影响外, 还会受到与合法信道相关的一次星座畸变, n 次酉矩阵变换刚性旋转和 m 次反转。预编码矩阵 C_P 有 $4N$ 种选择, 在发送端和合法接收端同步产生伪随机序列来选择 C_P, 即使在平稳的信道传输环境中, 窃听信道仍可等效为快变的信道, 窃听者接收到的星

座图遭受随机扰乱。合法信道与窃听信道不相关, 随机快变的等效信道使得窃听者很难采用盲均衡等算法对星座结构等信息进行恢复, 安全性有所保障。

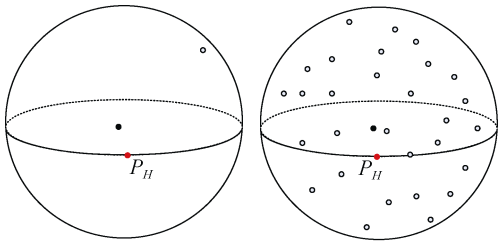
图 9 为信道预编码对垂直极化支路符号的影响, 图 10 则描述了其对极化星座点即矢量特征的影响。



(a) 高维星座映射后星座图 (b) 预编码后星座图

图 9 信道预编码对垂直极化支路符号的影响

Figure 9 The impact to the vertical polarization symbol caused by channel precoding



(a) 原始星座图 (b) 预编码后星座图

图 10 信道预编码对极化星座点的影响

Figure 10 The impact to polarization constellation caused by channel precoding

从图 9 中可以看出, 经过高维星座映射后, 各极化支路的符号受到了幅度调节和相位旋转的影响, 具体与极化星座点的设置有关, 经过随机预编码后, 水平和垂直支路的信号星座点进一步被随机扰乱, 分布在整个二维欧氏平面, 各支路不再具备传统调制信号的统计特性。图 10 则表明, 经过多个预编码矩阵作用后, 每个极化星座点随机分布在整个 Poincare 球面上, 星座结构严重畸变。上述分析是以一个星座点的影响为例, 实际调制阶数越大, 相应的星座图加密效果越好。

4.3 保密容量分析

本文比较分析了引入信道预编码前后系统的保密容量变化特点。保密容量是衡量保密通信性能的重要参数, 其定义如下[5]:

$$C_{\text{sec}}=\max\left\{I\left(X;Y_B\right)-I\left(X;Y_E\right)\right\} \tag{15}$$

其中, $I\left(X;Y\right)$表示 Y 对 X 的平均互信息量, 也称为交互熵。从输出端的角度看, 平均互信息量表示从 Y 获得的关于 X 的平均信息量, 从整个通信系统的角度看, 平均互信息量表示通信前后整个系统不确定度的减少量。当 X 和 Y 统计独立时, $I\left(X;Y\right)=0$, 意味着不能从一个变量获得关于另一个变量的任何信息。

从式(15)可以看出, 提升系统保密容量的关键在于增大合法信道和窃听信道的差异。增大 $I\left(X;Y_B\right)$, 如波束成形技术的应用, 或者减小 $I\left(X;Y_E\right)$ 降低窃听信道的通信质量, 如加入人工噪声等技术, 都可以提高系统的保密容量, 增强系统的安全性。

如果不引入信道预编码, 系统的保密容量为

$$\begin{aligned}C_{\text{sec}}{}'=\max\{&I\left(X;H_{AB}X+N_B\right)\\&-I\left(X;H_{AE}X+N_E\right)\}\end{aligned} \tag{16}$$

