文章编号：1003-0530(2021)03-0336-13

# 基于无线信道状态信息的密钥提取方案设计与实现

郭登科 熊 俊 高玉威 曹 阔 马东堂
(国防科技大学电子科学学院，湖南长沙 410073)

**摘 要**：基于无线信道状态信息(Channel State Information，CSI)的密钥提取技术可以利用无线信道的短时互易性和时空唯一性实现合法通信双方之间的共享密钥分发，且具有计算复杂度低和无需额外设施辅助的优点，是上层加密方案的有效补充。本文分别为无线通信中的合法节点和窃听节点设计了基于 CSI 的密钥提取方案和被动窃听方案，并在时分双工正交频分复用通信体制下实现了所提方案的原型系统。基于实现的原型系统，本文在室内和室外两种典型通信环境中的节点静止和移动两种情况下，进行了存在窃听节点场景下的密钥提取测试实验。通过对测试结果的分析，验证了无线信道的短时互易性和时空唯一性，并表明所提密钥提取方案在典型通信场景下可以实现较高的密钥性能和系统安全性。

**关键词**：物理层安全；密钥提取；信道状态信息；实验研究
**中图分类号**：TN918 **文献标识码**：A **DOI**：10.16798/j.issn.1003-0530.2021.03.003

**引用格式**：郭登科，熊俊，高玉威，等. 基于无线信道状态信息的密钥提取方案设计与实现[J]. 信号处理，2021，37(3)：336-348. DOI：10.16798/j.issn.1003-0530.2021.03.003.

**Reference format**：GUO Dengke，XIONG Jun，GAO Yuwei，et al. Design and Implementation of Key Extraction Scheme Based on Wireless Channel State Information[J]. Journal of Signal Processing，2021，37(3)：336-348. DOI：10.16798/j.issn.1003-0530.2021.03.003.

# Design and Implementation of Key Extraction Scheme Based on Wireless Channel State Information

GUO Dengke XIONG Jun GAO Yuwei CAO Kuo MA Dongtang
(College of Electronic Science and Technology，National University of Defense Technology，Changsha，Hunan 410073，China)

**Abstract**：Since wireless channels have the characteristics of short-term reciprocity and space-time uniqueness，key extraction based on wireless channel state information (CSI) can establish shared key between legitimate communication parties. This technique is considered to be an effective complement to the upper layer encryption scheme with the advantages of low computational complexity and no need of additional facilities. In this paper，we designed a CSI-based key extraction scheme for legitimate wireless communication nodes，and a passive eavesdropping scheme for eavesdropping nodes. Furthermore，we implemented the prototype system of proposed schemes under the time division duplex orthogonal frequency division multiplexing communication system. Finally，we conducted key extraction test experiments in the presence of eavesdropping nodes under two typical communication environments (indoor and outdoor)，in each of which we considered both static and mobile nodes. Analysis of test results verifies the short-term reciprocity and space-time uniqueness of the wireless channel，and shows that the proposed key extraction scheme can achieve considerable key performance and strong system security in typical communication scenarios.

**Key words**：physical layer security；key extraction；channel state information；experimental study

收稿日期：2020-12-21；修回日期：2021-01-24
基金项目：国家自然科学基金资助项目(61372099，U19B2024，61601480，61931020)

## 1　引言

基于密码学的上层加密方案是目前无线通信网络中的主要安全防护手段，包括对称加密体制和公钥加密体制[1]。其中，对称加密算法因实现简单而得到广泛应用，但需要保证共享密钥的安全分发。上层的密钥分发多是基于公钥密码实现的，而公钥密码的安全性来源于数学难题的计算复杂性[2]，如大整数分解、离散对数等，因此在算力强大的攻击者面前，此类方案的安全性可能难以保证。此外，公钥密码算法复杂度较高，很难适用于包含大量低成本无线节点的未来物联网通信场景。基于无线信道的物理层密钥提取方案旨在利用无线信道特性在两个合法通信节点之间建立共享密钥，与基于公钥的密钥分发方案相比，具有更低的计算复杂度且无需额外的硬件支持，近年来得到广泛关注。

无线信道具有短时互易性和时空唯一性，可以作为提取共享密钥的天然随机源[3]。当合法通信双方工作在时分双工（Time Division Duplex，TDD）模式时，信道相干时间内上下行信号几乎经历相同的衰落[4]，这保证了合法通信双方可以获取到高度相关的信道观测。而无线通信环境中物体的运动和收发双方的相对运动均会对无线信号传播过程中的反射、折射和散射造成影响，使得信道特性在时间和空间上呈现随机变化特性，因此无线信道可以作为一个天然的密钥源。更重要的是，这一密钥源仅由信道上的合法通信双方共享，而不容易被窃听者获取，因为无线信道的空间唯一性保证了当窃听者与合法节点相距半个波长以上时，其观测到的信道是与合法信道不相关的[5]。

综合现有的研究来看，基于无线信道的密钥提取方案可分为四个阶段：信道探测、特征量化、信息协商和保密增强[6]。在信道探测阶段，合法通信双方互相发送包含导频信息的探测信号，并利用接收信号获得信道估计并提取信道特征；特征量化就是将信道特征值转化为二进制序列，作为合法双方的初始密钥；受到硬件指纹、测量不同步等因素的影响，合法双方的初始密钥中往往存在不一致的比特，因此合法双方需要采取信息协商方案通过公开的信息交互消除不一致的密钥位；最后，经过保密增强消除信息协商过程中泄露的信息，保证密钥的安全性。

国内外对基于无线信道的密钥提取已有广泛的研究[7-16]，主要包括：信道特征的选取、特征预处理及量化算法的提出，以及信息协商方案的设计。接收信号强度（Received Signal Strength，RSS）具有易于获取的优势，在早期的相关研究或窄带系统中被广泛用于密钥提取[7-9]，但由于 RSS 仅刻画信道粗粒度信息，密钥提取速率非常有限。近期的研究中，特别是在正交频分复用（Orthogonal Frequency Division Multiplexing，OFDM）系统中，基于信道状态信息（Channel State Information，CSI）的密钥提取方案大量涌现，CSI 能够更精细地反映信道特性，从而实现更高的密钥提取速率[10-11]。为了使合法通信双方从有噪的信道观测中尽可能地提取出一致的密钥，一方面通过对量化前的信道特征进行预处理（如低通滤波、线性变换等）消除非对称因素的影响[12]，另一方面对量化算法进行改进以提升算法的鲁棒性[13-14]。信息协商方案的相关研究主要聚焦于协商效率的提升，追求以尽可能少的开销达到更高的协商成功率[15]。此外，考虑到未来物联网中海量低成本节点间的密钥提取，以更低的计算复杂度实现密钥提取也成为当下研究的热点[16]。

目前，在实际通信系统中实现的物理层密钥提取方案大多数是基于 RSS 的方案[17-18]，而对于基于 CSI 的密钥提取，尽管已经有大量的研究给出了具体的实现方案，但大都通过理论分析和仿真实验对所提方案进行性能评估，缺乏实际通信场景下的实测验证和性能分析。Xi 等人利用 802.11n 的 CSI 获取工具收集 Intel 5300 网卡设备上的 CSI 进行密钥提取[19]，但在商用网络设备上只能获取到有限的 CSI 信息。Zhang 等人在实验室环境下，利用 WARP（Wireless open-Access Research Platform）对 802.11 通信体制下基于 CSI 的密钥提取进行了实验研究[4]；东南大学的袁瑞等人基于 USRP（Universal Software Radio Peripheral）平台研究了 OFDM 系统在不同通信环境下的密钥提取性能[20]。但通用的硬件开发平台实时性较差，且目前尚未出现基于 CSI 的密钥提取原理样机实现及相关研究，缺乏对基于 CSI 的密钥提取在实际应用场景下的性能研究。此外，在窃听者存在的场景下，对基于 CSI 的密钥提取方案的安全性研究也缺乏实测数据的支撑。

