DOI：10.7652/xjtuxb201612018

一种利用 OFDM 系统无线信道相位响应的密钥提取方案

程龙旺，李为，马东堂，岳敖，刘潇然
（国防科学技术大学电子科学与工程学院，410073，长沙）

摘要：针对无线通信系统中利用信道特征提取密钥效率较低的问题，提出了一种利用正交频分复用(OFDM)系统无线信道相位响应的密钥提取方案，该方案首先利用相位随机化的信号对信道相位响应进行探测，并且随机选择一个合法节点通过对探测得到的信道相位进行量化生成初始密钥；其次，将初始密钥进行映射和预均衡处理后发送给对方节点，实现初始密钥的安全分发；最后，合法双方通过信息协商和保密增强获得安全密钥。该方案充分利用了无线信道相位响应的随机性和互易性，只需要一个合法节点来量化产生初始密钥，减少了量化处理，提升了密钥提取性能，同时由于信道相位响应对于收发端之间的距离十分敏感，而保证了该方案的安全性。仿真结果表明，当信噪比为 10 dB 时，与已有的基于信道相位和信道幅度的密钥提取方案相比，所提方案的密钥容量分别增加 34%和 70%，密钥不一致率分别降低 37%和 63%，密钥产生速率分别提高了 6.6%和 17%，同时所提方案生成的密钥通过了 NIST 随机性测试。

关键词：密钥提取；无线信道相位响应；预均衡；密钥容量
中图分类号：TN911.7 **文献标志码**：A **文章编号**：0253-987X(2016)12-0114-07

A Secret Key Extraction Scheme Using Wireless Channel Phase Response of OFDM Systems

CHENG Longwang, LI Wei, MA Dongtang, YUE Ao, LIU Xiaoran
(School of Electronic Science and Engineering, National University of Defense Technology, Changsha 410073, China)

Abstract: A secret key extraction scheme based on wireless channel-phase response of orthogonal frequency-division multiplexing (OFDM) systems is proposed to solve the low efficiency problem of secret key generation based on the characteristics of wireless channels. The proposed scheme probes the channel-phase response by using the probe signal with random phase, and a node is randomly selected to generate an initial secret key by quantizing the channel-phase response. The initial secret key is mapped and pre-equalized, and then sent to the other node to achieve secure distribution of the initial secret key. Finally, the both sides receive secure secret keys through information consultation and secrecy enhancement. The proposed scheme fully utilizes the randomness and reciprocity of the wireless channel-phase response and generates the initial secret key by quantifying a single legitimate node. Thus the performance of secret key extraction is improved. Further, the security of the scheme is ensured by the sensitivity of the channel-phase response to the distance between the transmitter and receiver. Simulation results and comparisons

收稿日期：2016-04-11。 作者简介：程龙旺(1988—)，男，博士生；马东堂(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金资助项目(61502518，61302140，61372099)。
网络出版时间：2016-10-26 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20161026.1755.004.html

with the existing channel-phase based scheme and the channel-amplitude based scheme show that the secret key capacity of the proposed scheme increases by 34% and 70%, the secret key mismatch rate decreases by 37% and 63%, and the secret key generation rate increases by 6.6% and 17%. Moreover, the extracted secret key passes the NIST test.

Keywords: secret key extraction; wireless channel-phase response; pre-equalization; secret key capacity

随着无线移动通信的快速发展，各种无线终端例如电脑、手机、PAD 的普及，以及手机银行、微信支付等应用的兴起，使得无线通信安全日益成为人们关注的热点问题，而无线信道的广播特性，使得这些通信过程很容易遭到窃听和攻击。密码学是保障信息安全的重要工具之一，但是传统的上层加密机制大多依赖于一些未经严格证明的数学难题和计算复杂性，只能实现计算安全，而且随着无线窃听设备和窃听技术以及量子计算机等高性能计算机的快速发展，使得传统加密机制在无线通信应用场景中面临着严峻挑战和威胁。利用物理层无线信道特征来补充和增强传统安全机制已引起了人们的广泛关注，其中利用无线信道特征提取密钥，使得“一次一密”的无条件安全成为可能，是当前的一个研究热点。

Maurer 等人首先证明了合法节点可以从具有相关性的信息（敌手对于这些相关信息的观测不同于合法节点）中提取密钥，并且可以在敌手具有很强计算能力情况下实现完全的安全[1-2]。随后 Hassan 等人在文献[3]中提出从无线信道的特征中提取密钥的思想。无线信道的时变性保证了合法双方每次探测获得密钥随机变化，进而生成具有噪声性质的真随机密钥；信道相干时间内的短时互易性确保了合法双方获得密钥的一致性；空变性保证了密钥生成过程的物理安全性。因此，无线信道可以作为一种天然的随机源来提取密钥，进而实现安全通信。