在本文提出的物理层安全传输方案中, 对于合法接收端而言, $I\left(X;Y_B\right)=I\left(X;X+N_B{}'\right)$, 经过信道预编码和去编码处理之后, 除了加性噪声的影响外, 理论上去除了信道衰落带来的影响, 如信道去极化效应引起的交叉极化干扰等, 从 Y_B 获得的关于 X 的平均信息量有所增加, 即

$$I\left(X;X+N_B{}'\right)\geqslant I\left(X;H_{AB}X+N_B\right) \tag{17}$$

当 $H_{AB}=I$, 即合法信道只受噪声影响时, 等号成立。

另外, $I\left(X;Y_E\right)=I\left(X;H_{AE}C_PX+N_E\right)$, 由于随机快变的预编码矩阵的作用, 窃听者接收到的信号 Y_E 受到随机的乘性干扰, 除了窃听信道衰落带来的影响外, 还会受到额外的随机干扰, 信号不再具备原有的统计特性, 减少了从 Y_E 获得的关于 X 的平均信息量, 即

$$I\left(X;H_{AE}C_PX+N_E\right)\leqslant I\left(X;H_{AE}X+N_E\right) \tag{18}$$

同样, 当 $H_{AB}=I$ 时等号成立。

式(18)满足信号传输理论中的数据处理定理(data processing theorem)。当消息经过多级处理时, 随着处理器数目的增多, 输入消息和输出消息之间的平均互信息量趋于变小, 每处理一次, 就有可能损失一部分信息。

联合式(15)~(18), 可以得出结论, $C_{\text{sec}}\geqslant C_{\text{sec}}{}'$。预编码矩阵 C_P 与合法信道状态直接相关, 在实际的无线通信系统中, 尤其在双极化天线应用系统中, 由于双极化天线隔离度的限制以及极化域的敏感性等问题, 无线信道不可能完全理想, 引入信道预编码能够提高系统的保密容量。

5 仿真实验与分析

结合 GNURadio、USRP X300 及水平-垂直正交双极化天线, 以及 MATLAB 仿真平台, 对本文所提物理层安全传输技术的性能进行了测试与分析。

由笔记本、USRP X300 和天线搭建成软件无线电平台, 连接方式如图 11 所示。

图 11 GNURadio+USRP 组成的软件无线电平台

Figure 11 The GNURadio+USRP based software radio platform

笔记本安装有 GNURadio 和 USRP 所需的 UHD 驱动; USRP X300 的 RF 子板选用 SBX-120, 支持 400-4400MHz 频率覆盖; 水平-垂直正交双极化天线型号为 KBT65VH15-24RT0, 频率范围为 2400-2500MHz。USRP 和笔记本之间通过千兆以太网线进行连接, 正交双极化天线的水平支路与 USRP 的 A 侧子板的 TX/RX 端口利用射频电缆进行连接, 垂直支路与 B 侧子板的 TX/RX 端口连接。

结合天线和 USRP 硬件参数, 设置实验参数如表 1 所示。

表 1 实验相关参数设置

Table 1 The related parameters of experiments

参数	指标
频率	2.4GHz
符号速率	400kHz
通信距离	25m
接收信噪比	10~22dB

搭建的无线通信系统包括发送端 Alice、合法接收端 Bob 和窃听端 Eve, 信道满足短时互易性和唯一性。三者均采用水平-垂直正交双极化天线发送或接收。双极化天线对通信两端天线的对齐程度有严格要求, 这更加有利于信息的安全传输, 对窃听者的位置有更加严格的限制。测试时 Alice、Bob 和 Eve 在一条直线上, 只是相对距离不同, 同样满足信道的唯一性等特点。

5.1 对接收星座图的影响

本节分别测试了不同信噪比下 Bob 和 Eve 接收星座图的情况。

设置 Alice 和 Bob 相距 25m, Alice 和 Eve 相距 30m, 通过在 Alice 端改变发射功率改变接收信噪比。图 12 和图 13 分别为 Bob 和 Eve 在接收信噪比为 22dB 时, 恢复出的 4MCM(BPSK-2POLSK)和 64MCM(16QAM-4POLSK tetrahedron)信号的星座图情况。

