文章编号：2095-4980(2021)04-0603-015

零中频数字通信发射机的射频指纹时域基带建模

俞佳宝[1]，李古月[1,2a]，胡爱群*[1,2b]

(1.网络通信与安全紫金山实验室 前沿交叉科学研究中心，江苏 南京 211111；
2.东南大学 a.网络空间安全学院；b.信息科学与工程学院，江苏 南京 210096)

摘　要：射频指纹(RFF)来源于发射机电路设计的差异和生产过程中硬件电路的制造容差，是一种新兴的设备身份识别和认证技术。对射频指纹产生机理进行建模是深入研究射频指纹技术的基础。本文根据一种通用的零中频数字通信发射机结构分析了各环节对射频指纹的影响，并建立了对应的射频指纹时域基带模型。此外，归纳总结了一系列通信标准的若干重要时域参数的容差，并着重研究了 LTE 标准下，正交相移键控(QPSK)和十六进制正交振幅调制(16-QAM)两种典型调制方式的最大均方根误差向量幅度(RMS EVM)。最后，通过理论推导和 Matlab 仿真给出了直流偏置、同相/正交(I/Q)增益不平衡、I/Q 正交偏移误差、I/Q 滤波器偏差、振荡器相噪和功放非线性参数的上下界，并分析了各种射频指纹参数临界情形下星座图的变化，为射频指纹提取和识别技术的研究提供了合理的参数指导。

关键词：物理层安全；射频指纹；时域建模；误差向量幅度；零中频

中图分类号：TP309.7　　**文献标志码：**A　　**doi：**10.11805/TKYDA2021139

Time-domain baseband modeling of Radio Frequency Fingerprint for zero-IF digital communication transmitter

YU Jiabao[1]，LI Guyue[1,2a]，HU Aiqun*[1,2b]

(1.Frontier Crossing Scientific Research Center，Purple Mountain Laboratories，Nanjing Jiangsu 211111，China；2a.School of Cyber Science and Engineering；2b.School of Information Science and Engineering，Southeast University，Nanjing Jiangsu 210096，China)

Abstract：Radio Frequency Fingerprint(RFF) originates from the differences in transmitter circuit design and the manufacturing tolerance of the hardware circuit in the production process. It is an emerging equipment identification and authentication technology. Modeling the generation mechanism of RFF is the basis for its in-depth research. Based on a general Zero Intermediate Frequency(ZIF) digital communication transmitter architecture, the influence of each component in the transmitter on RFF is analyzed, and the corresponding RFF time-domain baseband model is established as well. In addition, several important time-domain parameter tolerances of communication standards are summarized. The maximum Root Mean Square Error Vector Magnitudes(RMS EVMs) of the two typical modulation methods, Quadrature Phase Shift Keying(QPSK) and 16 Quadrature Amplitude Modulation(16-QAM), are mainly studied under the LTE standard. Finally, through theoretical derivation and Matlab simulation, the upper and lower bounds of Direct Current(DC) offset, In-Phase/Quadrature(I/Q) gain imbalance, I/Q quadrature offset error, I/Q filter offset, oscillator phase noise, and power amplifier nonlinearity parameters are given. The changes of the constellation diagram under the critical conditions of various RFF parameters are also analyzed, which provides reasonable parameter guidance for the future research of RFF extraction and identification.

Keywords：physical layer security；Radio Frequency Fingerprint(RFF)；time-domain modeling；error vector magnitude；Zero Intermediate Frequency

收稿日期：2021-04-06；**修回日期：**2021-05-19
基金项目：江苏省重点研发计划(BE2019109)；国家自然科学基金资助项目(61941115，61801115)
***通信作者：**胡爱群　email:aqhu@seu.edu.cn

近年来，物联网(Internet of Things，IoT)的发展呈现出指数级增长态势，万物互联已成为技术发展和产业应用的必然趋势。与此同时，随着第五代移动通信技术(5G)的正式商用，超高速的数据传输、超宽的无线覆盖以及超低的数据时延将促进物联网在智慧城市、智能家居、智能交通、工业互联网、智慧电网、智慧医疗等领域进一步普及和拓展，全面推动蜂窝物联网终端规模化部署和应用[1-2]。物联网主要通过接入认证和加密传输来保障空口安全。其中，接入认证用于鉴别终端身份，阻止非法终端的接入与访问，是确保空口安全的第一道防线。传统的接入认证通常是在物理层以上的环节进行的，主要是依靠存储在设备内的身份认证信息或输入的身份验证口令来阻止非法接入[3]。不幸的是，即使是安全性很强的口令和标识符，由于其纯数字性质，如果保护不当，恶意用户也可以轻松将其进行复制并进行仿冒攻击[4]。一旦非法攻击者恶意入侵成功，将给用户带来巨大的经济损失甚至人身伤害[5]。

射频指纹(RFF)技术是一种在物理层实施的接入认证方法，其利用发射机电路设计的差异和生产制造的容差导致的独特电路硬件特性。这种特性寄生在通信信号中，因此可以通过提取接收信号中的射频指纹来识别发射机终端的身份[3]。与人的指纹类似，设备的射频指纹具有唯一性且难以仿冒[6]。因此，射频指纹技术既可以用来识别和认证民用的无线通信设备，也可以用来识别军用的雷达等辐射源和通信电台，开展射频指纹提取与识别技术的研究在军事和民用领域都有着深刻的理论意义和重大的实用价值。

对射频指纹产生机理进行建模是深入研究射频指纹技术的基础，分析发射机各环节对于最终射频指纹的影响将对射频指纹特征选择起到重要指导作用。然而现有的文献对射频指纹建模鲜有研究。文献[7]从频域角度对发射机成型滤波器、放大器非线性和多径信道对射频指纹的影响做了初步研究，对于如何从频域提取射频指纹有一定指导意义。然而，该模型并未考虑时域的同相/正交(I/Q)不平衡等调制域特征，无法用于时域特征的选取。因此，为了更好地选取合适的射频指纹特征以提高识别的准确性，需要研究更加全面的射频指纹建模。

本文首先依托一种通用的零中频数字通信发射系统分析了射频指纹的产生机理，从而构建了对应的发射机时域基带射频指纹模型。然后根据现有典型通信体制的标准，归纳总结了几个重要参数的容差，并根据 LTE 标准规定的最大均方根误差向量幅度推导了 QPSK 和 16-QAM 调制下单个指纹来源参数最大容许偏差，包括直流偏置、I/Q 增益不平衡、I/Q 正交偏移误差、I/Q 滤波器偏差、振荡器相噪和功放非线性。最后，通过 Matlab 仿真各参数的临界场景，观察和分析了不同射频指纹成因对发射信号对应的星座图的影响。

1　时域基带射频指纹建模

1.1 射频指纹整体建模

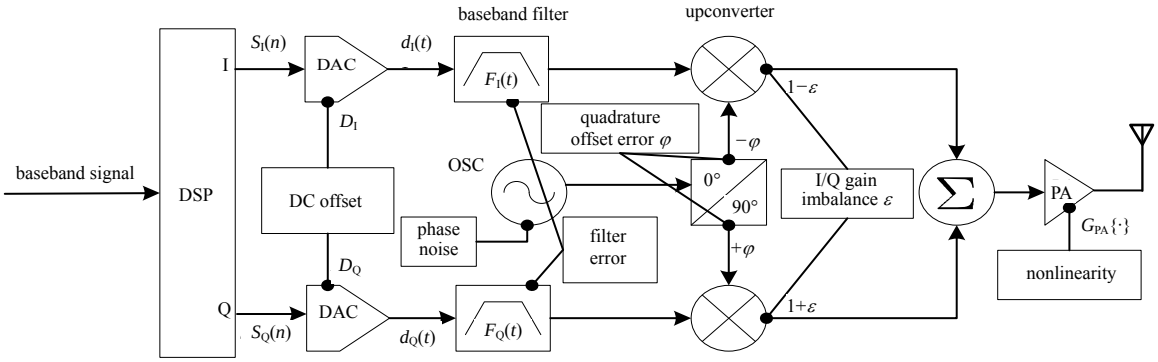


Fig.1 Radio Frequency Fingerprint modeling for zero-IF digital communication transmitters
图 1 零中频数字通信系统发射机射频指纹建模

如图 1 所示是一种典型的采用正交调制技术的零中频数字通信发射机框架，其中，发射机的模拟电路部分是射频指纹的主要引入环节。

通信系统发射机的 I/Q 两路数字基带信号 $s(n)$经过数模转换器(Digital-to-Analog Converter，DAC)成为模拟信号输出后，I/Q 两路就会分别存在直流偏置误差 D_I 和 D_Q，即 I/Q 两路存在一定的直流电平。之后，I/Q 两路的模拟信号分别经过对应的模拟基带低通滤波器 $F_I(t)$和 $F_Q(t)$，两路基带低通滤波器的频率响应误差也会寄生在信号上[8]。

经过基带滤波器的模拟信号首先需要通过混频器上变频至目标频段才能进行后续射频处理。然而，发射机混频器的载波频率和接收机的载波频率相比存在着误差，主要包括载波频率偏移误差 Δf 以及载波相位误差 ψ 。

此外，发射机的射频本振存在的相噪也会导致载波相位的抖动。载波信号通过 90°的相移，形成两组调制载波，分别用于调制 I 路和 Q 路的模拟信号。但实际电路中，I/Q 两路调制载波的相位偏差通常并不是正好 90°，存在一定的正交偏移误差φ，从而破坏了 I 路和 Q 路的正交性。同时，I/Q 两路的混频器通常也会存在增益失配ε，导致输出的 I 路和 Q 路信号的增益不平衡[9]。