采用时分双工（TDD）方式对信道进行探测时，无线信道的多种特征可以用来提取密钥。文献[4-6]利用接收信号强度来提取相同的密钥；文献[4,7-10]采用信道冲击响应来生成共享密钥；文献[11-12]中的合法双方通过测量多径信道中的多径相对时延来产生共享密钥。这些方法中的接收信号强度在现有设备上易于获取，但是密钥产生速率较低，并且可扩展性受到限制；基于信道冲击响应的方法能够有效提升密钥产生速率，但是量化误差等因素会影响密钥不一致率；基于多径相对时延的方法适用场景受限。

本文针对正交频分复用（OFDM）系统提出一种利用无线信道相位响应的密钥提取方案。为了确保生成密钥的随机性，该方案首先利用相位随机化的信号对无线信道相位响应进行探测，并且随机选择一个合法节点通过对探测得到的信道相位估计值进行量化生成初始密钥；其次，对初始密钥进行映射和预均衡处理后，初始密钥被隐藏在发送信号的相位中，该节点再将生成的发送信号发送给对方节点，实现初始密钥的安全分发；最后，双方通过信息协商和保密增强来获得安全密钥。本文所提方案充分利用了无线信道相位响应的随机性和互易性，减少了信道探测和量化处理，提升了密钥提取效率和性能；又由于无线信道相位响应对于收发端之间的距离十分敏感，这就保证了提取密钥的安全性。

1　系统模型

如图 1 所示，本文考虑 3 个节点的网络模型，物理层均采用 OFDM 技术。Alice 和 Bob 是合法节点，并且尝试利用信道特征来建立共享密钥；Eve 是一个敌手，试图在 Alice 和 Bob 的密钥建立过程中窃取密钥。$\boldsymbol{h}_{AB}$ 和 $\boldsymbol{h}_{BA}$ 分别是 Alice 与 Bob 之间的合法信道，$\boldsymbol{h}_{AE}$ 和 $\boldsymbol{h}_{BE}$ 分别是 Alice 和 Bob 到 Eve 之间的窃听信道。Eve 能够监听 Alice 和 Bob 之间的所有通信内容，但是不能主动篡改这些通信内容和干扰密钥建立过程。假设 Eve 到 Alice 和 Bob 的距离均大于 0.5λ（λ 是载波波长），在这种情况下，合法信道和窃听信道相互独立[13]。每个节点都配备一根天线，所有节点均采用半双工模式，这意味着任意一个节点无法同时接收和发送信号。为了确保相干时

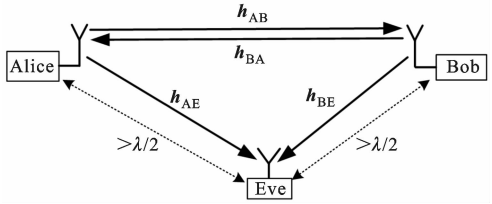

图 1　系统模型

间内上下行信道 $\boldsymbol{h}_{\mathrm{BA}}$ 和 $\boldsymbol{h}_{\mathrm{AB}}$ 之间的互易性，Alice 和 Bob 采用 TDD 通信模式。

2 利用信道相位响应的密钥提取

已有的大部分研究中，基于无线信道特征的密钥提取流程主要由 4 步组成：信道探测、特征量化、信息协商和保密增强，如图 2 所示。

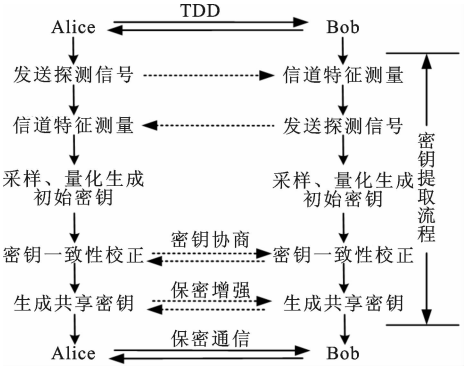

图 2 已有方案的密钥提取流程图

图 2 中信道探测和特征量化是合法双方节点分别依次进行的过程，这使得初始密钥的生成会引入量化过程产生的误差，这可能额外需要交互信道测量值的索引信息来消除这些误差，并且会导致更大的代价来实现密钥协商。本文方案的密钥提取流程如图 3 所示，主要包括信道探测、量化和初始密钥分发以及信息协商和保密增强（后面会详细介绍每个步骤），在该方案中，信道探测和量化过程只需要一个节点来完成，不需要交互相位测量值的索引信息，消除了量化误差带来的影响，降低了密钥协商的难度。