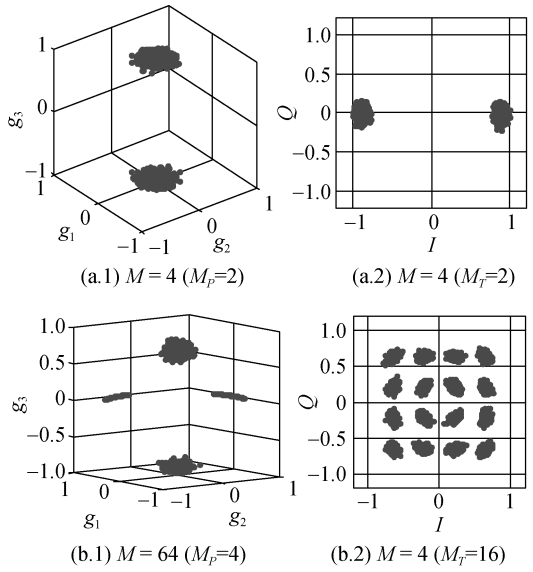


图 12 Bob 在信噪比为 22dB 时恢复出的 4MCM 和 16MCM 的星座图

Figure 12 The received constellation of 4MCM and 16MCM when SNR is 22dB

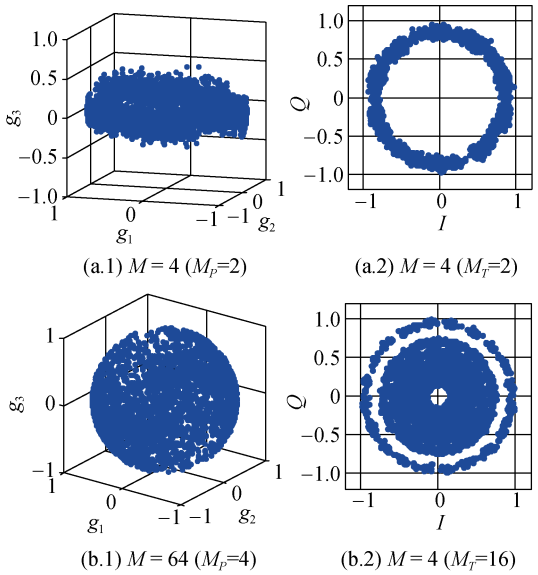


图 13 Eve 在信噪比为 22dB 时恢复出的 4MCM 和 16MCM 的星座图

Figure 13 The constellation of 4MCM and 16MCM received by Eve when SNR is 22dB

从图 12 和图 13 可以看出, 当信噪比为 22dB 时, 合法接收端能够很好的恢复出高维星座图, 而窃听端接收到的星座图十分紊乱, 无论是极化星座图还是传统调制对应的二维星座图, 都是严重扰乱过的。即使信噪比很高, 由于高维星座映射方案和信道预编码方案的引入, 窃听端仍然无法恢复出信号的有效信息。

5.2 对系统误码性能的影响

本节首先基于 MATLAB 仿真分析了系统的理论误码性能, 然后基于软件无线电平台分析了在实际的无线传输环境中 Bob 和 Eve 的接收误码性能。

5.2.1 系统的理论误码性能分析

原则上, 物理层安全算法不能降低系统的误码性能, 该部分分析了本文提出的 MCM 调制方案的误码性能。

由于 MCM 由 POLSK 和传统调制方式(PSK 和 QAM)结合而成, 其误码率可由这两类调制方式的误码率公式结合得出[22]:

$$P_{e,M-MCM}=1-\left(1-P_{e,M_T-TM}\right)\left(1-P_{e,M_P-POLSK}\right) \quad (19)$$

1 满足

$C_1: M_T \times M_P = M$, 且均为 2 的指数

$C_2: 2 \leqslant M_T, M_P < M$

对于 M 阶的 MCM 调制方案, 能够满足式(19)的 M_T 和 M_P 不唯一, 不同组合方式对应的误码性能不同, 具体与传统调制技术和 POLSK 的误码性能有关。

用 MATLAB 仿真绘制了各阶 PSK 和 POLSK 调制技术的误码率曲线[20,28], 如图 14 所示, 其中, E_s 为调制信号的平均符号能量, $N_0=2\sigma^2$ 为加性高斯白噪声的功率。从图 14 可以看出, 对于同阶的 PSK 和 POLSK 调制信号, PSK 性能更优, 比 POLSK 约有 3dB 的信噪比优势。另外, 对于 4 阶的 POLSK 调制, 采用四面体(tetrahedron)结构比四边形(circle)结构性能更好, 这是因为四面体具有更大的最小相邻星座距离。因此, 可以初步得出结论, 在设计高维星座映射方案时, 为取得更好的误码性能, M_T 应该不小于 M_P。