最后，I 路和 Q 路的信号叠加后需要经过射频前端功率放大器(Power Amplifier，PA)放大到合适的输出功率以进行远距离的传输。功率放大器在放大信号时通常会有一定的非线性，从而导致带外的频谱增生(通常通信标准对于带外频谱能量也有规定，本文对于频域参数不做深入研究)，放大器的非线性也是影响发射机射频指纹的一个重要因素。最终，经过放大的信号通过天线辐射至空中进行发射。

1.2 I/Q 链路误差

由于本文面向零中频数字通信系统发射机展开时域基带建模研究，其 I/Q 链路误差都可以近似建模成频率无关的[8]，下面从直流偏置开始建模。

记待传输的数字复基带信号为：

$$S(n)=S_{\mathrm{I}}(n)+\mathrm{j}S_{\mathrm{Q}}(n) \tag{1}$$

式中$S_{\mathrm{I}}(n)$和$S_{\mathrm{Q}}(n)$分别为输入 DAC 的 I 路和 Q 路数字基带信号。记$S_{\mathrm{I}}(t)$、$S_{\mathrm{Q}}(t)$分别为 DAC 输出的不带直流偏置的 I/Q 两路信号，则 DAC 输出的不带直流偏置的复基带信号为：

$$S(t)=S_{\mathrm{I}}(t)+\mathrm{j}S_{\mathrm{Q}}(t) \tag{2}$$

令D_{I}、D_{Q}分别为 I/Q 两路的 DAC 直流偏置，则 DAC 输出的带直流偏置的复基带信号可表示为：

$$d(t)=d_{\mathrm{I}}(t)+\mathrm{j}d_{\mathrm{Q}}(t) \tag{3}$$

式中$d_{\mathrm{I}}(t)$和$d_{\mathrm{Q}}(t)$分别定义如下：

$$d_{\mathrm{I}}(t)=S_{\mathrm{I}}(t)+D_{\mathrm{I}} \tag{4}$$

$$d_{\mathrm{Q}}(t)=\mathrm{S}_{\mathrm{Q}}(t)+D_{\mathrm{Q}} \tag{5}$$

记 I/Q 两路的基带低通滤波器时域传递函数分别为$F_{\mathrm{I}}(t)$和$F_{\mathrm{Q}}(t)$，则两路基带低通滤波器的输出分别为：

$$X_{\mathrm{I}}^{F}(t)=F_{\mathrm{I}}(t)\otimes d_{\mathrm{I}}(t)=F_{\mathrm{I}}(t)\otimes\left(S_{\mathrm{I}}(t)+D_{\mathrm{I}}\right) \tag{6}$$

$$X_{\mathrm{Q}}^{F}(t)=F_{\mathrm{Q}}(t)\otimes d_{\mathrm{Q}}(t)=F_{\mathrm{Q}}(t)\otimes\left(S_{\mathrm{Q}}(t)+D_{\mathrm{Q}}\right) \tag{7}$$

式中⊗代表卷积运算。

接下来分析混频器上变频时 I/Q 两路的增益失配ε和相位失配φ对射频指纹的影响。首先不考虑射频本振引入的误差(在下一小节进行详细分析)，设发射机的载波频率为ω_{c}^{t}，易知进入功放的射频调制信号可表示为：

$$\begin{aligned}X_{\mathrm{p}}(t)&=(1-\varepsilon)X_{\mathrm{I}}^{F}(t)\cos\left(\omega_{\mathrm{c}}^{t}t-\varphi\right)-(1+\varepsilon)X_{\mathrm{Q}}^{F}(t)\sin\left(\omega_{\mathrm{c}}^{t}t+\varphi\right)\\&=X_{\mathrm{I}}(t)\cos\left(\omega_{\mathrm{c}}^{t}t\right)-X_{\mathrm{Q}}(t)\sin\left(\omega_{\mathrm{c}}^{t}t\right),\end{aligned} \tag{8}$$

式中$X_{\mathrm{I}}(t)$和$X_{\mathrm{Q}}(t)$分别定义如下：

$$X_{\mathrm{I}}(t)=(1-\varepsilon)F_{\mathrm{I}}(t)\otimes\left(S_{\mathrm{I}}(t)+D_{I}\right)\cos\varphi-(1+\varepsilon)F_{\mathrm{Q}}(t)\otimes\left(S_{\mathrm{Q}}(t)+D_{\mathrm{Q}}\right)\sin\varphi \tag{9}$$

$$X_{\mathrm{Q}}(t)=-(1-\varepsilon)F_{\mathrm{I}}(t)\otimes\left(S_{\mathrm{I}}(t)+D_{\mathrm{I}}\right)\sin\varphi+(1+\varepsilon)F_{\mathrm{Q}}(t)\otimes\left(S_{\mathrm{Q}}(t)+D_{\mathrm{Q}}\right)\cos\varphi \tag{10}$$

由此，I/Q 链路误差导致的失真复基带信号可表示为：

$$X^{'}(t)=X_{\mathrm{I}}(t)+\mathrm{j}X_{\mathrm{Q}}(t) \tag{11}$$

上面分别从 I 路和 Q 路出发孤立考虑各个 I/Q 链路误差对射频指纹的影响，得到式(11)所示的失真复基带信号。接下来进一步从复基带角度给出式(11)的等效数学表达。

首先根据 I/Q 两路增益失配ε和相位失配φ分别定义α和β如下：

$$\alpha=\cos\varphi+\mathrm{j}\varepsilon\sin\varphi \tag{12}$$

$$\beta=\varepsilon\cos\varphi+\mathrm{j}\sin\varphi \tag{13}$$

然后引入$\mu(t)$和$v(t)$，其数学表达式分别为：

$$\mu(t)=\frac{\alpha-\beta}{2}F_{\mathrm{I}}(t)+\frac{\alpha+\beta}{2}F_{\mathrm{Q}}(t) \tag{14}$$

$$v(t)=\frac{\alpha-\beta}{2}F_{\mathrm{I}}(t)-\frac{\alpha+\beta}{2}F_{\mathrm{Q}}(t) \tag{15}$$

由此可以得知，式(11)可以等效表达为：

$$X'(t)=\mu(t)\otimes d(t)+v(t)\otimes d^*(t) \tag{16}$$

式中 $d^*(t)$ 代表 $d(t)$ 的复共轭。

如果 I/Q 两路基带低通滤波器时域传递函数一致，即 $F_{\mathrm{I}}(t)=F_Q(t)=F(t)$，则式(14)和式(15)可以简化为：

$$\mu(t)=\alpha F(t) \tag{17}$$

$$v(t)=-\beta F(t) \tag{18}$$

由此，式(16)可以简单表示为：

$$X'(t)=\left[\alpha d(t)-\beta d^*(t)\right]\otimes F(t) \tag{19}$$

1.3 振荡器误差

不同发射机采用的射频振荡器类型不同，振荡器的性能也有很大的差异。传统的石英晶体振荡器由于其低成本在无线通信系统中最常见，其频率稳定度一般可以达到 10^{-6}~10^{-8} 数量级，甚至更高，然而其频率精确度受温漂(即频率随温度变化而显著变化)影响严重，难以单纯从制造上克服。温补晶振和恒温晶振分别采用温度补偿电路和恒温槽来补偿或降低温度变化引起的振荡器输出频率变化，进一步提高了振荡器输出频率稳定度，但其成本相对较高，在低成本的无线发射机中一般不采用。本小节为了简单起见，不考虑温漂的影响，建模分析射频振荡器引入的 3 个射频指纹参数。

由于发射机振荡器的输出载波频率和相位与接收机振荡器的输出载波频率和相位存在误差，即频率偏移误差 Δf 和相位偏移误差 ψ，记 $\Delta\omega=2\pi\Delta f$，则式(16)中的失真复基带信号进一步引入了角度为 $\Delta\omega t+\psi$ 的旋转。

$$X(t)=X'(t)\mathrm{e}^{\mathrm{j}(\Delta\omega t+\psi)}=\left[\mu(t)\otimes d(t)+v(t)\otimes d^*(t)\right]\mathrm{e}^{\mathrm{j}(\Delta\omega t+\psi)} \tag{20}$$

上式提到的频偏 Δf 和相偏 ψ 其实是统计均值，由于发射机的射频本振存在相噪，会导致载波瞬时相位的抖动，从而使得瞬时频偏和瞬时相偏与均值 Δf 和 ψ 存在一定范围的抖动。

假设相噪为 $\phi(t)$，是一个随机过程。因此，加入相噪后的复基带失真信号可以表示为：

$$X_{\mathrm{PN}}(t)=X(t)\mathrm{e}^{\mathrm{j}\phi(t)}=\left[\mu(t)\otimes d(t)+v(t)\otimes d^*(t)\right]\mathrm{e}^{\mathrm{j}\left[\Delta\omega t+\psi+\phi(t)\right]} \tag{21}$$

由于自由运行的振荡器的相噪在 $t\to\infty$ 时趋于布朗运动[8]，因此，离散的相噪 $\phi(kT_{\mathrm{s}})$ 可以建模为：

$$\phi(kT_{\mathrm{s}})=\phi\left((k-1)T_{\mathrm{s}}\right)+\Psi(k) \tag{22}$$

式中：T_{s} 为采样间隔；$\Psi(k)\sim N\left(0,\delta_\psi^2\right)$ 是独立同分布的高斯随机变量，其均值为 0，方差为 δ_ψ^2。假设信号起始是完美同步的，即 $\phi(0)=0$，则 $\phi(t)$ 是一个均值为 0，方差为 $\frac{t}{T_{\mathrm{s}}}\delta_\psi^2$ 的高斯白噪声，即：

$$\phi(t)\sim N\left(0,\frac{t}{T_{\mathrm{s}}}\delta_\psi^2\right) \tag{23}$$

1.4 功率放大器误差

严格来讲，发射机的很多部件都具有非线性，但功率放大器是最主要的非线性器件。为简单起见，本文只考虑功放的非线性，而不考虑其记忆性。这里用 $G_{\mathrm{PA}}\{\cdot\}$ 来表示功放的非线性，则发射机的整体射频指纹时域复基带模型表达为：

$$Y(t)=G_{\mathrm{PA}}\left\{X_{\mathrm{PN}}(t)\right\}=G_{\mathrm{PA}}\left\{\left[\mu(t)\otimes d(t)+v(t)\otimes d^*(t)\right]\mathrm{e}^{\mathrm{j}\left[\Delta\omega t+\psi+\phi(t)\right]}\right\} \tag{24}$$