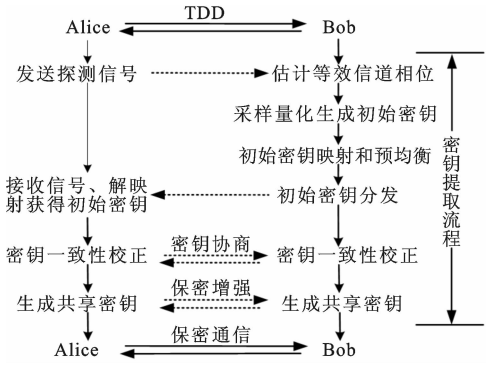

图 3 本文所提方案的密钥提取流程图

由于 OFDM 系统的多个子信道可以提供更多的随机源，本文利用 OFDM 系统中不同子信道的频域相位响应来提取密钥。假设 OFDM 子载波间隔足够大，确保不同子载波经历相互独立的信道衰落。在所提方案中，假设每一轮信道探测时间均小于信道相干时间，确保信道互异性成立，即 $\boldsymbol{h}_{\mathrm{AB}}=\boldsymbol{h}_{\mathrm{BA}}=\boldsymbol{h}$。如无特别说明，论文中所有的信号都是频域信号，它们的操作都是在频域进行。本文方案的密钥提取步骤如下。

(1)信道探测。在信道探测过程中，为了防止在静止环境中提取的密钥相关性过高、容易被窃听者获取的问题[5]，发送的探测信号相位是随机的。假设 Bob 是被随机选择进行量化的节点，那么 Alice 首先向 Bob 发送探测信号 $\boldsymbol{s}_{\mathrm{A}}=[s_{\mathrm{A},1},s_{\mathrm{A},2},\cdots,s_{\mathrm{A},N}]$，其中 $s_{\mathrm{A},i}=\exp(\mathrm{j}\theta_{\mathrm{A},i})$，$\theta_{\mathrm{A},i}$ 表示 $s_{\mathrm{A},i}$ 的随机相位，并且均匀分布在 $[0,2\pi)$，$i=1,2,\cdots,N$，N 表示 OFDM 系统中子载波数目。探测信号 $\boldsymbol{s}_{\mathrm{A}}$ 对于 Bob 和 Eve 是未知的。

(2)量化和密钥分发。不失一般性，这里只采用第 $i(1\leqslant i\leqslant N)$ 个子载波作为例子进行分析。Bob 接收到的第 i 个频域信号可以表示为

$$r_{\mathrm{B},i}=h_i s_{\mathrm{A},i}+w_{\mathrm{B},i}=|h_i|\exp(\mathrm{j}\theta_{\mathrm{h},i})s_{\mathrm{A},i}+w_{\mathrm{B},i}=|h_i|\exp(\mathrm{j}\theta_{\mathrm{h},i}+\mathrm{j}\theta_{\mathrm{A},i})+w_{\mathrm{B},i} \tag{1}$$

式中：h_i 表示 $\boldsymbol{h}$ 的第 i 个子信道的频域信道响应，假设每个子信道独立同分布，即 $h_i\sim\mathrm{CN}(0,\sigma_{\mathrm{h}}^2)$，$\angle h_i=\theta_{\mathrm{h},i}$，$w_{\mathrm{B},i}\sim\mathrm{CN}(0,\sigma_{\mathrm{n}}^2)$ 是独立同分布的复高斯噪声。Bob 将接收到的信号乘以一个随机系数 c_i，即 $\hat{r}_{\mathrm{B},i}=r_{\mathrm{B},i}c_i$，其中 $c_i=\exp(\mathrm{j}\theta_{\mathrm{c},i})$，$\theta_{\mathrm{c},i}\sim U[0,2\pi)$。Bob 根据 $\hat{r}_{\mathrm{B},i}$ 估计出相应的子信道相位响应为

$$\hat{\theta}_{\mathrm{B},i}=\arctan(\mathrm{imag}(\hat{r}_{\mathrm{B},i})/\mathrm{real}(\hat{r}_{\mathrm{B},i}))=\theta_{\mathrm{h},i}+\theta_{\mathrm{A},i}+\theta_{\mathrm{c},i}+\varepsilon_{\mathrm{B},i} \tag{2}$$

式中：$\varepsilon_{\mathrm{B},i}$ 表示相位估计误差。需要注意的是 Bob 估计的相位中还包含了探测信号的相位 $\theta_{\mathrm{A},i}$ 和随机系数 c_i 的相位 $\theta_{\mathrm{c},i}$，因此这里将 $\hat{\theta}_{\mathrm{B},i}$ 看作是等效子信道相位响应的估计值。接下来 Bob 对 $\hat{\theta}_{\mathrm{B},i}$ 进行量化生成初始密钥。

Bob 首先将 $[0,2\pi)$ 等间隔地划分为 2^M 个子区间（M 是一个整数），其中第 p 个子区间为 $[2\pi(p-1)/2^M,2\pi p/2^M)$，$p=1,2,\cdots,2^M$。每个区间按照格雷码分配长度为 M 的二进制比特序列，当 $M=2$ 时，相位量化示意图如图 4 所示。