为进一步确定误码性能最优的 MCM 设计方案, 建立关于 M_T 最佳误码率优化模型如下:

$$\hat{M}_T=\arg\min_{M_T}\left(1-\left(1-P_{e,M_T-TM}\right)\left(1-P_{e,M/M_T\text{-POLSK}}\right)\right) \quad (1)$$

由于 POLSK 的误码率函数与调制阶数 M_T 不线性相关, 无法表示成 M_T 的函数, 从数学表达式上直接推导求出最佳设计方案比较困难, 本文通过数值仿真验证各阶调制误码率, 在此基础上确定最佳方案。本文给出了 4、8、16、32、64 阶 MCM 的高阶设计方案。最后, 求解出的最佳设计方案如表 2 所示。

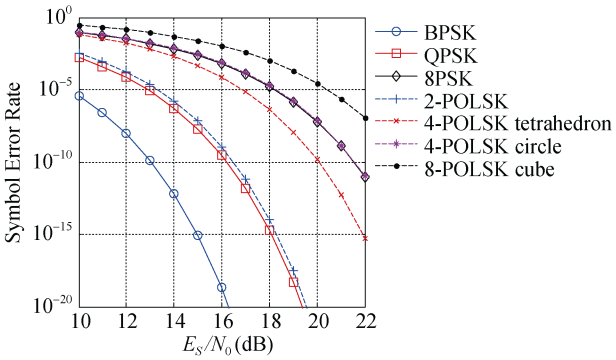


图 14 MPSK 和 M-POLSK 的误码率性能比较曲线

Figure 14 The symbol error rate curves comparison between MPSK and M-POLSK

表 2 高维星座映射最佳分配方案

Table 2 The optimal polarization constellation mapping method

调制阶数 M	传统调制方式及阶数 M_T	POLSK 调制阶数 M_P
4	BPSK	2
8	QPSK	2
16	QPSK	4-tetrahedron
32	8PSK	4-tetrahedron
64	16QAM	4-tetrahedron

可以看出, 与理论分析一致, POLSK 调制阶数均不大于传统调制阶数, 且当 $M \leqslant 64$ 时, $M_P \leqslant 4$。

图 15 为表 2 中各阶高维星座调制方案与传统调制技术误码性能曲线。从图 15 中可以看出, 当调制阶数为 4 时, MCM 误码性能相比 QPSK 损失 0.2dB, 而当调制阶数高于 4 阶时, MCM 具有更优的误码性能。另外, 与传统调制技术不同, 4 阶 MCM 和 8 阶 MCM 误码率曲线非常接近, 8 阶只比 4 阶损失 0.2dB 的性能, 这是由于 2 阶 POLSK 的误码性能相比 2 阶和 4 阶的传统调制技术性能差别较大, 这直接影响了低阶高维星座映射方案的性能。

可以得出结论, 在传统调制技术的基础上, 引入极化状态调制, 构建高维星座映射方案, 不仅不会降低系统的传输性能, 反而会提升高阶调制方案的误码性能。当调制阶数为 4 时, 系统约损失 0.2dB 的性能。信道预编码并不会影响合法通信的误码性能。