功放的非线性主要是由幅度引起的，可以用幅度调制–幅度调制和幅度调制–相位调制来描述。此外，在无线通信系统工作的频带内，由于载波频率通常远大于调制信号带宽，因此，可以近似认为功放的非线性是频率无关的。在这种情况下，通用的两个基带非线性模型为复系数多项式模型[10]和 Saleh 模型[11]。本文选用复系数多项式模型对功放进行建模，其数学表达式为：

$$Y(t)=G_{\mathrm{PA}}\left\{X_{\mathrm{PN}}(t)\right\}=\sum_{k=1}^{N}a_k X_{\mathrm{PN}}(t)\left|X_{\mathrm{PN}}(t)\right|^{k-1} \tag{25}$$

式中：a_k 是 k 次项复系数；N 是最大非线性阶数；$Y(t)$ 是功放输出信号。通常，对于一个带通信号主要考虑的是奇次项，它们会导致带内的互调失真和带外的频谱增生，偶次项基本没有贡献。因此，去除偶次项，上式可以进一步简化为：

$$Y(t)=\sum_{k=1}^{(N-1)/2} a_{2k-1}\left[\mu(t)\otimes d(t)+v(t)\otimes d^{*}(t)\right]\mathrm{e}^{\mathrm{j}\left[\Delta\omega t+\psi+\phi(t)\right]}\left|\mu(t)\otimes d(t)+v(t)\otimes d^{*}(t)\right|^{2k-2} \tag{26}$$

2 通信标准容差

虽然可通过质量控制或预失真等措施来消除/补偿设备的硬件缺陷，但这将极大增加设备制造成本。事实上，各种通信标准都明确规定了发射机相关参数的容差，允许发射机发射信号有一定范围的波动，且几乎不影响比特数据的传输。由于常用的 WiFi 标准版本较多，不同版本的容差范围也不同，因此，为了便于比较不同 WiFi 标准之间的差异，在表 1 中归纳总结了射频指纹研究领域相关的 WiFi 标准的几个重要参数的容差。此外，对于蓝牙、ZigBee、LTE 等非 WiFi 标准，则在表 2 中进行了参数容差对比。表 1 和表 2 中的空白部分代表未对该参数进行容差规定。表中选用的这些参数与现有的指纹提取特征相关性极大，其中，载波中心频率容差规定了频偏[12]的范围，符号时钟容差则规定了时钟偏斜[13]的范围，均方根误差矢量幅度(RMS EVM)[14]则定义了调制域误差的范围，信号开/关时间规定了瞬态信号的最大长度[15]。这些不同标准容许的不同容差一定程度上反映了不同类型的设备更适合选取哪些特征作为射频指纹。例如 GSM、UMTS、LTE 等蜂窝通信标准的载波频率容差只有±0.1 ppm，显然频偏不适合作为这些设备的射频指纹特征。然而，它们的瞬态信号长度(即开关机时间)和 WiFi 设备相比，高了一个数量级，因此，正如很多文献所述[16-17]，其瞬态指纹的差异性更大，识别效果更好。

误差向量幅度(EVM)反应了多种发射机损伤所造成的误差，包含 DAC 直流偏置(即 I/Q 偏移)、I/Q 正交偏移误差、IQ 增益不平衡、相位噪声与非线性失真，可以用来评估发射机的调制精确度，从而避免用多个参数来表征发送射频信号的质量，因此是通信系统最重要的测量参数之一。

表 1 WiFi 通信标准规定的发射机参数容差

Table1 Transmitter parameter tolerance specified by WiFi communication standards

standards	carrier center frequency tolerance	symbol clock tolerance	RMS EVM	on/off time
802.11[18]	± 25 ppm	± 25 ppm	peak EVM:−9 dB, 35%	(10%−90%)2 μs
802.11b[19]	± 25 ppm	± 25 ppm	peak EVM:−9 dB, 35%	(10%−90%)2 μs
802.11a[20]	± 20 ppm(10/20 MHz)	± 20 ppm(10/20 MHz)	−5 dB, 56.2% (BPSK *R*=1/2) −8 dB, 39.8% (BPSK *R*=3/4) −10 dB, 31.6% (QPSK *R*=1/2) −13 dB, 22.4% (QPSK *R*=3/4)	
	±10 ppm(5MHz)	±10 ppm(5MHz)	−16 dB, 15.9% (16-QAM *R*=1/2) −19 dB, 11.2% (16-QAM *R*=3/4) −22 dB, 7.9% (64-QAM *R*=2/3) −25 dB, 5.6% (64-QAM *R*=3/4)	
802.11g[21]	±25 ppm	±25 ppm	−5 dB, 56.2% (BPSK *R*=1/2) −8 dB, 39.8% (BPSK *R*=3/4) −10 dB, 31.6% (QPSK *R*=1/2) −13 dB, 22.4% (QPSK *R*=3/4)	
			−16 dB, 15.9% (16-QAM *R*=1/2) −19 dB, 11.2% (16-QAM *R*=3/4) −22 dB, 7.9% (64-QAM *R*=2/3) −25 dB, 5.6% (64-QAM *R*=3/4)	
802.11n[22]	±20 ppm(5 GHz)	±20 ppm(5 GHz)	−5 dB, 56.2% (BPSK *R*=1/2) −10 dB, 31.6% (QPSK *R*=1/2) −13 dB, 22.4% (QPSK *R*=3/4) −16 dB, 15.9% (16-QAM *R*=1/2)	
	±25 ppm(2.4 GHz）	±25 ppm(2.4 GHz）	−19 dB, 11.2% (16-QAM *R*=3/4) −22 dB, 7.9% (64-QAM *R*=2/3) −25 dB, 5.6% (64-QAM *R*=3/4) −27 dB, 4.5% (64-QAM *R*=5/6)	
802.11ac[23]	±20 ppm	±20 ppm	−5 dB, 56.2% (BPSK *R*=1/2) −10 dB, 31.6% (QPSK *R*=1/2) −13 dB, 22.4% (QPSK *R*=3/4) −16 dB, 15.9% (16-QAM *R*=1/2) −19 dB, 11.2% (16-QAM *R*=3/4) −22 dB, 7.9% (64-QAM *R*=2/3) −25 dB, 5.6% (64-QAM *R*=3/4) −27 dB, 4.5% (64-QAM *R*=5/6) −30 dB, 3.2% (256-QAM *R*=3/4) −32 dB, 2.5% (256-QAM *R*=5/6)	

表 2 非 WiFi 通信标准规定的发射机参数容差

Table2 Transmitter parameter tolerance specified by non-WiFi communication standards

standards	carrier center frequency tolerance	symbol clock tolerance	modulation domain tolerance	on/off time
802.3[24]	± 50 ppm	± 50 ppm		
802.15.4[25]	± 40 ppm	± 40 ppm	peak EVM:35%	
Bluetooth[26]	± 75 kHz	± 20 ppm	modulation index:0.28−0.35	
GSM[27]	± 0.1 ppm	± 0.1 ppm	maximum phase deviation:20°	
UMTS[28]	± 0.1 ppm	± 0.1 ppm	RMS EVM:17.5%	50 μs
LTE[29]	± 0.1 ppm	± 0.1 ppm	RMS EVM:17.5% (QPSK) RMS EVM:12.5% (16-QAM) RMS EVM:7.9% (64-QAM)	20 μs

误差向量(Error Vector，EV)是实际发射信号 P_{meas} 与理想信号 P_{ref} 的矢量差，EVM 则是误差向量的幅度和参考信号的幅度的比值：

$$EVM=\frac{|EV|}{|P_{\text{ref}}|}\cdot 100\%=\frac{|P_{\text{meas}}-P_{\text{ref}}|}{|P_{\text{ref}}|}\cdot 100\% \tag{27}$$

如图 2 所示以 QPSK 为例在 I/Q 平面展示了误差向量及对应的幅度误差和相位误差。

EVM 适用于每一个发射和接收的符号。实际上，通信标准都要求在多个符号上测量 EVM，例如，EDGE 标准[27]要求要在 200 个以上的突发脉冲上测量 EVM，因此，它通常指的是 RMS EVM 或者峰值 EVM。其中，RMS EVM 定义为平均误差矢量功率 P_{error} 与平均基准功率 $P_{\text{reference}}$ 的比值的平方根：

$$RMS\ EVM=\sqrt{\frac{P_{\text{error}}}{P_{\text{reference}}}}\cdot 100\% \tag{28}$$

而峰值 EVM 则是在测量区间内出现的最大 EVM。如表 1 和表 2 所示，大部分标准规定了 RMS EVM，少部分标准(例如 IEEE 802.11b、IEEE 802.15.4 等)则规定了最大峰值 EVM。此外，可以指定百分比(%)或分贝(dB)为 EVM 单位，例如 IEEE 802.11a/g 测量的 RMS EVM 是以分贝为单位，而 IEEE 802.11b 的峰值 EVM 是以百分比为单位，在表 1 和表 2 中已经进行了换算，同时列出了两种单位下的 EVM 值，换算公式如下：

$$EVM\left(\text{dB}\right)=20\log_{10}\left(\frac{EVM\left(\%\right)}{100\left(\%\right)}\right) \tag{29}$$