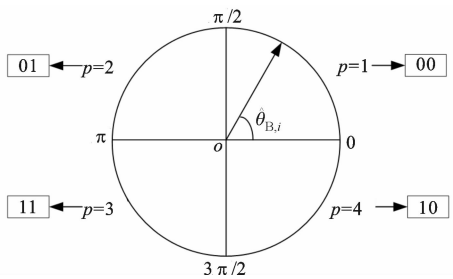

图 4 $M=2$ 时相位量化示意图

第 i 个等效子信道相位估计值 $\hat{\theta}_{\mathrm{B},i}$ 可以量化为

$$Q(\hat{\theta}_{\mathrm{B},i})=p_i,\ \hat{\theta}_{\mathrm{B},i}\in[2\pi(p_i-1)/2^M,2\pi p_i/2^M) \tag{3}$$

可以看出每个等效子信道相位估计值被量化成了长度为 M 的二进制比特。经过量化，Bob 获得初始密钥为 $\boldsymbol{k}_{\mathrm{B}}=[k_{\mathrm{B},1},k_{\mathrm{B},2},\cdots,k_{\mathrm{B},NM}]$。接下来 Bob 向 Alice发送探测信号，不同已有的方案中发送固定的探测信号，这里的探测信号是经过映射和预均衡处理的初始密钥，如此处理后的密钥信息就被隐藏在探测信号的相位信息中。Bob 发送的探测信号可以表示为

$$s_{\mathrm{B},i}=\exp(\mathrm{j}M(k_i^M)-\mathrm{j}(\hat{\theta}_{\mathrm{B},i}-\theta_{\mathrm{c},i})) \tag{4}$$

式中：$M(\cdot)$ 表示对初始密钥进行星座映射；$s_{\mathrm{B},i}$ 的相位中减去 $(\hat{\theta}_{\mathrm{B},i}-\theta_{\mathrm{c},i})$ 即为预均衡处理，正是预均衡处理将密钥隐藏在了相位中；k_i^M 表示映射输入的密钥，$k_i^M=[k_{\mathrm{B},(i-1)l+1},\cdots,k_{\mathrm{B},(i-1)l+l}]$，$l$ 表示输入密钥的长度，例如 $l=2$ 时，映射函数可以设计为

$$M(k_i^M)=\begin{cases}0, & k_i^M=[0\ \ 0]\\ \pi/2, & k_i^M=[0\ \ 1]\\ \pi, & k_i^M=[1\ \ 1]\\ 3\pi/2, & k_i^M=[1\ \ 0]\end{cases} \tag{5}$$

映射函数对于 Alice 和 Eve 都是已知的。

综上，Bob 完成等效相位估计的量化，获得初始密钥后，从 NM 个初始密钥中随机选择 Nl（$Nl\leqslant NM$）个密钥，并且将这些密钥进行 $M(\cdot)$ 映射，这里设定 $l=M$；随后，Bob 将预均衡后的探测信号 $\boldsymbol{s}_{\mathrm{B}}=[s_{\mathrm{B},i},s_{\mathrm{B},i},\cdots,s_{\mathrm{B},N}]$ 发送给 Alice。Alice 接收到的信号为

$$r_{\mathrm{A},i}=h_i s_{\mathrm{B},i}+w_{\mathrm{A},i} \tag{6}$$

式中：$w_{\mathrm{A},i}$ 服从 $\mathrm{CN}(0,\sigma_n^2)$ 分布，是独立同分布的复高斯噪声。由于上下行信道相位响应满足互易性，将式(4)带入式(6)可以得到

$$r_{\mathrm{A},i}=|h_i|\exp(\mathrm{j}(M(k_i^M)-\theta_{\mathrm{A},i}-\varepsilon_{\mathrm{B},i}))+w_{\mathrm{A},i} \tag{7}$$

可以看出，利用信道相位响应的互易性，Alice 在信号接收过程中就完成了信道相位均衡，消除了信道相位对初始密钥的加密。进一步，Alice 将接收的信号乘以第一步中发送的随机探测信号，可以得到

$$s_{\mathrm{A},i}r_{\mathrm{A},i}=|h_i|\exp(\mathrm{j}(M(k_i^M)-\varepsilon_{\mathrm{B},i}))+s_{\mathrm{A},i}w_{\mathrm{A},i} \tag{8}$$

接下来，Alice 根据 $s_{\mathrm{A},i}r_{\mathrm{A},i}$ 的相位进行解映射就可以获得 Bob 发送的初始密钥，即完成了初始密钥的安全分发。