本文第 2 节给出了一种 OFDM 系统中基于 CSI 的密钥提取方案设计，并且针对该方案为潜在的第三方窃听节点设计了一套被动窃听方案，使窃听节

点可以利用窃听到的信息来尝试仿造合法通信双方提取的密钥。第 3 节中介绍了基于 Zynq 架构设计的 TDD-OFDM 通信体制原理样机的硬件架构,以及所提方案原型系统的具体实现。在第 4 节,我们基于设计的原型系统,分别在室内和室外两种典型通信环境下进行了密钥提取测试实验,并考虑了节点静止和运动两种情况;利用各场景下的实测数据,本文从无线信道特性、密钥性能以及系统安全性三个角度出发,对基于 CSI 的密钥提取方案进行了较为全面的分析。第 5 节总结了本文的主要结论。

## 2 基于 CSI 的密钥提取方案设计

### 2.1 系统模型

本文研究的系统模型如图 1 所示。Alice 和 Bob 是 TDD-OFDM 系统中的两个合法通信节点,Eve 是无线通信场景中潜在的窃听节点。Alice 和 Bob 通过互相发送信道探测信号对合法信道进行估计,并基于各自的信道估计提取出一对共享密钥。Eve 试图通过窃听合法双方的通信内容恢复出合法节点之间的共享密钥。假设 Eve 可以监听到两个合法节点的所有通信内容,并能够借助合法双方发送的信道探测信号进行信道估计,而且已知合法双方的密钥提取方案及相关参数。

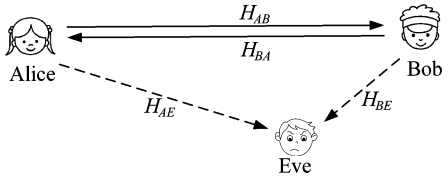



图 1 系统模型

Fig. 1 System model

### 2.2 密钥提取方案

本文实现的 OFDM 系统下的密钥提取方案主要包括:信道探测、特征量化、信息协商和保密增强四个阶段,下面分别对这四个阶段进行介绍。

#### 2.2.1 信道探测

在 TDD 工作模式下,Alice 和 Bob 交替发送包含导频信号的信道探测帧,并利用接收信号进行信道估计,如图 2 所示。以第 $i$ 轮信道探测为例,在 $t_i$ 时刻 Alice 向 Bob 发送信道探测信号 $x(t_i)$,则 Bob 处的接收信号为:

$$y_B(t_i)=\int_{-\infty}^{+\infty}h_{AB}(t_i,\tau)x(t_i-\tau)\,\mathrm{d}\tau+n_B(t_i) \quad (1)$$

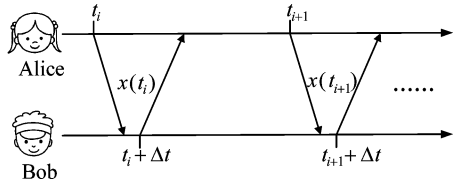



图 2 信道探测

Fig. 2 Channel probing

Bob 成功接收到 Alice 发送的探测信号后,在下一个时隙 $t_i+\Delta t$ 向 Alice 发送相同的探测信号,则 Alice 处的接收信号为:

$$y_A(t_i')=\int_{-\infty}^{+\infty}h_{BA}(t_i',\tau)x(t_i'-\tau)\,\mathrm{d}\tau+n_A(t_i') \quad (2)$$

其中,$h_{AB}(t_i,\tau)$ 和 $h_{BA}(t_i',\tau)$ 分别为 Alice 到 Bob 和 Bob 到 Alice 的信道冲激响应;$t_i'=t_i+\Delta t$,$\Delta t$ 为时隙间隔;$n_A(t_i)\sim\mathcal{CN}(0,\sigma_{n_A}^2)$,$n_B(t_i')\sim\mathcal{CN}(0,\sigma_{n_B}^2)$ 为加性高斯白噪声。

在 OFDM 系统中,Bob 处接收信号 $y_B(t_i)$ 的频域表达式可以写成:

$$Y_B(t_i,f_k)=H_{AB}(t_i,f_k)X(f_k)+Z_B(t_i,f_k) \quad (3)$$

其中,$f_k$ 为第 $k$ 个子载波的频率,$k=1,2,\cdots,K$,$K$ 为子载波总数。信道探测信号 $X(f_k)$ 已知,则 Bob 可以由接收信号 $Y_B(t_i,f_k)$ 得到信道频率响应(Channel Frequency Response,CFR)的最小二乘(Least Square,LS)估计:

$$\hat{H}_{AB}(t_i,f_k)=\frac{Y_B(t_i,f_k)}{X(f_k)}=H_{AB}(t_i,f_k)+\frac{Z_B(t_i,f_k)}{X(f_k)}$$
$$\triangleq H_{AB}(t_i,f_k)+\hat{Z}_B(t_i,f_k) \quad (4)$$

同理,Alice 也可以得到 CFR 的 LS 估计:

$$\hat{H}_{BA}(t_i',f_k)=H_{BA}(t_i',f_k)+\hat{Z}_A(t_i',f_k) \quad (5)$$

对比(4)、(5)两式,由噪声引入的信道估计误差 $\hat{Z}_B$ 和 $\hat{Z}_A$ 为相互独立的 0 均值高斯随机变量。当 Alice 和 Bob 发送信道探测帧的时间间隔远小于信道相干时间 $T_c$ 时,可以认为上下行信道是互易的,即:

$$H_{AB}(t_i,f_k)\approx H_{BA}(t_i',f_k),\ (\Delta t=t_i'-t_i\ll T_c) \quad (6)$$

#### 2.2.2 特征量化

选取 CFR 估计的幅值作为信道特征进行密钥提取,在特征量化阶段,合法通信双方 Alice 和 Bob 将信道特征值转换为二进制序列,作为初始密钥。本文所实现的密钥提取方案中特征量化阶段可以分为特征预处理和量化两个部分。由于此阶段中

Alice 和 Bob 执行相同的操作，下面以 Alice 为例对特征量化过程进行介绍。

Alice 对其得到的 CFR 估计 $\hat{H}_{BA}(t_i',f_k)$ 取模，得到 CFR 估计的幅值 $\hat{H}_A[k]$，$k=1,2,\cdots,K$。在进行量化前，首先对 CFR 估计的幅值进行滑动平均预处理：

$$\tilde{H}_A[m]=\frac{\sum_{i=1}^{w}\hat{H}_A[(m-1)s+i]}{w} \tag{7}$$

其中，$s$ 和 $w$ 分别为滑动平均的步长和窗口大小，$m=1,2,\cdots,M$，$M=\lfloor (K-w)/s \rfloor+1$。经过仿真实验分析，在本文的系统实现中取 $s=8$，$w=16$。通过预处理，一方面对信道特征进行了下采样，降低相邻子载波之间的相关性；另一方面取平均运算可以降低噪声对信道互易性的影响，增强合法双方信道特征值之间的相关性，从而可以有效降低合法双方初始密钥的不一致率。

$$K_A[m]=\begin{cases}00, & 若\ \tilde{H}_A[m-1]>\tilde{H}_A[m]<\tilde{H}_A[m+1]\\ 01, & 若\ \tilde{H}_A[m-1]>\tilde{H}_A[m]\geqslant\tilde{H}_A[m+1]\\ 11, & 若\ \tilde{H}_A[m-1]\leqslant\tilde{H}_A[m]\geqslant\tilde{H}_A[m+1]\\ 10, & 若\ \tilde{H}_A[m-1]\leqslant\tilde{H}_A[m]<\tilde{H}_A[m+1]\end{cases} \tag{8}$$