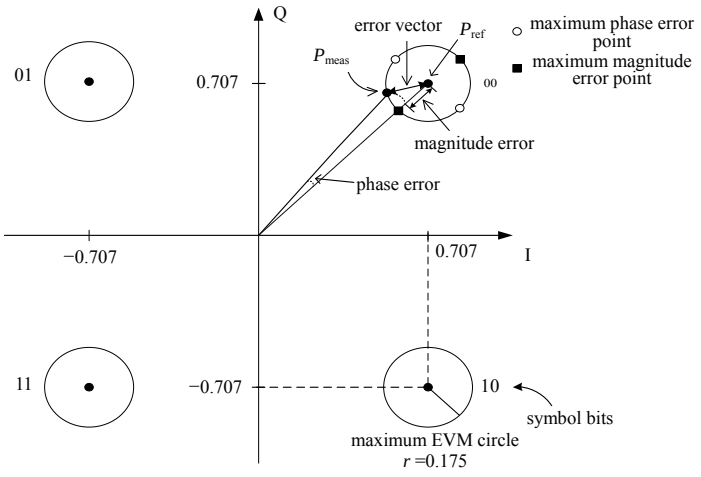


Fig.2 Schematic diagram of modulation domain error for QPSK

图 2 QPSK 调制域误差示意图

3　时域基带射频指纹模型仿真与分析

3.1 直流偏置的影响

若只考虑 DAC 直流偏置对于射频指纹的影响，则式(26)简化为：

$$Y\left(t\right)=d\left(t\right)=S_{\text{I}}\left(t\right)+D_{\text{I}}+\text{j}\left(S_{\text{Q}}\left(t\right)+D_{\text{Q}}\right) \tag{30}$$

由此可知，误差向量幅度为：

$$EVM\left(t\right)=\frac{|Y\left(t\right)-S\left(t\right)|}{|S\left(t\right)|}\cdot 100\%=\frac{\sqrt{D_{\text{I}}^2+D_{\text{Q}}^2}}{|S\left(t\right)|}\cdot 100\% \tag{31}$$

根据表 2 中 LTE 标准可知，QPSK 调制方式和 16-QAM 调制方式对应的最大 RMS EVM 分别为 17.5%和 12.5%，接下来依次推算最大容许的直流偏置范围。

3.1.1QPSK 调制

对于恒包络的 QPSK 调制而言，由于 $|S\left(t\right)|=1$，因此，

$$RMS\ EVM\leqslant 17.5\%\Leftrightarrow\sqrt{D_{\text{I}}^2+D_{\text{Q}}^2}\leqslant 0.175 \tag{32}$$

即：

$$D_{\mathrm{I}}^2+D_{\mathrm{Q}}^2\leqslant 0.175^2 \tag{33}$$

3.1.2 16-QAM 调制

图 3 为 16-QAM 调制的星座图，为了便于和 QPSK 进行比较，将其功率也归一化到 1。则其星座点幅度存在 3 种情形，最内圈四点幅度为 $\frac{1}{\sqrt{5}}$，中圈八点幅度为 1，最外圈四点幅度为 $\sqrt{\frac{9}{5}}$。因此，

$$RMS\ \ EVM\leqslant 12.5\%\Leftrightarrow\frac{\sqrt{D_{\mathrm{I}}^2+D_{\mathrm{Q}}^2}}{\sqrt{mean\left(\left|S(t)\right|^2\right)}}\leqslant 0.125 \tag{34}$$

式中 $mean(\cdot)$ 代表取平均值，由于 $mean\left(\left|S(t)\right|^2\right)=1$，式(34)可以进一步简化为：

$$D_{\mathrm{I}}^2+D_{\mathrm{Q}}^2\leqslant 0.125^2 \tag{35}$$

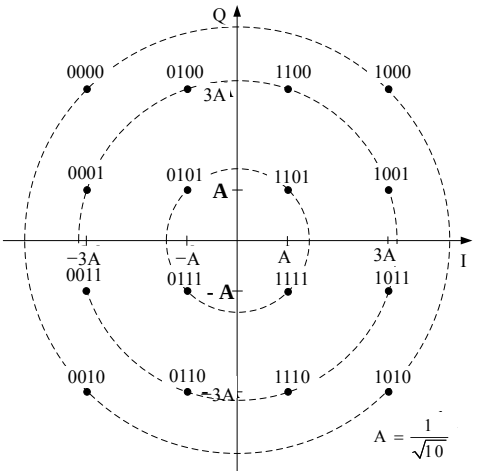
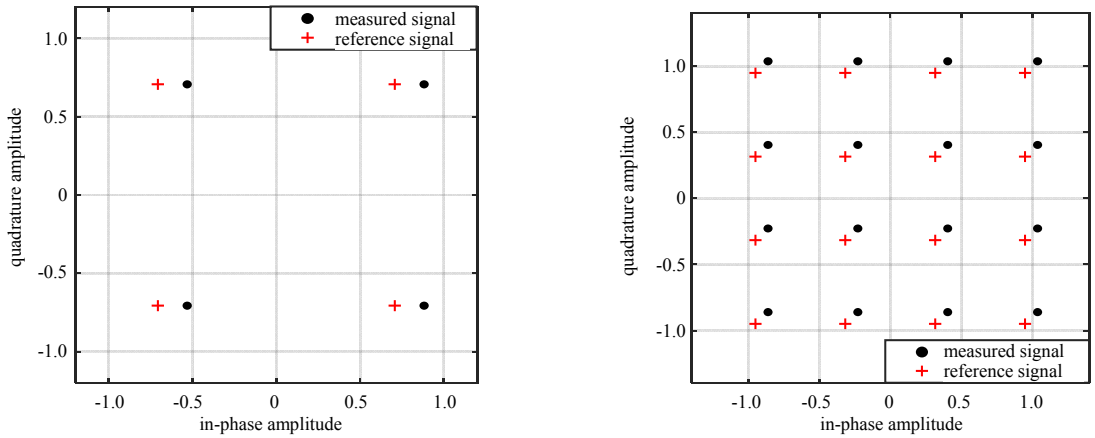


Fig.3 Constellation graph for 16-QAM

图 3 16-QAM 星座图

3.1.3 星座图变化

图 4 展示了 QPSK 在 $D_{\mathrm{I}}=0.175, D_{\mathrm{Q}}=0$ 和 16-QAM 在 $D_{\mathrm{I}}=0.088, D_{\mathrm{Q}}=0.088$ 这两种极端情形下(即 RMS EVM 分别为 0.175 和 0.125)信号星座图的变化。可以看出，直流偏置导致 QPSK 和 16-QAM 的星座点沿着 I 轴向右平移了 D_{I}，沿着 Q 轴向上平移了 D_{Q}，整体形状依然保持不变，相当于理想星座图的原点(0,0)移动到了(D_{I} , D_{Q})，因此，DAC 直流偏置也被称为 I/Q 偏移。



(a) QPSK, D_{I} = 0.175, D_{Q}=0　　(b) 16-QAM, D_{I} = 0.088, D_{Q}=0.088

Fig.4 Influence of DC offset on QPSK and 16-QAM constellation diagrams

图 4 直流偏置对 QPSK 和 16-QAM 星座图的影响

3.2 I/Q 增益不平衡的影响

若只考虑 I/Q 增益不平衡对于射频指纹的影响，则式(26)简化为：

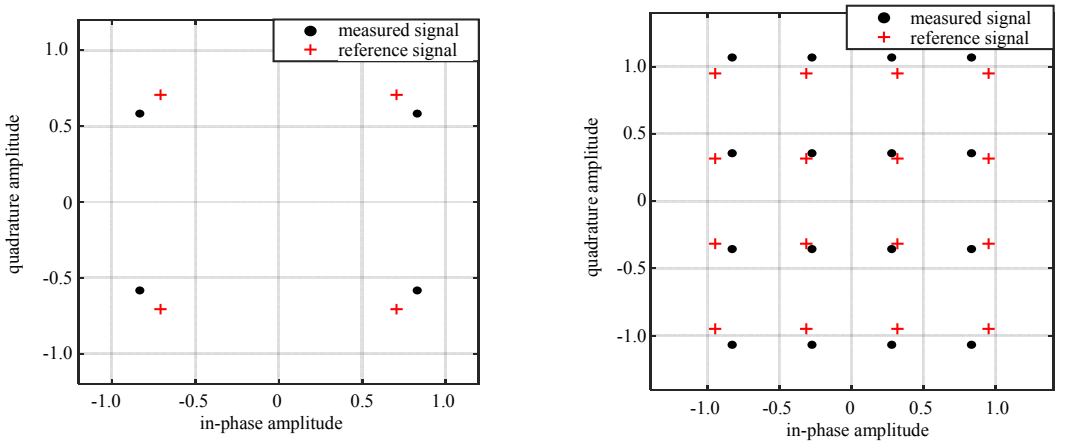
$$Y(t)=(1+\varepsilon)S_{\mathrm{I}}(t)+\mathrm{j}(1-\varepsilon)S_{\mathrm{Q}}(t) \tag{36}$$

由此可知，误差向量幅度为：

$$EVM(t)=\frac{\left|Y(t)-S(t)\right|}{\left|S(t)\right|}\cdot 100\%=\left|\varepsilon\right| \tag{37}$$

因此，对于 QPSK 而言，要求 $\left|\varepsilon\right|\leqslant 0.175$；对于 16-QAM，则要求 $\left|\varepsilon\right|\leqslant 0.125$。