从式(6)～(8)可以看出，Alice 的接收信号受到噪声 $w_{\mathrm{B},i}$ 和 $w_{\mathrm{A},i}$ 的双重影响，其中 $w_{\mathrm{B},i}$ 是式(1)中 Bob 接收 Alice 发送的探测信号时的噪声，由该噪声产生的相位估计误差随着 Bob 的初始密钥分发被传递给 Alice。假设 $w_{\mathrm{B},i}$ 和 $w_{\mathrm{A},i}$ 是独立同分布的，这里近似认为 $w_{\mathrm{B},i}$ 和 $w_{\mathrm{A},i}$ 对 Alice 的接收带来双重加性噪声影响，接收信噪比变为 $\sigma_h^2/2\sigma_n^2$，即对 Alice 的密钥估计带来 3 dB 性能恶化。图 5 给出了 $w_{\mathrm{B},i}=0$ 和 $w_{\mathrm{B},i}\neq0$ 时，Alice 的密钥估计误比特率性能（即密钥比特不一致率）。可以看出 $w_{\mathrm{B},i}\neq0$ 时，Alice 的密钥估计性能比 $w_{\mathrm{B},i}=0$ 时恶化了大约 3 dB，随着信噪比的增加，2 种情况下的性能越接近。

从上面的分析可以看出，该步骤实现了初始密钥的安全分发，但是由于这些噪声无法避免，同时也带来了一定的性能损失。因此，在实际系统中利用所提方法提取密钥时，应尽可能提高信噪比。

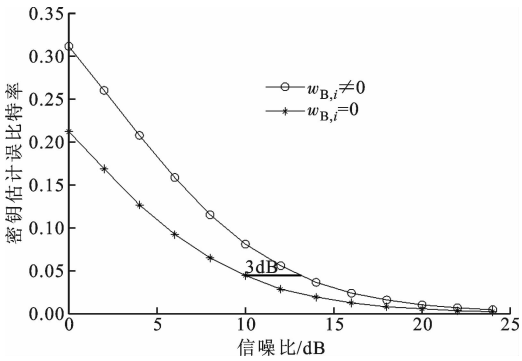

图 5　Alice 估计密钥的误比特率性能比较

(3)密钥协商和保密增强。每轮探测 Alice 的探测信号和 Bob 使用的随机系数都进行更新，经过多轮信道探测和密钥分发，Alice 和 Bob 获得足够多的密钥。由于噪声等干扰的存在，可能导致 Alice 和 Bob 获得密钥存在不一致情况，针对这种情况，Alice 和 Bob 采用信息协商来完成不一致密钥比特的校正，例如 BCH 编码或者 Cascade 协议[14]。需要注意的是，信息协商过程中双方是通过公共信道进行校验信息的交互，这可能会泄露关于密钥的部分信息。可以采用保密增强来解决这个问题，例如利用 Hash 函数来产生最终安全的密钥。

在图 3 所示的密钥提取流程中，需要注意的是，每一轮信道探测和初始密钥分发的时间需要小于信道相干时间来保证信道的互易性。可以看出，信道探测过程中，Alice 发送的是相位随机的探测信号，这就保证了等效信道相位随机变化，有效解决了静止环境中由于信道变化缓慢导致提取的密钥相关性

过高、不安全的问题[8]。因此,本文所提的密钥提取方案同样适用于静止环境中的密钥提取。

3 性能分析

本节将从安全性和密钥提取性能两方面对所提方案进行评估。

3.1 安全性分析

假设在密钥提取过程中,Eve 一直处于被动窃听,但是 Eve 知道密钥提取的每个步骤和相关参数。在本文方案密钥提取步骤 1 中,Eve 接收到 Alice发送的探测信号为

$$r_{\mathrm{EA},i}=h_{\mathrm{AE},i}s_{\mathrm{A},i}+w_{\mathrm{AE},i}=|h_{\mathrm{AE},i}|\exp(\mathrm{j}\theta_{\mathrm{hAE},i}+\mathrm{j}\theta_{\mathrm{A},i})+w_{\mathrm{AE},i} \tag{9}$$

式中:$h_{\mathrm{AE},i}=|h_{\mathrm{AE},i}|\exp(\mathrm{j}\theta_{\mathrm{hAE},i})$表示 Alice 到 Eve 的第 i 个子信道;$w_{\mathrm{AE},i}$表示 Eve 的观测噪声。从步骤 1 可以看出:Alice 不需要发送用于信道估计的训练序列,由于每次探测 $s_{\mathrm{A},i}$ 的相位均随机分布在[0,2π],因此 Eve 无法获得关于 $h_{\mathrm{AE},i}$ 和 $h_{\mathrm{AB},i}$ 的相位信息;进一步,由于 Eve 不知道 Bob 量化过程中采用的随机系数 c_i,使得 Eve 无法通过接收到的信号量化产生密钥。因此,在此过程,Eve 无法获得关于密钥的任何信息。