在量化时，我们采用了一种无门限的 2 比特量化方法，对于预处理后的信道特征值 $\tilde{H}_A[m]$，$m=2,3,\cdots,M-1$，依据式(8)的规则将其量化为 2 个比特。图 3 给出了本量化方法与传统 2 比特等概量化的性能比较结果，其中，用于评估量化方法的信道估计值均来自于 4.1 节所述的各场景下的测试数据，并考虑以下两个评估指标：

1）密钥不一致率：合法双方量化得到初始密钥中不一致比特数占总密钥长度的比例；

2）平均密钥长度：合法双方平均从每轮信道探测的 CSI 中量化得到的一致密钥长度。

从比较结果可以看出，本方案中的量化方法在各种实现场景下均能够实现更低的密钥不一致率，这主要得益于本量化方法无需借助门限即可实现对信道特征值的量化，可以有效避免门限附近的特征值引发的合法双方量化结果不一致，进一步减少 Alice 与 Bob 的初始密钥中不一致比特数量。此外，同为 2 比特量化，在多数场景下本量化方法的平均密钥长度优于等概量化，说明本量化方法可以实现较高的密钥提取效率。

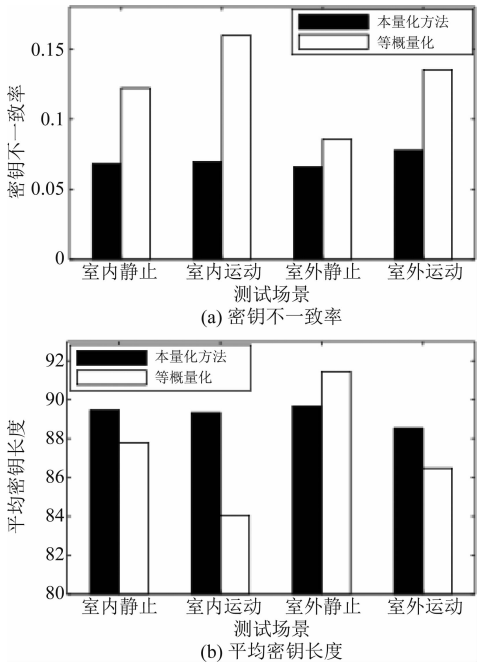



图 3　量化方法性能比较

Fig. 3　Performance comparison of quantization methods

### 2.2.3　信息协商

由于硬件指纹、测量不同步等非对称因素的影响，合法双方得到的初始密钥中会存在不一致的比特。为了得到完全一致的共享密钥，合法双方需要在公共信道上进行信息协商。

本文采用一种基于分组校验和交织操作的交互式信息协商方案，包括两轮完全相同的分组校验操作，并在两轮分组校验之间执行一次交织操作，方案流程如图 4 所示。在第一轮分组校验时，Alice 和 Bob 对各自的初始密钥进行分组，每组包含 3 个比特，而后计算每个分组的奇偶校验值，并将各组的奇偶校验值发送给对方。Alice 和 Bob 通过比对双方初始密钥各分组的奇偶校验，将校验值不一致的分组删除。经过第一轮分组校验后，Alice 和 Bob 分别对各自保留下来的密钥比特执行交织操作，将密钥比特序列按照行优先的规则写入一个 3 列的矩阵，然后按照列优先的规则读出，即得到交织后的密钥。Alice 和 Bob 对各自交织后的密钥执行第二轮分组校验，方法与第一轮分组校验相同。最后，双方对各自留存下来的密钥比特进行循环冗余校

验(Cyclic Redundancy Check,CRC),若校验位一致则信息协商成功,否则返回信道探测阶段,重新开始密钥提取。经过信息协商后,Alice 和 Bob 可以有效去除初始密钥中的不一致比特得到一致的密钥。

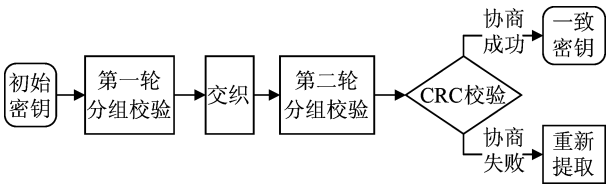



图 4 信息协商

Fig. 4 Information reconciliation

### 2.2.4 保密增强

保密增强的目的是通过一个不可逆的变换消除信息协商过程中泄露的与密钥相关的信息,增强提取密钥的安全性。散列函数是常用的保密增强方法[2,6],在本文的实现中,我们采用 SHA-1 算法实现保密增强。

## 2.3 被动窃听方案

在实际通信场景下,为了研究潜在窃听者 Eve 的存在对基于 CSI 的密钥提取方案的安全威胁,针对 2.2 节给出的密钥提取方案,我们为窃听者 Eve 制定了相应的窃听方案。窃听方案的设计遵循 2.1 节的系统模型假设,因此 Eve 清楚地掌握合法双方的密钥提取方案,并且可以监听到合法双方在密钥提取过程中公开交互的所有信息。下面对 Eve 的被动窃听方案设计进行具体介绍。

与合法双方的密钥提取方案中的四个阶段相对应,Eve 的被动窃听方案也可以划分为四个阶段:

1)阶段 1:Eve 监听合法节点发送的信道探测帧,并利用接收到的探测信号和已知的导频信号完成信道估计;

2)阶段 2:对得到的信道估计进行特征量化,方法与合法节点的特征量化相同,得到窃听初始密钥;

3)阶段 3:监听并接收来自 Alice 和 Bob 的分组校验和 CRC 校验信息,并根据合法双方的校验信息对窃听得到的初始密钥进行处理,进一步,计算最终所得密钥的 CRC 校验并与合法节点密钥的 CRC 校验值进行比对,若一致则窃听成功;否则窃听失败,返回阶段 1;