图 5 展示了 QPSK 在 ε=0.175 和 16-QAM 在 ε=−0.125 这两种极端情形下信号星座图的变化。显然，若 I/Q 增益不平衡 ε 为正，星座点会沿着 I 轴拉伸 ε 倍，沿着 Q 轴收缩 ε 倍，整个星座图变成了一个长方形；反之，若 I/Q 增益不平衡 ε 为负，星座点会沿着 I 轴收缩 $-\varepsilon$ 倍，沿着 Q 轴拉伸 $-\varepsilon$ 倍。



(a) QPSK, $\varphi=0.175$　　(b) 16-QAM, $\varphi=-0.125$

Fig.5 Influence of I/Q gain imbalance on QPSK and 16-QAM constellation diagrams

图 5 I/Q 增益不平衡对 QPSK、16-QAM 星座图的影响

3.3 I/Q 正交偏移误差的影响

若只考虑 I/Q 正交偏移误差(I/Q 相位不平衡)对于射频指纹的影响，则式(26)简化为：

$$Y(t)=\cos\varphi S(t)-\mathrm{j}\sin\varphi S^{*}(t)=S(t)\mathrm{e}^{-\mathrm{j}\varphi} \tag{38}$$

由此可知，误差向量幅度为：

$$EVM(t)=\frac{|Y(t)-S(t)|}{|S(t)|}\cdot 100\%=\frac{\left|\left((\cos\varphi-1)S_I(t)+\sin\varphi S_Q(t)\right)+\mathrm{j}\left((\cos\varphi-1)S_Q(t)-\sin\varphi S_I(t)\right)\right|}{|S_{\mathrm{I}}(t)+\mathrm{j}S_{\mathrm{Q}}(t)|}=2\left|\sin\frac{\varphi}{2}\right| \tag{39}$$

因此，对于 QPSK 而言，要求：

$$2\left|\sin\frac{\varphi}{2}\right|\leqslant 0.175\Leftrightarrow|\varphi|\leqslant 0.1752 \tag{40}$$

对于 16-QAM，则要求：

$$2\left|\sin\frac{\varphi}{2}\right|\leqslant 0.125\Leftrightarrow|\varphi|\leqslant 0.1251 \tag{41}$$

因此，文献[9]在对不同阶数的 QAM(最高为 64-QAM)和不同阶数的 MPSK 信号(最高为 8PSK)仿真时设置的相同的相位不平衡参数范围，[−10°,10°](即[−0.1744,0.1744])是不合理的。除了 BPSK 和 QPSK 两种调制，其他调制方式在部分参数值对应的 RMS EVM 已经超出了标准规定的最大 RMS EVM，并不是对实际通信设备射频指纹的合理假设与仿真。

图 6 展示了 QPSK 在φ=0.175 2 和 16-QAM 在φ=−0.1251 这两种极端情形下信号星座图的变化。显然，若 I/Q 交偏移误差φ为正，原来的正方形星座图会沿着 $\frac{\pi}{4}$ 的对角线收缩 $2\left|\sin\frac{\varphi}{2}\right|$ 倍，沿着 $-\frac{\pi}{4}$ 的对角线拉伸 $2\left|\sin\frac{\varphi}{2}\right|$ 倍；反之，若 I/Q 交偏移误差 φ 为负，原来的正方形星座图则会沿着 $\frac{\pi}{4}$ 的对角线拉伸 $2\left|\sin\frac{\varphi}{2}\right|$ 倍，沿着 $-\frac{\pi}{4}$ 的对角线收缩 $2\left|\sin\frac{\varphi}{2}\right|$ 倍。

3.4 I/Q 两路低通滤波器偏差的影响

若只考虑 I/Q 两路低通滤波器偏差对于射频指纹的影响，则式(26)简化为：

$$Y(t)=F_{\mathrm{I}}(t)\otimes S_{\mathrm{I}}(t)+F_{\mathrm{Q}}(t)\otimes S_{\mathrm{Q}}(t) \tag{42}$$

在 Matlab 中仿真时，设定采样间隔为符号持续时间的 1/10，$T_{\mathrm{s}}=\frac{1}{10}T_{\mathrm{sym}}$，即每个符号采 10 个点，则上式可以离散化为：

$$Y(n)=F_{\mathrm{I}}(n)\otimes S_{\mathrm{I}}(n)+F_{\mathrm{Q}}(n)\otimes S_{\mathrm{Q}}(n) \tag{43}$$

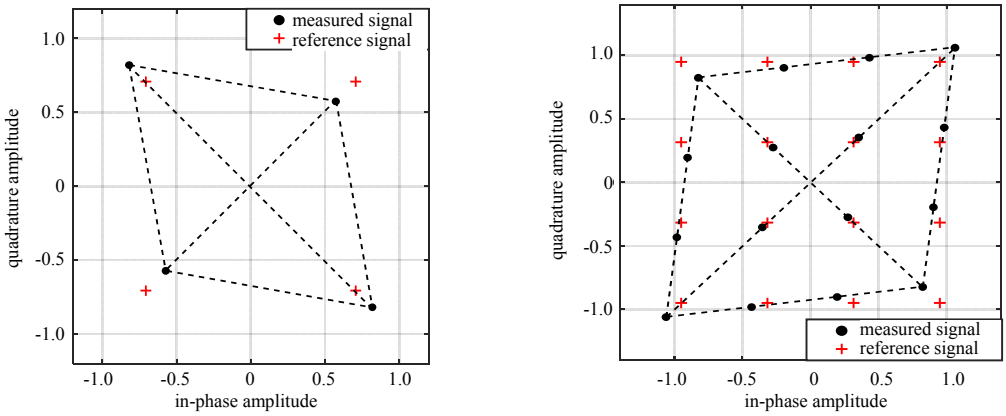
式中 $F_{\mathrm{I}}(n)$ 和 $F_{\mathrm{Q}}(n)$ 是 $F_{\mathrm{I}}(t)$ 和 $F_{\mathrm{Q}}(t)$ 的 K 阶数字近似，对应的 z 域传递函数分别为：

$$H_{\mathrm{I}}(z)=\left(1+h_0^{\mathrm{I}}\right)+h_1^{\mathrm{I}}z^{-1}+\cdots+h_K^{\mathrm{I}}z^{-K} \tag{44}$$

$$H_{\mathrm{Q}}(z)=\left(1+h_0^{\mathrm{Q}}\right)+h_1^{\mathrm{Q}}z^{-1}+\cdots+h_K^{\mathrm{Q}}z^{-K} \tag{45}$$

由此可知，对应的单点误差向量幅度为：

$$EVM(n)=\frac{\left|Y(n)-S(n)\right|}{\left|S(n)\right|}\cdot 100\%=\frac{\left|\sum_{i=0}^{K}h_i^{\mathrm{I}}S_{\mathrm{I}}(n-i)+\mathrm{j}\sum_{i=0}^{K}h_i^{\mathrm{Q}}S_{\mathrm{Q}}(n-i)\right|}{\left|S(n)\right|} \tag{46}$$



(a) QPSK, $\varphi=0.175\ 2$ (b) 16-QAM, $\varphi=-0.125\ 1$

Fig.6 Influence of I/Q quadrature offset on QPSK and 16-QAM constellation diagrams

图 6 I/Q 正交偏移误差对 QPSK、16-QAM 星座图的影响

3.4.1 QPSK 调制

对于 QPSK 调制而言，由于 $\left(S_{\mathrm{I}}(n)\right)^2=\left(S_{\mathrm{Q}}(n)\right)^2=\frac{1}{2}$，因此，式(46)可以化简为：

$$\begin{aligned}EVM_{\mathrm{QPSK}}(n)&=\left(\sum_{i=0}^{K}\sum_{k=0}^{K}h_i^{\mathrm{I}}h_k^{\mathrm{I}}sgn\left(S_{\mathrm{I}}(n-i)S_{\mathrm{I}}(n-k)\right)\left|S_{\mathrm{I}}(n-i)S_{\mathrm{I}}(n-k)\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}h_i^{\mathrm{Q}}h_k^{\mathrm{Q}}sgn\left(S_{\mathrm{Q}}(n-i)S_{\mathrm{Q}}(n-k)\right)\left|S_{\mathrm{Q}}(n-i)S_{\mathrm{Q}}(n-k)\right|\right)^{\frac{1}{2}}\\&\leqslant\frac{\sqrt{2}}{2}\sqrt{\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{I}}\right|\left|h_k^{\mathrm{I}}\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{Q}}\right|\left|h_k^{\mathrm{Q}}\right|}\end{aligned} \tag{47}$$

式中符号函数 $sgn(\cdot)$ 定义如下：

$$sgn(x)=\begin{cases}1, & x>0\\0, & x=0\\-1, & x<0\end{cases} \tag{48}$$

因此，对于 QPSK 调制，要求：

$$\frac{\sqrt{2}}{2}\sqrt{\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{I}}\right|\left|h_k^{\mathrm{I}}\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{Q}}\right|\left|h_k^{\mathrm{Q}}\right|}\leqslant 0.175\Leftrightarrow\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{I}}\right|\left|h_k^{\mathrm{I}}\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{Q}}\right|\left|h_k^{\mathrm{Q}}\right|\leqslant\frac{49}{800} \tag{49}$$

若 K=1，即只考虑一阶有限脉冲响应(Finite Impulse Response，FIR)滤波器，则上式简化为：

$$\left(\left|h_0^{\mathrm{I}}\right|+\left|h_1^{\mathrm{I}}\right|\right)^2+\left(\left|h_0^{\mathrm{Q}}\right|+\left|h_1^{\mathrm{Q}}\right|\right)^2\leqslant\frac{49}{800}, \tag{50}$$

等号当且仅当 $sgn\left(h_0^I h_1^I\right)=sgn\left(S_I(n)S_I(n-1)\right)$，$sgn\left(h_0^Q h_1^Q\right)=sgn\left(S_Q(n)S_Q(n-1)\right)$ 时成立。