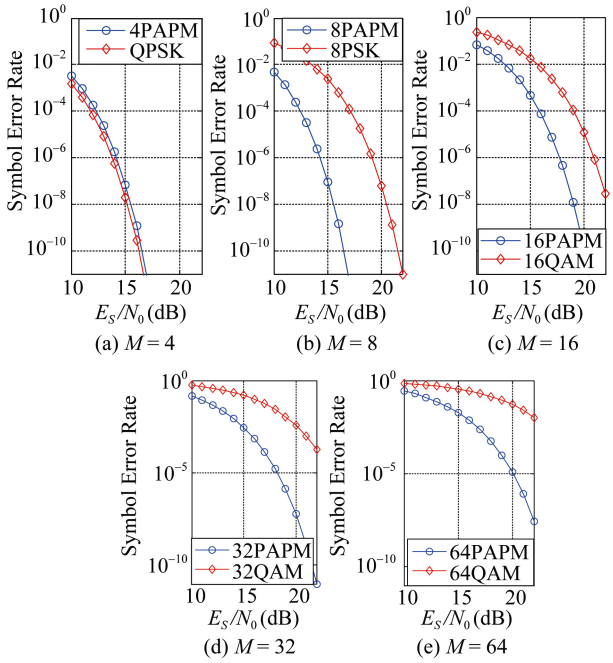


图 15 基于高维星座映射的调制技术与传统调制技术的理论误码率性能比较

Figure 15 The theoretical symbol error rate performance comparison between the proposed modulation scheme and traditional modulation scheme

5.2.2 系统实际接收误码性能分析

设置 Alice 和 Bob 相距 25m, Alice 和 Eve 相距 30m, 通过改变发射功率改变接收信噪比, 测得 Bob 和 Eve 不同调制阶数在不同接收信噪比下的误比特率性能, 记录结果见图 16。

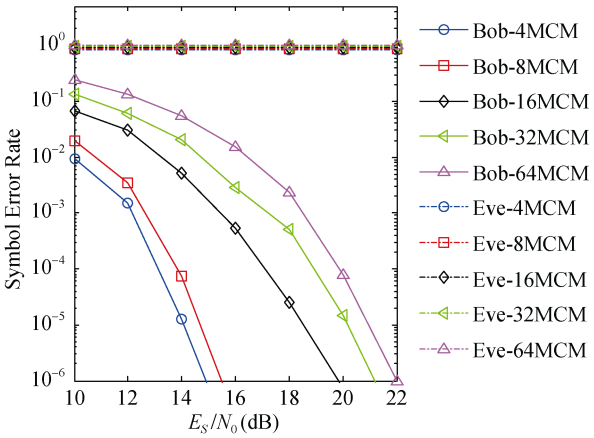


图 16 不同接收信噪比下 Bob 和 Eve 误码率性能

Figure 16 The symbol error rate performance comparison between Bob and Eve with varying RSNR

可以看出, 随着接收信噪比的增大, Bob 接收误码率降低, 但 Eve 的误码率基本保持不变, 平均误码率为 95%, 这是因为 Eve 接收信号受到了随机加扰, 即使接收信噪比增大, 也无法正确恢复信息。另外, 对于合法接收端, 实际误码率测试结果比理论误码率要高, 这是由于信道估计算法精度限制以及实际环境的复杂性导致去极化效应很难完全被消除, 但是相比同阶的传统调制技术, 误码率性能仍然有很大提升。

为测试不同信道环境下系统的安全性能, 本文还分析了 Eve 在相同接收信噪比下处于不同位置处的误码性能, 每次间隔 5m, 远远大于信号波长的一半(选择 2.4G 作为通信载波频率, 此时信号波长约为 0.125m), 结果如图 17 所示。

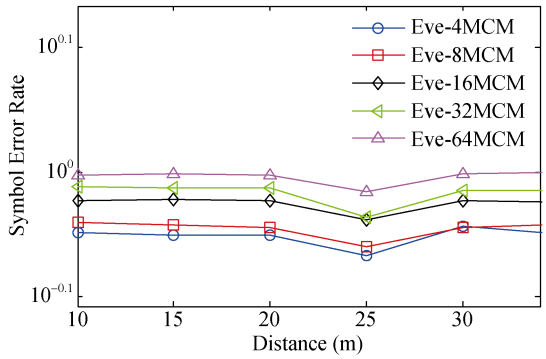


图 17 不同通信距离(信道)下 Eve 误码率性能

Figure 17 The symbol error rate performance of Eve with varying propagation distance