在步骤 2 中,Eve 接收到 Bob 发送的信号为

$$r_{\mathrm{EB},i}=h_{\mathrm{BE},i}s_{\mathrm{B},i}+w_{\mathrm{BE},i}=|h_{\mathrm{BE},i}|\exp(\mathrm{j}(\theta_{\mathrm{hBE},i}+M(k_i^M)-\theta_{\mathrm{h},i}-\theta_{\mathrm{A},i}-\varepsilon_{\mathrm{B},i}))+w_{\mathrm{BE},i} \tag{10}$$

式中:$h_{\mathrm{BE},i}=|h_{\mathrm{BE},i}|\exp(\mathrm{j}\theta_{\mathrm{hBE},i})$表示 Bob 到 Eve 的第 i 个子信道;$w_{\mathrm{BE},i}$表示观测噪声。Bob 的发送信号同样不包含用于信道估计的训练序列,Eve 也无法获得关于 $h_{\mathrm{BE},i}$ 和 $h_{\mathrm{BA},i}$ 的相位信息,因此也无法只从 $r_{\mathrm{EB},i}$ 的相位中得到密钥信息。

从式(9)和(10)可以看出,影响 Eve 窃取密钥的主要因素包括主信道系数 h_i、窃听信道系数 $h_{\mathrm{AE},i}$ 和 $h_{\mathrm{BE},i}$ 以及 Alice 发送的随机探测信号 $s_{\mathrm{A},i}$ 的相位。如果忽略噪声影响,Eve 将上面 2 个公式相乘,得到如下结果

$$r_{\mathrm{EB},i}r_{\mathrm{EA},i}=|h_{\mathrm{BE},i}h_{\mathrm{AE},i}|\exp(\mathrm{j}(\theta_{\mathrm{hBE},i}+\theta_{\mathrm{hAE},i}+M(k_i^M)-\theta_{\mathrm{h},i}-\varepsilon_{\mathrm{B},i})) \tag{11}$$

从式(11)可以看出,影响 Eve 窃取密钥的因素减少为主信道和窃听信道的相位信息。假设 Eve 距离 Alice 很近,近似认为 $h_{\mathrm{BE},i}=h_{\mathrm{BA},i}$,那么式(11)变成

$$r_{\mathrm{EB},i}r_{\mathrm{EA},i}=|h_{\mathrm{BE},i}h_{\mathrm{AE},i}|\exp(\mathrm{j}(\theta_{\mathrm{hAE},i}+M(k_i^M)-\varepsilon_{\mathrm{B},i})) \tag{12}$$

由于 Eve 不知道与 Alice 之间的信道相位信息,同样地无法获得密钥信息;假设 Eve 距离 Bob 较近,近似认为 $h_{\mathrm{AE},i}=h_{\mathrm{AB},i}$,则式(11)变成

$$r_{\mathrm{EB},i}r_{\mathrm{EA},i}=|h_{\mathrm{BE},i}h_{\mathrm{AE},i}|\exp(\mathrm{j}(\theta_{\mathrm{hBE},i}+M(k_i^M)-\varepsilon_{\mathrm{B},i})) \tag{13}$$

同样,Eve 无法获得与 Bob 之间的信道相位信息,也无法获得密钥信息。

由于信道相位响应对于收发端之间的距离十分敏感,Eve 在距离 Alice 和 Bob 大于 0.5λ 情况下,就能够保证窃听信道相位响应与主信道相位响应相互独立。因此,针对 Eve 的被动窃听,通过分析可以看出利用所提方法提取密钥的安全性能够得到有效保证。此外,文献[15]指出通过设计合适的编码速率对初始密钥进行纠错编码,理论上就可以保证 Alice 在无误接收初始密钥的同时,使 Eve 无法完全获得密钥信息,这就意味着可以通过设计合适速率的纠错编码对初始密钥进行编码来进一步保证所提方案的安全性。

3.2 密钥提取性能分析

(1)密钥容量分析。密钥容量定义为密钥生成速率的上界[1]。本文所提的方法可建模为 Bob 产生一个随机源 $X=h$,Alice 对 Bob 产生的随机源进行观测 $Y=X+W_{\mathrm{A}}$,其中 $h\sim\mathrm{CN}(0,\sigma_{\mathrm{h}}^2)$,$W_{\mathrm{A}}\sim\mathrm{CN}(0,\sigma_{\mathrm{w}}^2)$表示观测噪声。双方利用 X 和 Y 的相位 θ_X 和 θ_Y 所能提取密钥的密钥容量为 $C_{\mathrm{P}}=I(\theta_X;\theta_Y)$。由于 θ_X 和 θ_Y 的联合概率密度函数不容易求解,这里利用信息论估计(ITE)工具[16]对 $I(\theta_X;\theta_Y)$ 进行估计。需要注意的是这里的密钥容量只采用 1 个子信道进行分析。