3.4.2 16-QAM 调制

对于 16-QAM 而言，由于 $\left|S_{\mathrm{I}}(n)\right|$ 和 $\left|S_{\mathrm{Q}}(n)\right|$ 有两种取值：$\frac{1}{\sqrt{10}}$ 和 $\frac{3}{\sqrt{10}}$，因此，式(46)可以化简为：

$$\begin{aligned}EVM_{\mathrm{QAM}}(n)&=\left(\sum_{i=0}^{K}\sum_{k=0}^{K}h_i^{\mathrm{I}}h_k^{\mathrm{I}}sgn\left(S_{\mathrm{I}}(n-i)S_{\mathrm{I}}(n-k)\right)\left|S_{\mathrm{I}}(n-i)S_{\mathrm{I}}(n-k)\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}h_i^{\mathrm{Q}}h_k^{\mathrm{Q}}sgn\left(S_{\mathrm{Q}}(n-i)S_{\mathrm{Q}}(n-k)\right)\left|S_{\mathrm{Q}}(n-i)S_{\mathrm{Q}}(n-k)\right|\right)^{\frac{1}{2}}\\&\leqslant\frac{9}{10}\sqrt{\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{I}}\right|\left|h_k^{\mathrm{I}}\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{Q}}\right|\left|h_k^{\mathrm{Q}}\right|}\end{aligned} \tag{51}$$

因此，对于 16-QAM 调制，要求：

$$\frac{9}{10}\sqrt{\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{I}}\right|\left|h_k^{\mathrm{I}}\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{Q}}\right|\left|h_k^{\mathrm{Q}}\right|}\leqslant 0.125\Leftrightarrow\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{I}}\right|\left|h_k^{\mathrm{I}}\right|+\sum_{i=0}^{K}\sum_{k=0}^{K}\left|h_i^{\mathrm{Q}}\right|\left|h_k^{\mathrm{Q}}\right|\leqslant\left(\frac{5}{36}\right)^2 \tag{52}$$

若 K=1，即只考虑一阶 FIR 滤波器，则上式简化为：

$$\left(\left|h_0^{\mathrm{I}}\right|+\left|h_1^{\mathrm{I}}\right|\right)^2+\left(\left|h_0^{\mathrm{Q}}\right|+\left|h_1^{\mathrm{Q}}\right|\right)^2\leqslant\left(\frac{5}{36}\right)^2 \tag{53}$$

等号当且仅当 $sgn\left(h_0^{\mathrm{I}}h_1^{\mathrm{I}}\right)=sgn\left(S_{\mathrm{I}}(n)S_{\mathrm{I}}(n-1)\right)$，$sgn\left(h_0^{\mathrm{Q}}h_1^{\mathrm{Q}}\right)=sgn\left(S_{\mathrm{Q}}(n)S_{\mathrm{Q}}(n-1)\right)$，$\left|S_{\mathrm{I}}(n)\right|=\left|S_{\mathrm{Q}}(n)\right|=\left|S_{\mathrm{I}}(n-1)\right|=\left|S_{\mathrm{Q}}(n-1)\right|=\frac{3}{\sqrt{10}}$ 时成立。

3.4.3 星座图变化

图 7 和图 8 分别展示了 QPSK 和 16-QAM 在多种一阶 I/Q 滤波器极端参数下信号星座图的变化。显然，当 I/Q 滤波器只有零阶参数时，只会改变 I/Q 两路的增益。如图 7(a)和 8(a)所示，当 h_0^{I} 与 h_0^{Q} 都为正时，整个星座图沿着 I 路和 Q 路分别拉伸了 h_0^{I} 与 h_0^{Q} 倍；反之，当 h_0^{I} 与 h_0^{Q} 都为负时，整个星座图沿着 I 路和 Q 路分别压缩了 h_0^{I} 与 h_0^{Q} 倍。而当 h_0^{I} 与 h_0^{Q} 一正一负时，则会沿着一个方向拉伸，沿着另一个方向压缩。特殊情况下，若 $h_0^{\mathrm{I}}=-h_0^{\mathrm{Q}}$，则等同于 I/Q 增益不平衡 $\varepsilon=h_0^{\mathrm{I}}$ 造成的效果，可以看到图 7(b)与图 5(a)中的星座图变化完全一致。

滤波器的一阶参数以及更高阶参数则会引入符号间干扰，导致星座点的扩散，如图 7(c)、7(d)、8(c)和 8(d)所示。对于 QPSK 而言，由于单路符号的取值只有两种，因此一路非零一阶参数会导致原来的一个星座点扩散成两个点，如果 I/Q 两路都存在非零一阶参数，则会扩散成 4 个星座点。对于 16-QAM 而言，由于单路符号的取值有 4 种，因此，一路非零一阶参数会导致原来的一个星座点扩散成 4 个点，如果 I/Q 两路都存在非零一阶参数，则会扩散成 16 个星座点。

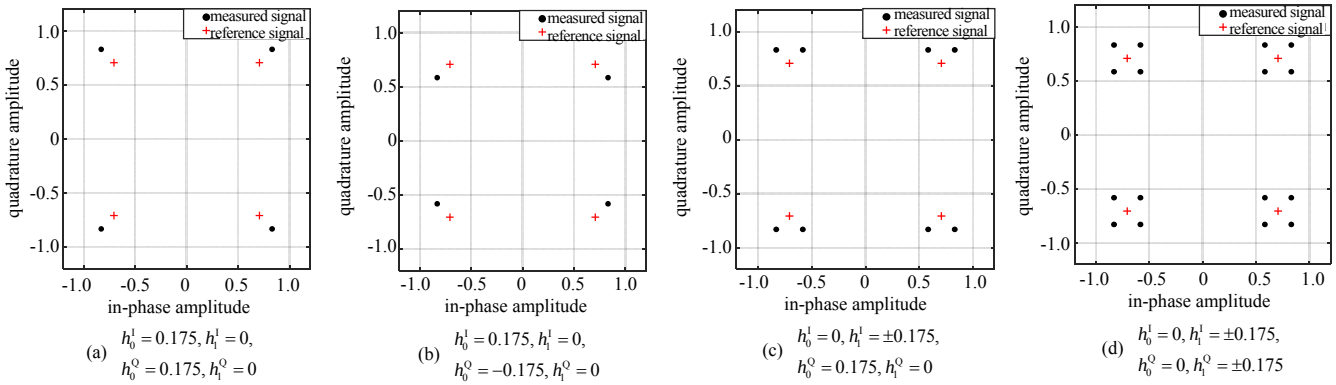


Fig.7 Influence of first-order I/Q filters on QPSK constellation diagrams

图 7 一阶 I/Q 滤波器对 QPSK 星座图的影响

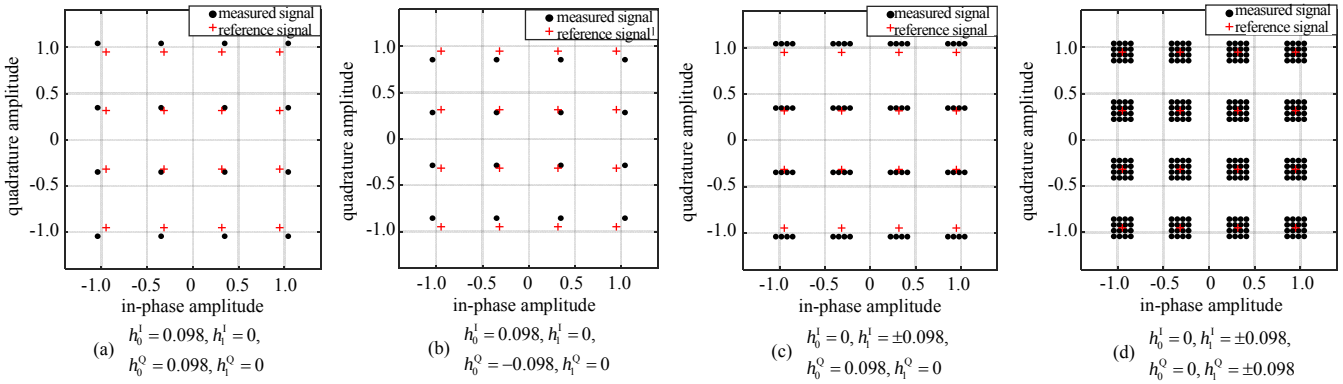


Fig.8 Influence of first-order I/Q filters on 16-QAM constellation diagrams

图 8 一阶 I/Q 滤波器对 16-QAM 星座图的影响

3.5 振荡器相位噪声的影响

若只考虑射频振荡器相噪对于射频指纹的影响，则式(26)简化为：

$$Y(t)=S(t)\mathrm{e}^{\mathrm{j}\phi(t)},\quad \phi(t)\sim N\left(0,\frac{t}{T_\mathrm{s}}\delta_\psi^2\right) \tag{54}$$

由此可知，误差向量幅度为：

$$EVM(t)=\frac{\left|\left(\left(\cos\phi(t)-1\right)S_\mathrm{I}(t)-\sin\phi(t)S_\mathrm{Q}(t)\right)+\mathrm{j}\left(\left(\cos\phi(t)-1\right)S_\mathrm{Q}(t)+\sin\phi(t)S_\mathrm{I}(t)\right)\right|}{\left|S_\mathrm{I}(t)+\mathrm{j}S_\mathrm{Q}(t)\right|}=2\left|\sin\frac{\phi(t)}{2}\right| \tag{55}$$

因此，对于 QPSK 而言，要求：

$$RMS\ EVM=\frac{1}{T}\int_0^T\left(2\left|\sin\frac{\phi(t)}{2}\right|\right)^2\mathrm{d}t\leqslant 0.175 \tag{56}$$

式中 T 代表测量 RMS EVM 的信号持续时间。在 $|\phi(t)|<0.35$ 时，可以认为 $\sin\phi(t)\approx\phi(t)$，则上式可以变为：