从图 17 可以看出, 调制阶数越高, Eve 的接收误码率越大, 这与理论分析是一致的。而且, 即使 Eve 相比距离 Alice 更近, 即与合法信道相比, 未进行预编码时的窃听信道具有更好的接收条件, 由于与合法信道相关的预编码矩阵的作用, Eve 的接收性能仍然很差。当 Eve 处于 25m, 即与 Bob 位置重叠时, 由于窃听信道与合法信道十分接近, 特定的预编码矩阵会产生信道均衡的效果, 系统的安全性能有所降低, 但由于预编码矩阵对于窃听者是随机变化的, 系统误码率仍大于 90%。

5.3 对抗调制方式识别攻击的能力

本文的高维星座映射过程是在传统调制技术的基础上, 对其进行极化加权得到水平和垂直极化分量。该部分验证了所提方案对抗基于瞬时特征的调制方式识别攻击的能力, 观察经过高维星座映射和信道预编码后, 传统调制部分对应的标量特征是否仍具备相应的特性。

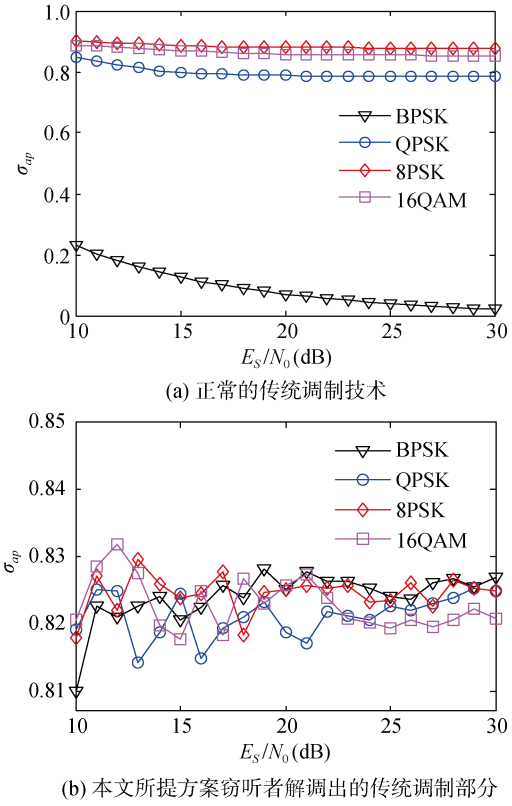
考虑到很多研究依据绝对瞬时相位信息的不同, 来区分 PSK 和 QAM 信号, 本文选择零中心瞬时相位非线性分量绝对值的标准偏差参数 σ_{ap}, 来衡量加密

前后瞬时特征参数的变化。σ_{ap} 定义如下[29]:

$$\sigma_{ap}=\sqrt{\frac{1}{N_s}\left[\sum_{i=1}^{N_s}\phi_{NL}^2(i)\right]-\left[\frac{1}{N_s}\sum_{i=1}^{N_s}\left|\phi_{NL}(i)\right|\right]^2} \tag{20}$$

式中，N_s 为采样总点数，$\phi_{NL}(i)$ 为零中心瞬时相位的非线性分量，$\phi_{NL}(i)=\phi_0(i)-\frac{1}{N_s}\sum_{i=1}^{N_s}\phi_0(i)$，$\phi_0(i)$ 为去掉线性分量后的瞬时相位。

分别计算应用本文所提方案窃听者解调出的传统调制部分和未经过高维星座映射的正常传统调制技术的 σ_{ap} 值，比较结果见图 18。



(a) 正常的传统调制技术

(b) 本文所提方案窃听者解调出的传统调制部分

图 18 信号瞬时特征参数 σ_{ap} 比较

Figure 18 The σ_{ap} acquired by Eve using proposed modulation scheme and traditional modulation scheme

图 18(a)显示了正常的传统调制信号的瞬时相位特征参数的值，可以看出，当信噪比大于 15dB 时，利用该特征能够很好地区分各类调制信号，尤其对于 MPSK 信号类内识别具有很高的识别率；图 18(b)显示了采用本文所提方案后所解调出的传统调制部分对应的瞬时特征参数，从图中可以看出，经过高维星座映射和预编码后，传统调制部分对应的各阶调制信号瞬时相位特征值已经无法区分，已经无法利用该特征识别出各类调制方式。