由于基于接收信号强度的密钥提取方案的密钥产生速率较低,因此选择已有的基于信道增益和信道相位的方案与本文所提方案的密钥提取性能进行比较。文献[8]研究了基于信道增益的密钥提取方案,文献[10]则是以信道相位响应作为随机源来提取密钥,这 2 种方案的密钥提取过程与图 2 一致。图 6 比较了不同信噪比下,这 2 种密钥提取方案与本文所提方案的密钥容量。由图 6 可以清晰地看出,本文所提方案的密钥容量要明显高于已有的基于信道增益和信道相位 2 种方案的密钥容量,在信噪比等于 10 dB 时,本文方案的密钥容量相对于基于信道相位和信道增益的方案分别增加了 34% 和 70%。

(2)密钥不一致率和密钥产生速率分析。密钥不一致率指的是合法双方获得的初始密钥中不一致的密钥比特占初始密钥的比例,而密钥产生速率这

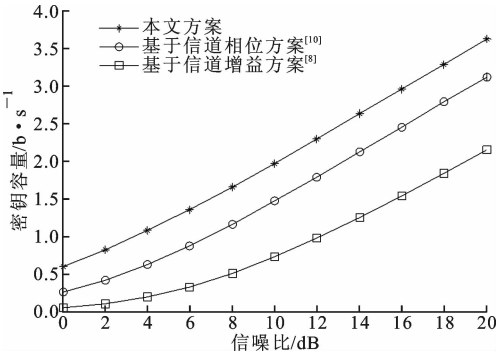

图 6　不同方案的密钥容量比较

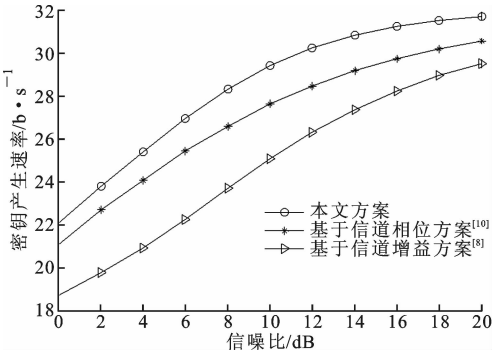

图 8　密钥产生速率比较

里定义为平均每次信道探测能够提取的密钥比特数。对于本文所提方案的密钥不一致率和密钥产生速率性能，可以通过蒙特卡洛仿真进行分析。仿真系统为 OFDM 系统，子载波数 $N=64$，频域子信道为相互独立的瑞利衰落信道。通过蒙特卡洛仿真比较了本文方案与文献[8]和文献[10]方案在不同信噪比下的密钥不一致率和密钥产生速率的性能。假设 2 种密钥提取方案与本文所提方案均采用等间隔量化方案，即信道特征空间被等间隔地划分成 $M=4$ 个间隔相等的子空间，并且采用相同的密钥协商和保密增强方法。

图 7 和图 8 分别比较了 3 种方案的密钥不一致率和密钥产生速率。可以看出，随着信噪比的增大，各种方案的密钥产生速率逐渐增大，密钥不一致率逐步降低，本文所提方案的密钥不一致率和密钥产生速率明显优于其他 2 种方案，在信噪比等于 10 dB 时，与基于信道相位和信道增益的方案相比，所提方案的密钥不一致率分别降低了 37%和 63%，密钥产生速率分别提升了 6.6%和 17%。

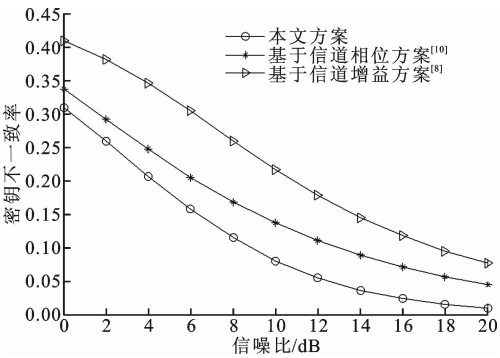

图 7　3 种方案的密钥不一致率比较

(3)密钥随机性分析。对于本文方案最终生成密钥的随机性，采用 NIST 随机性测试工具[17]进行测试。在 NIST 测试套件中，一共有 16 个不同的统计测试，每个测试的 p 值(p 值是一个概率值，大小在 0 到 1 之间)都大于 0.01，则表示通过随机性测试。在信噪比等于 10 dB 时，从仿真生成的共享密钥中随机选取了 10 组密钥序列，并且选择了 9 个典型指标进行测试，分别计算了 p 值，具体测试结果如表 1 所示。从表 1 可以看出，利用本文方案提取的密钥能够通过随机性测试，并且密钥序列的熵值很接近真实的随机序列。