4)阶段 4:对窃听成功的密钥执行 SHA-1 算法,得到最终密钥。

在上述 4 个阶段中,阶段 2 和阶段 4 的处理过程与密钥提取方案相应的阶段相同,下面对阶段 1 和阶段 3 进行详细的说明。

在阶段 1 中,Eve 监听合法节点发送的信道探测帧,并利用接收到的信道探测信号和已知的公开导频进行信道估计。在本文实现的密钥提取方案中,Alice 与 Bob 是两个对等的节点,双方角色可以互换,不失一般性,我们设定 Eve 在阶段 1 的监听对象为 Alice。Eve 启动被动窃听程序后,一直保持在监听状态,当接收到 Alice 发送的信道探测帧后,利用接收信号和已知的导频信息完成信道估计,信道估计算法同样采用 LS 估计。仍考虑合法双方进行第 $i$ 轮信道探测,此时 Eve 得到的第 $k$ 个子载波上的 CFR 估计为:

$$\hat{H}_{AE}(t_i,f_k)=H_{AE}(t_i,f_k)+\hat{Z}_E(t_i,f_k) \tag{9}$$

其中,$\hat{Z}_E(t_i,f_k)$ 为第 $k$ 个子载波上由噪声引入的估计误差,$H_{AE}$ 为 Alice 与 Eve 之间的 CFR。对比(4)、(9)两式,估计误差 $\hat{Z}_B$ 和 $\hat{Z}_E$ 为相互独立的 0 均值高斯变量;另外,依据 Jakes 信道模型可知,当 Eve 与 Bob 相距半个波长以上的距离时,合法信道 $H_{AB}$ 和窃听信道 $H_{AE}$ 是不相关的,此时 Eve 无法从自己的信道估计中获取到任何与合法信道相关的信息,从而可以保证密钥提取过程的安全性。

在阶段 3 中,Eve 监听合法双方发送的分组校验和 CRC 校验信息,并据此对自己量化得到的窃听初始密钥进行处理,来试图仿造出合法双方提取的共享密钥。针对合法双方信息协商阶段的两次分组校验和一次交织操作,Eve 采取的相应措施如下:

1)在 Alice 和 Bob 进行第一轮分组校验时,Eve 将己方的窃听初始密钥按照与合法节点相同的方式进行分组,同时监听并接收合法双方发送的分组校验数据,对比 Alice 和 Bob 的分组校验值,找到合法双方校验值不同的分组索引,然后将己方的窃听初始密钥中相应索引的分组删除;

2)完成第一轮分组校验后,Eve 按照与合法节点相同的方式执行交织操作;

3)在合法双方进行第二轮分组校验时,Eve 执行的操作与第一轮校验时相同;

4)完成两轮分组校验后,Eve 计算存留的窃听密钥的 CRC 校验值,同时监听并接收合法双方在公开信道上交互的 CRC 校验值。若己方 CRC 校验值与合法双方的 CRC 校验值一致,则说明合法双方密

钥提取成功，并且窃听成功；否则窃听失败，重新从阶段 1 开始执行。

总体而言，Eve 的被动窃听方案是针对 2.2 节中合法双方的密钥提取方案而设计的，该方案的主要目的是通过窃听合法节点的通信内容，仿造出合法通信双方提取的共享密钥，因此该方案的流程与合法节点的密钥提取方案高度匹配，方案中大部分的数据处理方法也尽可能模仿密钥提取方案，从而达到密钥仿造的目的。

## 3　基于 CSI 的密钥提取系统实现

基于 Zynq 架构实现的基于 CSI 的密钥提取原型系统如图 5 所示，系统中包括合法通信节点 Alice 和 Bob，以及被动窃听节点 Eve。每个节点由一台原理样机和一台笔记本构成，其中笔记本通过网线与原理样机连接，作为系统参数配置的控制台以及测试数据的导出和存储介质。原型系统中的原理样机工作在 TDD-OFDM 通信体制下，本节对原理样机的硬件架构和密钥提取原型系统实现进行详细介绍。

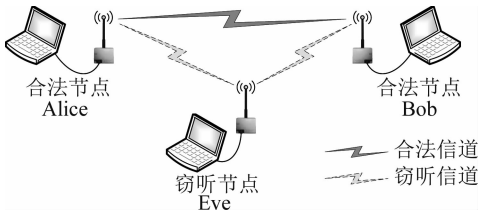



图 5　原型系统示意图

Fig. 5　Schematic diagram of prototype system

### 3.1　原理样机硬件架构

原理样机的外观结构如图 6 所示，包括样机主体模块、射频天线和供电电池三个部件。样机整体硬件架构分为基带、射频、接口和供电四个部分，如图 7 所示。基带部分用于射频信号的调制和解调，射频模块对射频信号进行放大和滤波处理，接口模块中包含了多种外设接口，供电部分则分布在上述三个模块中，负责硬件电路的稳压直流供电。

在原理样机的硬件架构中，基带部分是核心模块。样机的基带板主要包括四个部分：Z7030 片上系统（System on Chip，SoC）、AD9361 电路、外部接口电路和电源管理部分。每个部分的主要功能如下：

1）Z7030 SoC 芯片内部包含了处理系统（Processing System，PS）和可编程逻辑资源（Programmable Logic，PL）两个部分。原理样机的系统内核和驱


| | |
|---|---|
| 1: 射频天线接口(公) | 2: 射频天线接口(母) |
| 3: J30J数据网口 | 4: 电源输入接口 |
| 5: 电池放电接口 | 6: 电池充电接口 |

图 6　原理样机外观图

Fig. 6　Appearance diagram of the prototype

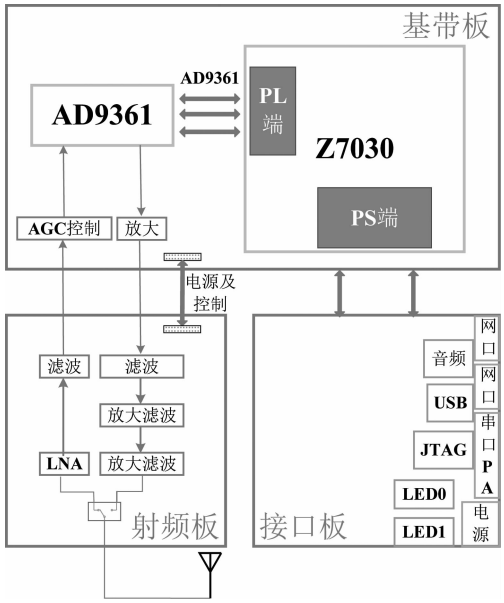



图 7　原理样机硬件架构

Fig. 7　The hardware architecture of prototype

动程序运行于 PS 部分，该部分集成了 ARM 核心、32 MB的 4-bit SPI 闪存、8 GB 的 eMMC 以及 521 MB 的 DDR3 RAM 存储器；而基带信号处理电路则由 PL 中的可编程逻辑资源构建。

2）AD9361 电路支持两发两收设计，芯片内含 12 比特位宽的 DAC 和 ADC。电路输出的发送信号经增益为 12 dB 的放大器后，输出功率为 0 dBm 的信号给射频模块；来自射频模块的接收信号经过 3 dB的数控衰减器，再经过一个限幅器后进入 AD9361。

3）外部接口电路，基带板集成了以太网 PHY 和

USB PHY 芯片,单板通过 PHY 转换后向接口模块输出差分对信号。

4)电源管理部分将来自接口模块的+5 V 电压转换为+1.0 V、+1.35 V、+1.8 V 和+3.3 V 的电压为 Zynq 芯片供电,并对外输出+1.8 V 和+3.3 V 电压。

### 3.2 原型系统实现

我们首先在上述硬件平台的物理层实现了 TDD-OFDM 通信体制,相关设计参数如表 1 所示。进一步,在已实现的 TDD-OFDM 通信体制基础上,实现了基于 CSI 密钥提取的原型系统。整个原型系统从功能上可以分为两个部分:密钥提取方案实现和被动窃听方案实现,所实现的两种方案分别运行在合法通信双方和被动窃听节点上。