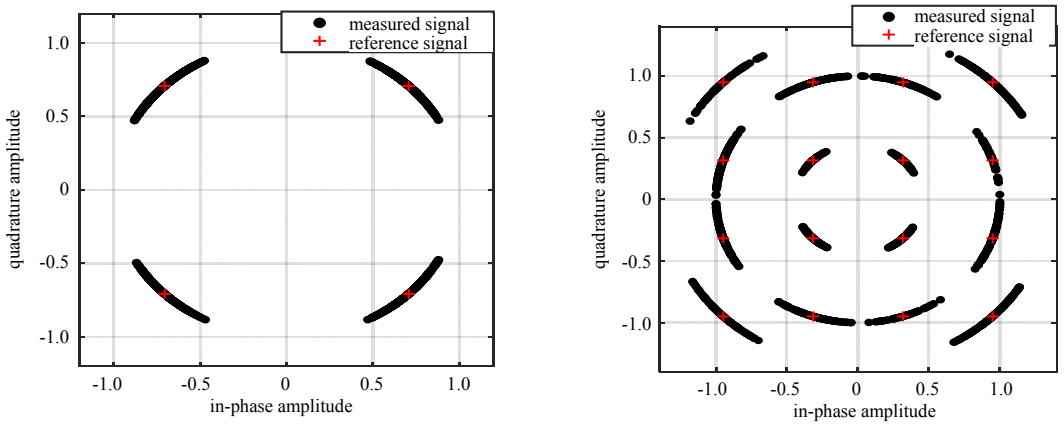
$$RMS\ EVM\approx\frac{1}{T}\int_0^T\phi(t)^2\mathrm{d}t\leqslant 0.175 \tag{57}$$

同理易知对于 16-QAM，则要求：

$$RMS\ EVM\approx\frac{1}{T}\int_0^T\phi(t)^2\mathrm{d}t\leqslant 0.125 \tag{58}$$

由于式(57)和式(58)中的 EVM RMS 近似服从广义卡方分布，没有闭式解，因此本文参照 EDGE 标准，通过 Matlab 仿真测试 200 个符号来计算 RMS EVM。每个符号采 10 个点，对 QPSK 和 16-QAM 分别进行 10 000 次仿真，计算不同相噪系数 δ_ψ^2 下的平均 RMS EVM。

仿真结果显示，在 $\delta_\psi^2=1.155\mathrm{e}^{-4}$ 时，QPSK 的平均 RMS EVM 为 17.5%，因此，粗略判定对于 QPSK 而言，要求 $\delta_\psi^2\leqslant 1.155\mathrm{e}^{-4}$。在 $\delta_\psi^2=5.88\mathrm{e}^{-5}$ 时，QPSK 的平均 RMS EVM 为 12.5%，因此，粗略判定对于 16-QAM 而言，要求 $\delta_\psi^2\leqslant 5.88\mathrm{e}^{-5}$。两种调制方式在各自极端情形下信号星座图的变化如图 9 所示，相噪导致原来的星座点沿着同幅度的圆随机向两侧发散，尤其对于仿真测试的 16-QAM 场景而言，在 RMS EVM 逼近标准上限时，幅度为 1 的 8 个星座点已经接近解调出错。



(a) QPSK, $\delta_\psi^2=1.155\mathrm{e}^{-4}$　　(a) 16-QAM, $\delta_\psi^2=5.88\mathrm{e}^{-5}$

Fig.9 Influence of oscillator phase noise on QPSK and 16-QAM constellation diagrams

图 9 振荡器相噪对 QPSK、16-QAM 星座图的影响

3.6 功放非线性的影响

若只考虑功放非线性对于射频指纹的影响，则式(26)简化为：

$$Y(t)=\sum_{k=1}^{(N-1)/2}a_{2k-1}S(t)\left|S(t)\right|^{2k-2} \tag{59}$$

由此可知，误差向量幅度为：

$$EVM(t)=\frac{\left|\left(\sum_{k=1}^{(N-1)/2}a_{2k-1}\left|S(t)\right|^{2k-2}-1\right)S(t)\right|}{\left|S(t)\right|}=\left|\sum_{k=1}^{(N-1)/2}a_{2k-1}\left|S(t)\right|^{2k-2}-1\right| \tag{60}$$

3.6.1QPSK 调制

对于 QPSK 而言，由于$|S(t)|=1$，上式可以化简为：

$$EVM_{\mathrm{QPSK}}(t)=\left|\sum_{k=1}^{(N-1)/2}a_{2k-1}-1\right| \tag{61}$$

因此，对于 QPSK 调制，要求：

$$\left|\sum_{k=1}^{(N-1)/2}a_{2k-1}-1\right|\leqslant 0.175 \tag{62}$$

由于无线通信设备功率相对较小，一般呈弱非线性，因此，可以假设忽略七次及以上非线性项，即只考虑非线性阶数 $N\leqslant 5$，则上式可以进一步简化为：

$$|a_1+a_3+a_5-1|\leqslant 0.175 \tag{63}$$

3.6.2 16-QAM 调制

对于 16-QAM 而言，由于$|S(t)|^2$有 3 种取值，$\frac{1}{5}$，1 和$\frac{9}{5}$，因此，式(60)可以化简为：

$$EVM_{\mathrm{QAM}}(t)=\begin{cases}\left|\sum_{k=1}^{(N-1)/2}\frac{a_{2k-1}}{5^{k-1}}-1\right|, & |S(t)|^2=\frac{1}{5}\\ \left|\sum_{k=1}^{(N-1)/2}a_{2k-1}-1\right|, & |S(t)|^2=1\\ \left|\sum_{k=1}^{(N-1)/2}\frac{a_{2k-1}\cdot 9^{k-1}}{5^{k-1}}-1\right|, & |S(t)|^2=\frac{9}{5}\end{cases} \tag{64}$$

因此，对于 16-QAM 调制，要求：

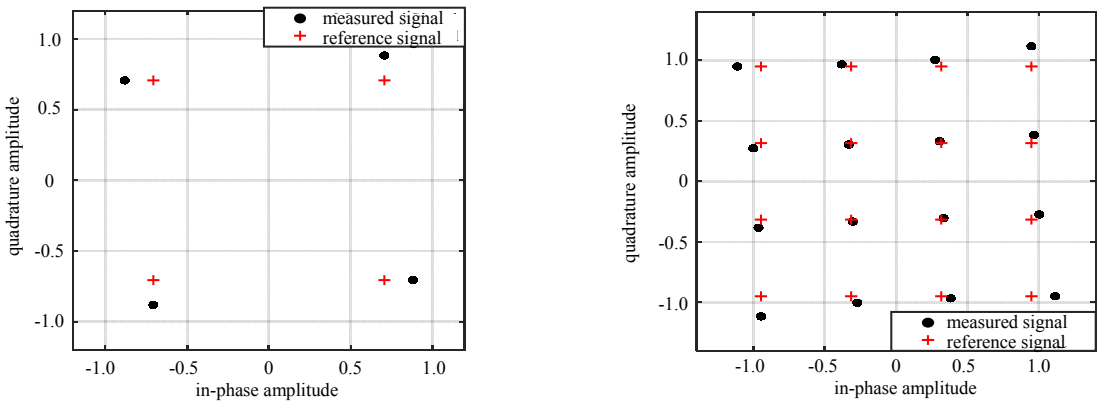
$$max\left\{\left|\sum_{k=1}^{(N-1)/2}\frac{a_{2k-1}}{5^{k-1}}-1\right|,\left|\sum_{k=1}^{(N-1)/2}a_{2k-1}-1\right|,\left|\sum_{k=1}^{(N-1)/2}\frac{a_{2k-1}\cdot 9^{k-1}}{5^{k-1}}-1\right|\right\}\leqslant 0.125 \tag{65}$$

式中 $max\{\cdot\}$ 代表取最大值函数。同样地，若只考虑非线性阶数 $N\leqslant 5$，则上式可以进一步简化为：

$$max\left\{\left|a_1+\frac{a_3}{5}+\frac{a_5}{25}-1\right|,|a_1+a_3+a_5-1|,\left|a_1+\frac{9}{5}a_3+\frac{81}{25}a_5-1\right|\right\}\leqslant 0.125 \tag{66}$$

3.6.3 星座图变化

图 10 展示了 QPSK 和 16-QAM 在两种功率放大器极端参数下信号星座图的变化。显然，正交调制信号经放大器放大后，将引起信号幅度和相位的失真，在星座图上表现为星座点散布，星座图扭曲变形，同时伴随着相位旋转。对于 QPSK 而言，各个点的相位旋转一致，因此，其相位旋转可以在载波相位同步时进行补偿。而对于 16-QAM 而言，由于其星座点存在 3 种不同的幅度，因此，可以观察到星座点的幅度偏差也有 3 种，正如式(64)所述。同样的，不同幅度的星座点旋转角度也不一致，导致不能由载波相位同步完全补偿。



(a) QPSK, a_1=1+0.248j, a_3=0.062, a_5=0.062−0.124j

(b) 16-QAM, a_1=1+0.044j, a_3=0.024 4, a_5=0.013 6+0.013 6j

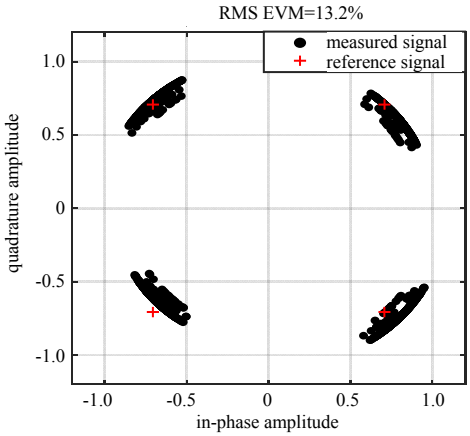
Fig.10 Influence of power amplifier nonlinearity on QPSK and 16-QAM constellation diagrams