表 1　本文方案随机性测试结果

测试项	p 值
频数检验	0.44
块内频数检验	0.53
前向累积和检验	0.63
后向累积和检验	0.27
游程检验	0.73
块内最长游程检验	0.27
线性复杂度检验	0.74
序列检验	0.35，0.63
近似熵检验	0.82

4　结　论

针对现有的基于无线信道特征提取密钥的方案中，由于合法通信双方分别量化产生初始密钥，导致密钥不一致率较高和密钥产生速率较低的问题，本文基于 OFDM 系统提出了一种利用等效信道相位响应提取密钥的方案，本文所提方案只需要一个节点进行信道探测和量化，简化了量化过程；通过预均衡将初始密钥隐藏在探测相位中，利用信道互易性实现初始密钥的分发。分析和仿真结果表明：利用本文所提方案提取密钥的安全性能够得到有效保证；本文方案的密钥容量、密钥不一致率、密钥产生速率等密钥提取性能要优于已有的基于信道增益和信道相位的密钥提取方案，并且提取的密钥通过了随机性测试。下一步将针对敌手主动窃听和多天线系统的场景进行研究。

参考文献：

[1] MAURER U M. Secret key agreement by public discussion from common information [J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742.

[2] AHLSWEDE R, CSISZÁR I. Common randomness in information theory and cryptography: part I Secret sharing [J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-1132.

[3] HASSAN 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.

[4] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel [C]// Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. New York, USA: ACM, 2008: 128-139.

[5] JANA S, PREMNATH S N, CLARK M, et al. On the effectiveness of secret key extraction from wireless signal strength in real environments [C]// Proceedings of the Annual International Conference on Mobile Computing and Networking. New York, USA: ACM, 2009: 321-332.

[6] LIU H, YANG J, WANG Y, et al. Group secret key generation via received signal strength: protocols, achievable rates, and implementation [J]. IEEE Transactions on Mobile Computing, 2014, 13(12): 2820-2835.

[7] WANG Q, XU K, REN K. Cooperative secret key generation from phase estimation in narrow band fading channels [J]. IEEE Journal on Selected Areas in Communications, 2012, 30(9): 1666-1674.

[8] CHENG Longwang, LI Wei, MA Dongtang. Secret key generation via random beamforming in stationary environment [C]// Proceedings of 2015 International Conference on Wireless Communications and Signal Processing. Piscataway, NJ, USA: IEEE, 2015: 7341290.

[9] 蔡文炳，付双红，张水莲，等. 一种无线信道密钥容量求解方法 [J]. 西安交通大学学报，2014，48(6)：31-36.
CAI Wenbing, FU Hongshuang, ZHANG Shuilian, et al. A solution of secret key capacity for wireless channel [J]. Journal of Xi'an Jiaotong University, 2014, 48(6): 31-36.

[10] WANG Qian, SU Hai, REN Kui, et al. Fast and scalable secret key generation exploiting channel phase randomness in wireless networks [C]// Proceedings of IEEE INFOCOM. Piscataway, NJ, USA: IEEE, 2011: 1422-1430.

[11] HUANG Jingjing, JIANG Ting. Dynamic secret key generation exploiting ultra-wideband wireless channel characteristics [C]// Proceedings of 2015 IEEE Wireless Communications and Networking Conference. Piscataway, NJ, USA: IEEE, 2015: 1701-1706.

[12] 周百鹏，黄开枝，金梁，等. 一种基于多径相对时延的密钥生成方法 [J]. 计算机应用研究，2011，28(6)：2196-2198.
ZHOU Baipeng, HUANG Kaizhi, JIN Liang, et al. Scheme of key generation based on multipath relative-delay [J]. Application Research of Computers, 2011, 28(6): 2196-2198.

[13] JAKES W C. Microwave mobile communications [M]. Piscataway, NJ, USA: Wiley-IEEE Press, 1994: 121-127.

[14] BRASSARD G, SALVAIL L. Secret-key reconciliation by public discussion [M]// Lecture Notes in Computer Science: Vol. 765. Berlin, Germany: Springer, 1998: 410-423.

[15] 戴峤，宋华伟，金梁，等. 基于等效信道的物理层认证和密钥分发机制 [J]. 中国科学，2014，44(12)：1580-1592.
DAI Qiao, SONG Huawei, JIN Liang, et al. Physical layer authentication and secret key distribution mechanism based on equivalent channel [J]. Science China, 2014, 44(12): 1580-1592.

[16] SZABO Z. Information theoretical estimators toolbox [J]. Journal of Machine Learning Research, 2014, 15: 283-287.

[17] RARESCHI F, ROVATTI R, SETTI G. On statistical tests for randomness included in the NIST SP800-22 test suite and based on the binomial distribution [J]. IEEE Transactions on Information Forensics and Security, 2012, 7(2): 491-505.

（编辑　刘杨）