表 1 OFDM 通信体制设计参数

Tab. 1 Design parameters of OFDM communication system

| 参数 | 参数值 |
|---|---|
| 载波频率/MHz | 1450 |
| 数字调制方式 | QPSK |
| FFT 点数 | 512 |
| 数据子载波数 | 408 |
| CP 长度 | 128 |
| OFDM 符号长度 | 640 |
| 基带采样率/MHz | 4 |
| 子载波频率间隔/kHz | 7.8125 |
| OFDM 符号时间/μs | 160 |

密钥提取方案实现流程如图 8 所示,具体流程如下:

1)合法通信双方利用接收信号中的导频符号和已知的导频数据得到合法信道的 CFR 估计,并将估计值推送至处理器;

2)合法节点的处理器中,CFR 估计值经过特征提取、预处理和量化过程,转化为二进制的初始密钥;

3)合法双方执行信息协商,通过在公共信道上交换初始密钥的校验数据,来消除初始密钥中的不一致比特,并通过 CRC 校验判断协商是否成功;

4)若信息协商成功,则合法双方利用 SHA-1 算法对协商后的密钥进行处理得到最终的共享密钥,否则,重新进行信道探测。

被动窃听方案实现流程如图 9 所示,窃听节点 Eve 运行第 2.3 节中提出的被动窃听方案,监听并接收来自合法通信双方的信道探测帧和信息协商的交互数据,并针对密钥提取流程的四个阶段实施相应的处理流程,从而试图仿造出合法双方提取的密钥。

## 4 系统测试及结果分析

按照图 5 搭建原型系统,系统中部署两个合法通信节点 Alice 和 Bob,以及两个与 Bob 相距不同距离的被动窃听节点 Eve1 和 Eve2。合法节点运行 2.2 节中设计的密钥提取方案,被动窃听节点运行 2.3 节中设计的被动窃听方案。

### 4.1 测试场景设置

为了充分研究基于 CSI 的密钥提取方案应用于

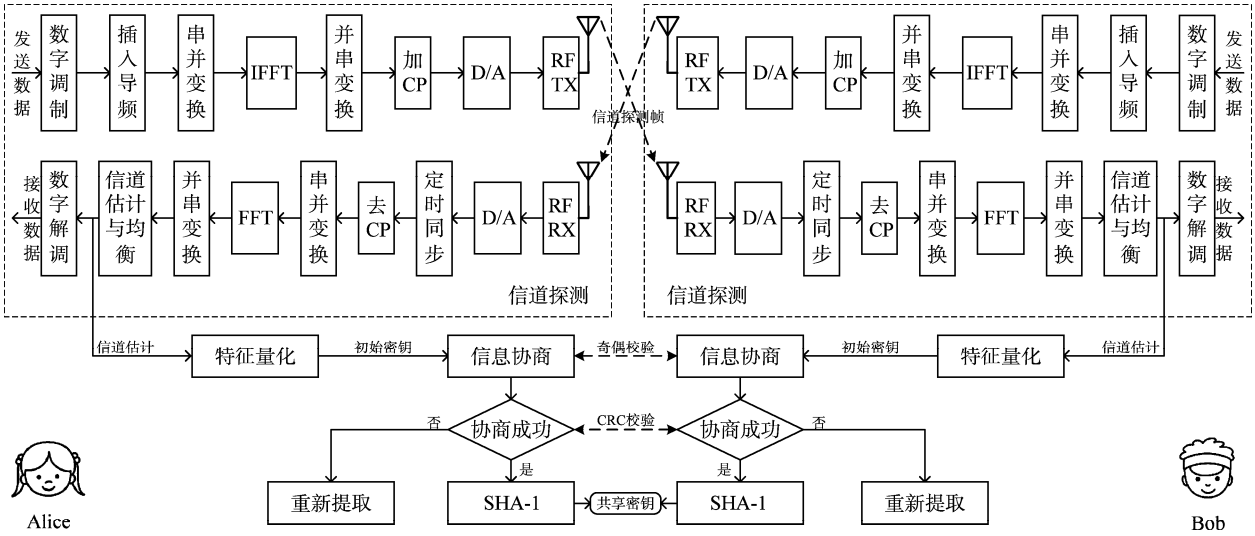



图 8 密钥提取方案实现框图

Fig. 8 Block diagram of the key extraction scheme

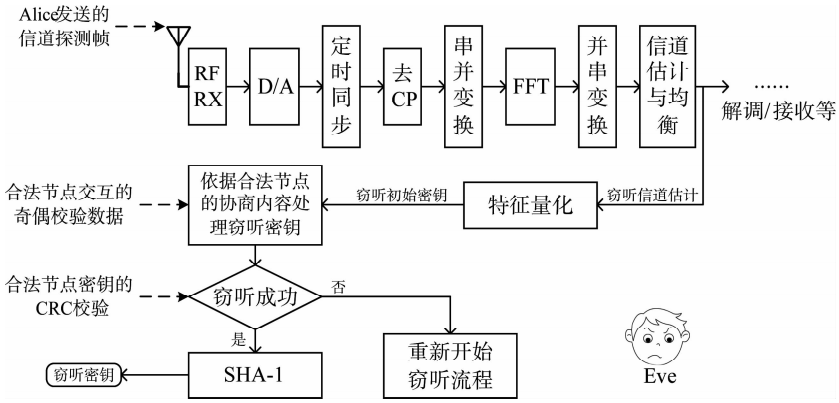



图 9　被动窃听方案实现框图

Fig. 9　Block diagram of the passive eavesdropping scheme

实际通信系统时的性能，本文的测试实验包括室内通信和室外通信两种典型通信测试环境，每种测试环境下又分为节点静止和节点运动两种情况，共计四种测试场景。在每种测试场景下，两个被动窃听节点分别部署在 Bob 周围的不同区域内：

1）Eve1 与 Bob 相距 1 个波长以内（<0.2 m）；

2）Eve2 部署在与 Bob 相距 30 ~ 50 个波长（6 ~ 10 m）的区域内。

图 10 为室内通信场景示意图，节点静止情况下两个合法节点 Alice 和 Bob 部署在图中所示位置；节点运动情况下，Alice 在图中标注的运动区域内做不规则运动，Bob 仍保持静止。室外通信场景的俯视图如图 11 所示，节点静止情况下两个合法节点所处位置以及节点运动情况下 Alice 的运动区域已在图上标出。