6 结论与下一步工作

本文提出一种基于极化状态调制的无线通信物理层安全传输技术，引入极化域，设计高维星座映射方案，并基于无线信道的去极化效应，设计随机快变的信道预编码矩阵，进一步对高维星座图进行扰乱，保障无线通信的安全传输。仿真和实验结果表明，在不降低系统误码性能的基础上，系统的安全性得到了提高。即使窃听者配置正交双极化天线，接收到的星座图仍是严重扰乱过的，对应的传统调制部分也不再具备正常传统调制技术的瞬时相位特征特点，信息具有很好的隐蔽性。

本文分析了单载波调制情况下物理层安全传输技术，实际上，该技术同样可以应用在多载波调制技术中。下一步，将针对基于极化状态调制的多载波调制信息安全防护技术展开研究。

参考文献

[1] E. Jorswieck, S. Tomasin and A. Sezgin, “Broadcasting Into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing,” in *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702-1724, Oct. 2015.

[2] Y. S. Shiu, S. Y. Chang, H. C. Wu and C. H. Huang, “Physical Layer Security in Wireless Networks: A Tutorial,” *IEEE Wireless Communications*, vol. 18, no. 2, pp. 66-74, Apr. 2011.

[3] C.E. Shannon, “Communication Theory of Secrecy Systems,” *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[4] A.D. Wyner, “The Wire-Tap Channel,” *Bell Labs Technical Journal*, vol. 54, no. 8, pp. 1355-1387, 1975.

[5] I. Csiszar, J. Korner, “Broadcast Channels with Confidential Messages,” *IEEE Transactions on Information Theory*, vol. 24, no.3, pp. 339-348, 1978.

[6] S. Leung-Yan-Cheong, M. Hellman, “The Gaussian Wire-Tap Channel,” *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451-456, 1978.

[7] A. Mukherjee, S.A.A. Fakoorian, Huang J and A.L. Swindlehurst, “Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,” *IEEE Communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550-1573, 2014.

[8] T. Wang, Y. Liu and A.V. Vasilakos, “Survey on Channel Reciprocity based Key Establishment Techniques for Wireless Systems,” *Wireless Networks*, vol. 21, no. 6, pp. 1835-1846, 2015.

[9] D. Wang, A. Hu and L. Peng, “A Novel Secret Key Generation Method in OFDM System for Physical Layer Security,” *International Journal of Interdisciplinary Telecommunications and Networking*, vol. 8, no.1, pp.21-34, 2016.

[10] H. Liu, Y. Wang, J. Yang and Y. Chen, “Fast and Practical Secret Key Extraction By Exploiting Channel Response,” in *Proceedings of International Conference on Computer Communications(INFOCOM’13)*, pp. 3048-3056, 2013.

[11] J.M. Carey and D. Grunwald, “Enhancing WLAN Security with Smart Antennas: A Physical Layer Response for Information As-

surance," *IEEE Vehicular Technology Conference(VTC'04)*, pp. 318-320, 2004.

[12] X. Li, J. Hwu and E.P. Ratazzi, "Using Antenna Array Redundancy and Channel Diversity for Secure Wireless Transmissions," *Journal of Communications*, vol. 2, pp. 3, pp.24-32, 2007.

[13] S. Goel and R. Negi, "Guaranteeing Secrecy Using Artificial Noise," *IEEE Transactions on Wireless Communications*, vol. 7, no. 6, pp. 2180-2189, 2008.

[14] Y.W.P. Hong, P.C. Lan and C.C.J. Kuo, "Signal Processing Approaches to Secure Physical Layer Communications in Multi-Antenna Wireless Systems," Springer, 2013.

[15] L. Simone, N. Salerno and M. Maffei, "Frequency-Hopping Techniques for Secure Satellite TT&C: System Analysis & Trade-offs," in *International Workshop on Satellite and Space Communications(IWSSC'06)*, pp. 13-17, 2016.