图 10 功放非线性对 QPSK、16-QAM 星座图的影响

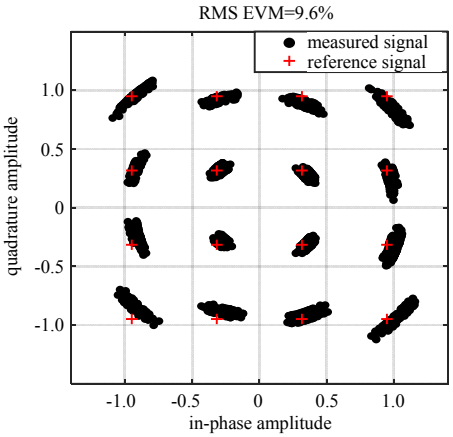
3.7 混合参数的影响

本章前面几小节研究了单个射频指纹来源参数对于星座图的影响，可以看到，大部分单参数对于星座图的影响还相对比较容易分析。因此，针对只有一个参数对射频指纹产生了影响，而其他参数均不引入指纹的情形，可以从星座图推出直流偏置、I/Q 增益不平衡、I/Q 相位不平衡等部分单参数的值。许多现有文献也是通过假设只有单参数产生影响，根据星座图来估计参数的值。例如文献[14]依次估计了设备的 I/Q 增益不平衡、I/Q 相位不平衡、I/Q 偏移作为射频指纹特征。但实际设备的射频指纹一般受到多个参数的影响，这些参数之间相互影响，且部分参数可以进行转换，例如一阶 I/Q 滤波器参数就等同于 I/Q 增益不平衡造成的效果。

当多个参数混杂在一起对射频指纹产生综合效应时，产生的星座图就会非常复杂。将前几小节研究的参数的值设为之前仿真的临界参数的 1/4，得到的 QPSK 和 16-QAM 调制下的星座图如图 11 所示。可以看到，虽然此时的 RMS EVM 分别为 13.2%和 9.6%，还在标准规定范围内，不会影响信号的解调，但星座点已经发生了不规则的发散。根据这样的星座图依次对单个参数进行估计的结果会与实际值存在很大偏差，而现阶段还没有有效的多参数联合估计的方法。当存在高斯噪声时，偏差会进一步放大，难以精确估计 I/Q 增益不平衡等参数。



(a) QPSK,
$D_I=0.0438, D_Q=0, \varepsilon=0.0438, \varphi=0.0438,$
$h_0^I=0, h_1^I=0.0438, h_0^Q=0, h_1^Q=0.0438,$
$\delta_\psi^2=2.888\mathrm{e}^{-5}, a_1=0.969-0.031\mathrm{j}, a_3=0, a_5=0$



(b) 16-QAM,
$D_I=0.0313, D_Q=0, \varepsilon=0.0313, \varphi=0.0313,$
$h_0^I=0, h_1^I=0.0245, h_0^Q=0, h_1^Q=0.0245,$
$\delta_\psi^2=1.47\mathrm{e}^{-5}, a_1=0.978-0.077\mathrm{j}, a_3=0, a_5=0$

Fig.11 Influence of mixing parameters on QPSK and 16-QAM constellation diagrams
图 11 混合参数对 QPSK、16-QAM 星座图的影响

4 结论

本文根据一种通用的零中频数字通信发射机结构分析了发射机各环节对于射频指纹的影响，建立了对应的射频指纹时域基带模型。总结归纳了 WiFi、ZigBee、LTE 等常用通信标准中载波中心频率、符号时钟、误差向量幅度以及信号开关机时间这 4 个重要参数的容差。然后，以 QPSK 和 16-QAM 两种典型调制方式为例，根据均方根误差向量幅度容差理论推导了 DAC 直流偏置、I/Q 增益不平衡、I/Q 正交偏移误差、I/Q 滤波器偏差、振荡器相噪和功放非线性的上下界，并通过 Matlab 仿真了各种极端情形下星座图的变化，分析了各个参数对星座图的影响，为射频指纹领域建模和仿真提供了合理的参数指导。

参考文献：

[1] JI Xinsheng,HUANG Kaizhi,JIN Liang,et al. Overview of 5G security technology[J]. Science China, 2018,61(8):107–131.

[2] AHMAD I,KUMAR T,LIYANAGE M, et al. Overview of 5G security challenges and solutions[J]. IEEE Communication Standards Magazine, 2018,2(1):36–43.

[3] 俞佳宝,胡爱群,朱长明,等. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报, 2016,3(5):433–446. (YU Jiabao, HU Aiqun,ZHU Changming,et al. RF fingerprinting extraction and identification of wireless communication devices[J]. Journal of Cryptologic Research, 2016,3(5):433–446.)

[4] 贾济铖,齐琳. 基于双谱的射频指纹提取方法[J]. 太赫兹科学与电子信息学报, 2021,19(1):107–111. (JIA Jicheng, QI Lin. RF fingerprint extraction method based on bispectrum[J]. Journal of Terahertz Science and Electronic Information

Technology, 2021,19(1):107-111.)
[5] 李古月,俞佳宝,胡爱群. 基于设备与信道特征的物理层安全方法[J]. 密码学报, 2019,5(5):1-2. (LI Guyue,YU Jiabao, HU Aiqun. Research on physical-layer security based on device and channel characteristics[J]. Journal of Cryptologic Research, 2019,5(5):1-2.)
[6] SHEN G,ZHANG J,MARSHALL A,et al. Radio frequency fingerprint identification for LoRa using spectrogram and CNN[C]// IEEE International Conference on Computer Communications. [S.l.]:IEEE, 2021:1-10.
[7] WANG W,SUN Z,PIAO S,et al. Wireless physical-layer identification:modeling and validation[J]. IEEE Transactions on Information Forensics and Security, 2016,11(9):2091-2106.
[8] LI Y. Frequency independent IQ imbalance estimation and compensation[M]. New York:Springer, 2014:29-47.
[9] WONG L J,HEADLEY W C,MICHAELS A J. Specific emitter identification using convolutional neural network-based IQ imbalance estimators[J]. IEEE Access, 2019(7):33544-33555.
[10] LIU M W,DOHERTY J F. Specific emitter identification using nonlinear device estimation[C]// IEEE Sarnoff Symposium. Princeton,NJ,USA:IEEE, 2008:1-5.
[11] HANNA S S,CABRIC D. Deep learning based transmitter identification using power amplifier nonlinearity[C]// IEEE International Conference on Computing,Networking and Communications(ICNC). Honolulu,HI,USA:IEEE, 2019:674-680.
[12] WHEELER C G,REISING D R. Assessment of the impact of CFO on RF-DNA fingerprint classification performance[C]// IEEE International Conference on Computing,Networking and Communications(ICNC). Silicon Valley,USA:IEEE, 2017: 110-114.
[13] JANA S,KASERA S K. On fast and accurate detection of unauthorized wireless access points using clock skews[J]. IEEE Transactions on Mobile Computing, 2009,9(3):449-462.
[14] SHI Y,JENSEN M A. Improved radiometric identification of wireless devices using MIMO transmission[J]. IEEE Transactions on Information Forensics and Security, 2011,6(4):1346-1354.
[15] TOMKO A A,RIESER C J,BUELL L H. Physical-layer intrusion detection in wireless networks[C]// IEEE Military Communications Conference(MILCOM), Washington,DC,USA:IEEE, 2006:1-7.
[16] REISING D R,TEMPLE M A,MENDENHALL M J. Improved wireless security for GMSK-based devices using RF fingerprinting[J]. International Journal of Electronic Security and Digital Forensics, 2010,3(1):41-59.
[17] ZHUANG Z,JI X,ZHANG T, et al. Fbsleuth:fake base station forensics via radio frequency fingerprinting[C]// Asia Conference on Computer and Communications Security. Incheon,Korea:[s.n.], 2018:261-272.
[18] IEEE Standards Association. IEEE 802.11-1997-IEEE standard for wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications[S]. 1997.
[19] IEEE Standards Association. IEEE 802.11b-1999-IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan networks—specific requirements-part 11:wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications:higher speed Physical Layer(PHY) extension in the 2.4 GHz band[S]. 1999.
[20] IEEE Standards Association. IEEE 802.11a-1999-IEEE standard for telecommunications and information exchange between systems—LAN/MAN specific requirements—part 11:wireless Medium Access Control(MAC) and Physical Layer (PHY) specifications:high speed Physical Layer in the 5 GHz band[S]. 1999.
[21] IEEE Standards Association. IEEE 802.11g-2003-IEEE standard for information technology—local and metropolitan area networks—specific requirements—part 11:wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications:further higher data rate extension in the 2.4 GHz band[S]. 2003.
[22] IEEE Standards Association. IEEE 802.11n-2009-IEEE Standard for Information technology-Local and metropolitan area networks-Specific requirements-Part 11:Wireless LAN Medium Access Control(MAC)and Physical Layer(PHY) Specifications Amendment 5:Enhancements for Higher Throughput[S]. 2009.
[23] IEEE Standards Association. IEEE 802.11ac-2013-IEEE standard for information technology—telecommunications and information exchange between systems—local and metropolitan area networks—specific requirements—part 11:wireless LAN Medium Access Control(MAC) and Physical Layer(PHY) specifications—amendment 4:enhancements for very high throughput for operation in bands below 6 GHz[S]. 2013.
[24] IEEE Standards Association. IEEE 802.3-2000-IEEE standard for information technology—LAN/MAN—specific requirements—part 3:Carrier Sense Multiple Access with Collision Detection(CSMA/CD) access method and physical layer specifications[S]. 2000. (下转第 622 页)