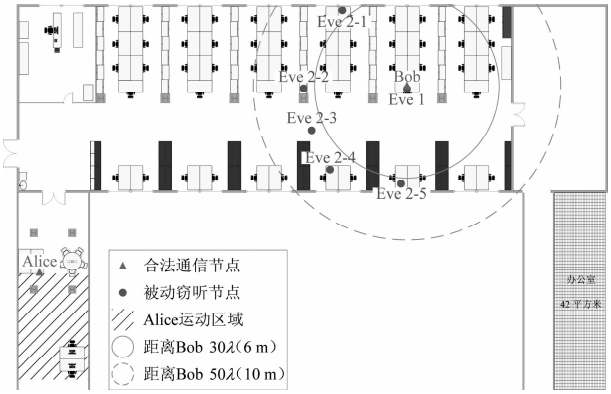



图 10　室内通信场景节点部署示意图

Fig. 10　Schematic diagram of node deployment in indoor communication scenario

在上述四种测试场景下，每种场景进行五组测试，在第 $i$ 组测试时，两个被动窃听节点分别部署在

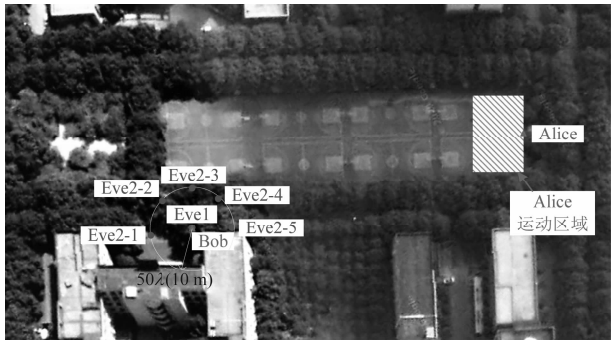



图 11　室外通信场景节点部署示意图

Fig. 11　Schematic diagram of node deployment in outdoor communication scenario

图 10 和图 11 所示的 Eve1 和 Eve2-$i$ 处，$i \in \{1,2,3,4,5\}$，即 Eve2 在五组测试中分别部署在划定区域内的五个不同位置上；每组测试包含若干次重复测试，每次测试持续 150 s。测试所得数据包括各节点的信道估计值和提取的密钥。本节后续的内容将对测试数据进行处理与分析，数据处理所得结果为各节点五组测试结果的统计平均。

### 4.2　信道特性分析

无线信道的短时互易性和时空唯一性是基于无线信道进行密钥提取的理论基础，通过对测试实验中合法节点的信道估计值进行分析，可以对实际通信场景下无线信道的上述性质进行验证和评估。为了使结果更加清晰，本文将时空唯一性分为时变性和空间去相关性两项内容分别进行分析。

#### 4.2.1　短时互易性

无线信道的短时互易性保证了同一信道两端的用户在相干时间内所观测到的信道衰落特性是几乎一致的，因此合法通信双方可以基于各自的信

道观测提取出一致的密钥。通过比较 Alice 和 Bob 在同一轮信道探测中所得信道估计的相似性,可以对无线信道的短时互易性进行评估。信道估计之间的相似性通常用相关系数来定量描述,假设 Alice 和 Bob 的信道估计分别为 $\hat{H}_A$ 和 $\hat{H}_B$,则两者之间的相关系数为:

$$\rho(\hat{H}_A,\hat{H}_B)=\frac{\mathrm{Cov}\ (\hat{H}_A,\hat{H}_B)}{\sqrt{\mathrm{Var}\ (\hat{H}_A)\mathrm{Var}\ (\hat{H}_B)}} \tag{10}$$

在设定的不同测试场景下,Alice 和 Bob 的信道估计之间的平均相关系数如图 12 所示。从测试结果可以看出,各实验场景下 Alice 和 Bob 的信道估计之间的相关系数均大于 0.87,这表明合法通信双方所获取到的信道估计值具有很好的一致性,从而验证了无线信道的短时互易性。此外,无论是在室内还是室外测试环境中,节点运动情况下的互易性比静止情况下略差,这是因为相较于节点静止的情况下,节点运动时的信道多普勒扩展变大,相干时间 $T_c$ 减小,Alice 和 Bob 在一定的时间间隔 $\Delta t(\ll T_c)$ 内获取到的信道估计相关性变小,这一点在后续的时变性分析中有明显体现。

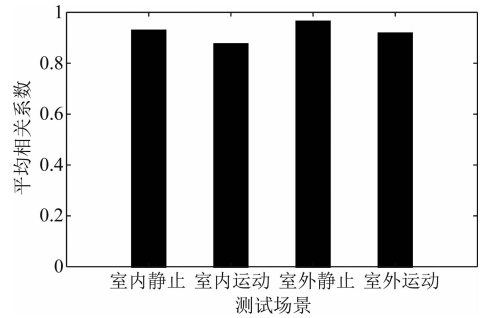



图 12 合法双方信道估计之间的平均相关系数

Fig. 12 Average correlation coefficient between the channel estimations of legitimate parties

### 4.2.2 时变性

无线信道的时变性是由环境中物体的运动或通信双方之间相对运动导致的,这保证了基于 CSI 提取的密钥可以得到持续更新。为了分析实际通信场景下的信道时变性,我们依次计算 Alice 在起始时刻 $t_1$ 所得信道估计 $\hat{H}_A(t_1)$ 与后续时刻 $t_1+\tau$ 所得信道估计 $\hat{H}_A(t_1+\tau)$ 之间的相关系数 $\rho(\hat{H}_A(t_1),\hat{H}_A(t_1+\tau))$,以下称为时间相关系数。

各场景下的平均时间相关系数曲线如图 13 所示。测试结果表明,在相同的测试环境中,节点运动情况下随着时间间隔 $\tau$ 的增大,信道的时间相关系数迅速降至 0.4 以下,而节点静止情况下,信道的时间相关系数下降缓慢,且始终保持在较高的水平,这验证了节点运动时信道具有较强的时变性,而节点静止情况下信道时变性较弱;在相同的节点状态下,室外环境下信道的时间相关系数比室内环境低,这是因为室外环境中运动物体较多,环境具有更强的动态性。

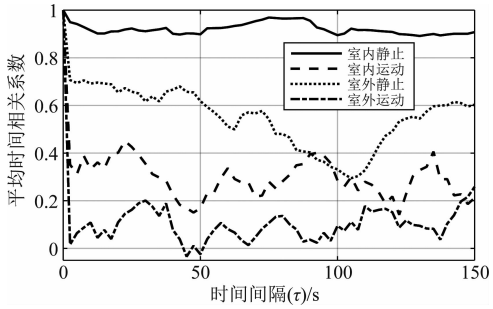



图 13 Alice 信道估计的平均时间相关系数

Fig. 13 Average time correlation coefficient of Alice's channel estimation

### 4.2.3 空间去相关性

在均匀散射环境下,两个相距半个波长以上的用户所接收到的来自同一发射机的信号经历了不相关的多径衰落,这意味着一个与合法节点相距半个波长以上的窃听节点无法获取到与合法信道相关的观测,从而保证了密钥提取的安全性。在本文的测试实验中,Bob 和 Eve 都是通过接收 Alice 的信道探测帧来进行信道估计,因此通过计算各场景下 Bob 的信道估计 $\hat{H}_B$ 与处于不同位置上的 Eve1、Eve2 的信道估计 $\hat{H}_{E1}$、$\hat{H}_{E2}$ 之间的相关系数 $\rho(\hat{H}_B,\hat{H}_{E1})$、$\rho(\hat{H}_B,\hat{H}_{E2})$,可以反映信道在空间上的去相关特性。

在设定的不同测试场景下,Bob 与 Eve1、Eve2 所得信道估计之间的平均相关系数如图 14 所示。从测试结果可以看出,在所有的测试场景下,与 Bob 相距较远的窃听者 Eve2 所获取的信道估计与 Bob 信道估计之间的相关系数明显低于 Eve1 与 Bob 信道估计之间的相关系数;且即使 Eve1 与 Bob 相距不足 1 个波长,其相关系数也均低于 0.5,明显低于 Alice 和 Bob 的信道估计相关系数(>0.87),以上结果验证了无线信道在空间上具有快速去相关特性。