[16] M. A. Khan, M. Asim, V. Jeoti and R.S. Manzoor, "Chaos Based Constellation Scrambling in OFDM Systems: Security & Interleaving Issues," *International Symposium on Information Technology(ISIT'08)*, pp.1-7, 2008.

[17] R.F. Ma, L. Dai, Z. Wang and J. Wang, "Secure Communication in TDS-OFDM System Using Constellation Rotation and Noise Insertion," *IEEE Transactions on Consumer Electronics*, vol. 56, no. 3, pp. 1328-1332, 2010.

[18] M. Tahir, S.P. Jarot and M.U. Siddiqi, "Wireless Physical Layer Security Using Channel State Information," *International Conference on Computer and Communication Engineering (ICCCE'10)*, pp. 1-5, 2010.

[19] H. Li, X.B. Wang and W.K. Hou, "Secure Transmission in OFDM Systems by Using Time Domain Scrambling," *IEEE Vehicular Technology Conference (VTC'13)*, pp. 1-5, 2013.

[20] S. Benedetto and P. Poggiolini, "Theory of Polarization Shift Keying Modulation," *IEEE Transactions on Communications*, vol. 40, no.4, pp. 708-721, 1992.

[21] H. Bulow, "Polarization QAM Modulation (POL-QAM) for Coherent Detection Schemes," *Conference on Optical Fiber Communication(OFC'09)*, pp. 1-3, 2009.

[22] H.B. Song, "Theoretical Study of Three Dimensional Modulator and Demodulator [Ph.D. dissertation]," Fudan University: Shanghai, 2012.
(宋汉斌, "三维调制解调器的理论研究", 复旦大学: 上海, 2012.)

[23] D. Wei, C. Feng and C. Guo, "An Optimal Pre-Compensation based Joint Polarization-Amplitude- Phase Modulation Scheme for the Power Amplifier Energy Efficiency Improvement," IEEE International Conference on Communications (ICC'13), pp. 4137-4142, 2013.

[24] D. Wei, L.L. Liang, M. Zhang and C.W. Miao, "A Polarization State Modulation based Physical Layer Security Scheme for Wireless Communications," *IEEE Military Communications Conference (MILCOM'16)*, pp. 1195-1201, 2016.

[25] T. Pratt T, B. Walkenhorst B and Nguyen S, "Adaptive Polarization Transmission of OFDM Signals in Channels with Polarization Mode Dispersion and Polarization-Dependent Loss," *IEEE Transactions on Wireless Communications*, vol. 8, no. 7, pp. 3354-3359, 2009.

[26] X.B. Wu, C.L. Guo and C.Y. Feng, "Statistical Characteristic of Polarization Dependent Loss," *Wireless Communications and Networking Conference (WCNC'13)*, pp. 3426-3431, 2013.

[27] A.J. Poelman, "Virtual Polarisation Adaptation A Method of Increasing the Detection Capability of A Radar System Through Polarisation-Vector Processing," *IEEE Proceedings F-Communications, Radar and Signal Processing*, vol. 128, no.5, pp. 261-270, 1981.

[28] C.X. Fan and L.N. Cao, "Principles of Communications," National Defense Industry Press, 2006.
(樊昌信, 曹丽娜, "通信原理", 国防工业出版社, 2006.)

[29] A. K. Nandi and E.E. Azzouz, "Automatic Modulation Recognition of Communication Signals," *IEEE Trans on Communications*, vol. 46, no.4, pp.431-436, 1998.

李敏 现任中国科学院信息工程研究所, 第一工程部高级工程师。研究领域为信息保密技术、网络安全、电磁监测与防护。Email: limin@iie.ac.cn

魏冬 于 2013 年在北京邮电大学通信与信息系统专业获得博士学位。现任中国科学院信息工程研究所, 第四研究室副研究员。研究领域为无线通信物理层安全、调制识别、信号处理。Email: weidong@iie.ac.cn

梁莉莉 于 2014 年在北京科技大学通信工程专业获得学士学位。现在中国科学院信息工程研究所信息安全专业攻读硕士学位。研究领域为无线通信物理层安全、调制识别、信号处理。Email: lianglili@iie. ac.cn