表 2　密钥 NIST 随机性测试结果

Tab. 2　NIST randomness test results of keys

| 测试项 | 室内静止 | 室内运动 | 室外静止 | 室外运动 |
|---|---|---|---|---|
| Frequency | 0.7399 | 0.7399 | 0.5341 | 0.1223 |
| Block Frequency | 0.8343 | 0.2757 | 0.1223 | 0.0487 |
| Cumulative Sums | 0.0909, 0.7399 | 0.3505, 0.7399 | 0.8343, 0.9114 | 0.3505, 0.9114 |
| Runs | 0.1626 | 0.5341 | 0.7399 | 0.4373 |
| Longest Run of Ones | 0.0352 | 0.2757 | 0.0909 | 0.7399 |
| FFT | 0.0127 | 0.2133 | 0.1626 | 0.8343 |
| Approximate Entropy | 0.0000 | 0.3505 | 0.0487 | 0.0127 |
| Serial | 0.0000, 0.0002 | 0.3505, 0.0909 | 0.0909, 0.2757 | 0.2133, 0.3505 |

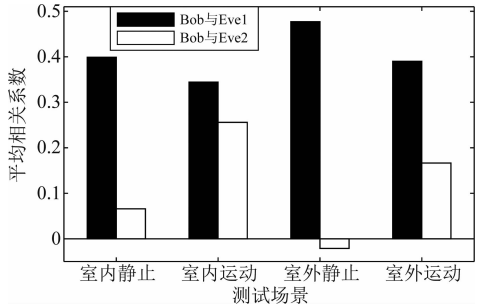



图 14　Bob 与不同位置上窃听节点的信道估计之间的平均相关系数

Fig. 14　Average correlation coefficient between Bob's channel estimation and those of the eavesdropping nodes deployed at different locations

### 4.3　密钥性能分析

#### 4.3.1　密钥随机性

随机性是对密钥序列最基本的要求，不满足随机性要求的密钥被敌方破解的概率会大大增加。本文采用 NIST 随机性测试工具来测试合法双方在不同场景下提取密钥的随机性，结果如表 2 所示。通常，若某一测试项的测试结果大于 0.01，则认为该项测试通过。从测试结果可以看出，在室内静止场景下，存在两项未通过的测试项，其余场景下提取的密钥均可以通过随机性测试。这说明本文的密钥提取方案在大多数场景下可以提取出符合随机性要求的密钥；而室内静止场景下信道响应的随机性较差，这与 4.2.1 节中得出的室内静止场景下信道时变性差的结论是相吻合的。

#### 4.3.2　密钥熵

密钥熵反映了密钥可以达到的安全强度，通常来说密钥熵值越高能够保证的安全强度就越高。本文通过计算密钥的近似熵，来评估文中实现的密钥提取方案在各种测试场景下提取出密钥的安全强度。密钥近似熵计算方法如下：

1）将长度为 $L$ 的密钥 $K_{AB}$ 的前 $m-1$ 个比特的副本补充到密钥 $K_{AB}$ 的结尾，得到一个长度为 $L+m-1$ 的新序列 $K'_{AB}$，其中 $m$ 为设定的子序列长度；

2）长度为 $m$ 的二进制序列共有 $2^m$ 个，记作 $s_j(j=1,2,\cdots,2^m)$，统计 $s_j$ 在序列 $K'_{AB}$ 的所有长度为 $m$ 的子序列中出现的次数 $\nu_j$；

3）计算 $\varphi_m=\sum_{j=1}^{2^m}\frac{\nu_j}{2^m}\ln\frac{\nu_j}{2^m}$；

4）将子序列长度改为 $m+1$，重复 1）至 3）的计算过程得到 $\varphi_{m+1}$；

5）归一化的密钥近似熵为：$\mathrm{ApEn}=(\varphi_m-\varphi_{m+1})/\ln 2$。

从每个测试场景下提取的所有密钥中随机选取 500 个密钥组成密钥流，并按照上述方法计算密钥流的归一化近似熵，然后重复进行 100 次随机选取和归一化近似熵计算操作，得到各场景下的平均归一化近似熵如表 3 所示。密钥的归一化近似熵越接近 1，表示密钥的无序性越强，则安全强度越高。从各场景测试实验所提取的密钥的近似熵来看，室内静止场景下由于时变性较差，且可分辨的多径数较少，所得密钥熵稍低；其余场景下的均可达到 0.7 左右的密钥熵，这表明本文的密钥提取方案所提取出的密钥具有一定的安全强度。

表 3　密钥归一化近似熵

Tab. 3　Normalized approximate entropy of keys

| 测试场景 | 室内静止 | 室内运动 | 室外静止 | 室外运动 |
|---|---|---|---|---|
| 近似熵 | 0.6351 | 0.6858 | 0.6920 | 0.7209 |

#### 4.3.3　密钥提取速率

为了评估本文所实现的密钥提取方案的执行效率，我们计算了各场景下的平均密钥提取速率，

计算方法为:对于某一测试场景,首先计算单次密钥提取用时,即从发送信道探测帧到完成信息协商的时间间隔;然后,用信息协商成功后所得密钥长度除以单次密钥提取用时得到单次密钥提取速率;最后,对该场景下所有密钥的单次密钥提取速率取平均得到平均密钥提取速率。

不同测试场景下的平均密钥提取速率如表 4 所示,可以看出基于 CSI 的密钥提取可以实现较高的密钥提取速率,这说明基于 CSI 的物理层密钥提取方案能够保证密钥的持续更新,从而提供良好的前向安全性。此外,在相同的测试环境中,节点运动情况下的密钥速率比节点静止时略低,原因是节点运动时信道互易性有所下降,合法双方的信道估计相似性变差,经过对信道估计的量化后得到的一致密钥比特数减少,从而使得密钥提取速率有一定的降低。

表 4 密钥提取速率

Tab. 4 Key extraction rate

| 测试场景 | 室内静止 | 室内运动 | 室外静止 | 室外运动 |
|---|---|---|---|---|
| 密钥提取速率/bps | 431.05 | 412.49 | 440.59 | 410.44 |

### 4.4 安全性分析

当通信环境中存在被动窃听者时,基于 CSI 的密钥提取方案的安全性取决于在密钥提取过程中的信息泄露情况,而在整个密钥提取过程中可能存在信息泄露的阶段为信道探测和信息协商,针对这两个阶段,我们分别利用测试实验中三个节点的信道估计和信息协商后的密钥,分析密钥提取方案的信息泄露情况,从而评估方案的安全性。

#### 4.4.1 信道信息泄露率

在信道探测过程中,为了分析各种通信场景下 Eve 在不同位置时能够获取到的合法信道相关的信息量,我们分别在窃听者存在和不存在两种情况下计算密钥容量,并由这两种密钥容量定义信道信息泄露率。密钥容量是合法通信双方提取安全密钥的速率上界,可以从信息论的角度定量描述密钥提取性能。

如图 15 所示,$\hat{H}_A$ 和 $\hat{H}_B$ 分别表示 Alice 和 Bob 对合法信道的估计,$\hat{H}_E$ 表示 Eve 通过监听合法节点的信道探测帧获取的信道估计。在不考虑窃听者 Eve 的情况下,合法通信双方可以达到的密钥容量即为双方信道估计之间的互信息:

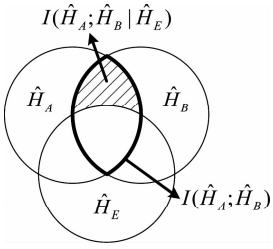



图 15 密钥容量示意图

Fig. 15 Schematic diagram of key capacity

$$C=I(\hat{H}_A;\hat{H}_B)=\log_2\frac{|\boldsymbol{R}_A||\boldsymbol{R}_B|}{|\boldsymbol{R}_{AB}|} \tag{11}$$

其中,$|\cdot|$ 表示行列式,$\boldsymbol{R}_{X_1X_2\cdots X_n}=\mathrm{Cov}(\hat{H}_{X_1},\hat{H}_{X_2},\cdots,\hat{H}_{X_n})$ 为信道协方差矩阵,$X_1,X_2,\cdots,X_n\in\{A,B,E\}$。

进一步考虑窃听者 Eve 存在的情况,此时 Alice 和 Bob 之间的安全密钥容量为:

$$C_s=\min\{I(\hat{H}_A;\hat{H}_B),I(\hat{H}_A;\hat{H}_B|\hat{H}_E)\} \tag{12}$$

其中,

$$I(\hat{H}_A;\hat{H}_B|\hat{H}_E)=\log_2\frac{|\boldsymbol{R}_{AE}||\boldsymbol{R}_{BE}|}{|\boldsymbol{R}_E||\boldsymbol{R}_{ABE}|} \tag{13}$$

利用 $C$ 和 $C_s$,本文定义信道信息泄露率为:

$$\gamma_H=1-\frac{C_s}{C} \tag{14}$$

表示信道探测阶段向 Eve 泄露的信息量占合法双方密钥容量的比例。

不同测试场景下,Eve1 和 Eve2 处的信道信息泄露率如图 16 所示。观察可得,在所有的测试场景下,Eve1 信道信息泄露率均低于 0.25,且在大部分场景下低于 0.2,这说明在实际测试中,即使窃听节点 Eve 与合法节点 Bob 相距不足 1 个波长,Eve 通过窃听合法双方的信道探测帧而获取到的与合法信道相关的信息也十分有限。此外,Alice 和 Bob 向

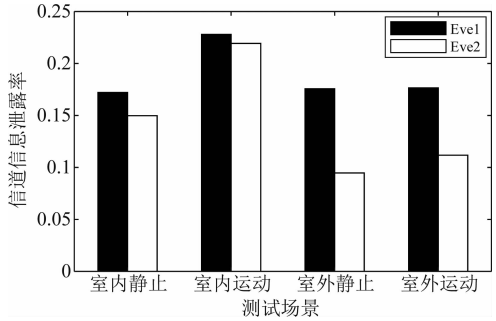



图 16 不同窃听节点处的信道信息泄露率

Fig. 16 Channel information leakage rate at different eavesdropping nodes

Eve2 的信道信息泄露率低于向 Eve1 的泄露率，这与信道的空间去相关性的测试结果相吻合。

### 4.4.2　窃听方密钥错误率

在信息协商阶段，Alice 和 Bob 为了消除量化后所得初始密钥的中的不一致比特，需要在公共信道上交换密钥校验值，这一过程也会向 Eve 泄露一定量的信息。为了评估经过信息协商后所得密钥的安全性，本文定义窃听方密钥错误率为 Eve 仿造的密钥与合法双方提取密钥中不一致的比特数占密钥长度的比例：

$$\gamma_e=\frac{\sum(K_{AB}\oplus K_E)}{L} \tag{15}$$

其中，$K_{AB}$ 和 $K_E$ 分别为合法双方和 Eve 在信息协商后所得到的密钥，$L$ 为密钥长度，⊕表示逐位异或运算。

不同测试场景下，Eve1 和 Eve2 的窃听方密钥错误率如图 17 所示，观察测试结果可以看出，一方面 Eve1 通过窃听合法节点的通信内容所实现的窃听方密钥错误率在 0.1 以上，这说明在实际通信场景下，即使窃听节点与合法节点十分接近，也很难完全仿造出合法双方提取的密钥；另一方面，室外测试环境下窃听方密钥错误率明显高于室内环境，这说明本文方案在信道多径丰富的场景下具有更高的安全性。

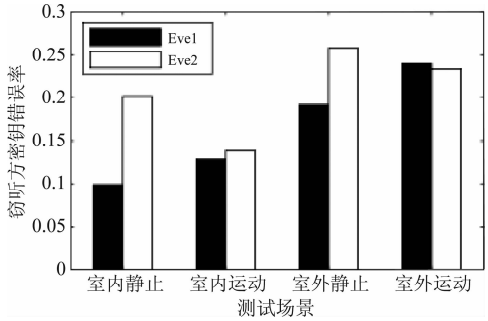



图 17　窃听方密钥错误率

Fig. 17　Key error rate of eavesdroppers

## 5　结论

本文在 TDD-OFDM 通信体制下，设计了一种基于 CSI 的密钥提取方案，并根据该方案为潜在的窃听节点设计了一种针对性的被动窃听方案。依据所提密钥提取方案及窃听方案，本文基于 Zynq 架构完成了合法节点和窃听节点的原理样机设计，并实现了基于 CSI 的密钥提取原型系统。基于实现的原型系统，我们进行了大量的测试实验，并对实验结果进行了全面分析。首先，通过分析实际测试中各节点的信道估计，验证了实际通信场景下无线信道的短时互易性、时变性和空间去相关性；然后，通过对合法通信双方在不同测试场景下提取的密钥进行分析，可以发现所提方案能够实现较高的密钥提取速率，且在大多数测试场景下提取的密钥符合随机性要求，并具有较高的密钥熵；最后，通过对密钥提取过程中合法信道信息泄露情况和窃听节点最终仿造的密钥结果进行分析，表明了基于 CSI 的密钥提取方案在存在窃听节点的场景下具有较强的安全性能。综合对密钥性能和安全性的分析，也进一步验证了基于 CSI 的密钥提取方案在实际通信场景中应用的可行性。

### 参考文献

[1] MUSA S M. Network security and cryptography [M]. Dulles, VA: Mercury Learning and Information, 2018: 111-138.

[2] ZHAN Furui, ZHAO Zixiang, CHEN Yuhua, et al. On the using of Rényi's quadratic entropy for physical layer key generation [J]. Computer Communications, 2019, 137: 32-43.

[3] 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 15th Annual International Conference on Mobile Computing and Networking. ACM, 2009: 321-332.

[4] ZHANG Junqing, WOODS R, DUONG T Q, et al. Experimental study on key generation for physical layer security in wireless communications [J]. IEEE Access, 2016, 4: 4464-4477.

[5] GOLDSMITH A. Wireless communications [M]. New York, NY: Cambridge University Press, 2005: 64-98.

[6] ZHANG Junqing, DUONG T Q, MARSHALL A, et al. Key generation from wireless channels: A review [J]. IEEE Access, 2016, 4: 614-626.

[7] 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. ACM, 2008: 128-139.

[8] PATWARI N, CROFT J, JANA S, et al. High-rate uncorrelated bit extraction for shared secret key generation

from channel measurements[J]. IEEE Transactions on Mobile Computing, 2010, 9(1): 17-30.

[9] RUOTSALAINEN H, ZHANG Junqing, GREBENIUK S. Experimental investigation on wireless key generation for low-power wide-area networks[J]. IEEE Internet of Things Journal, 2020, 7(3): 1745-1755.

[10] ROTTENBERG F, NGUYEN T-H, DRICOT J-M, et al. CSI-based versus RSS-based secret-key generation under correlated eavesdropping[J]. IEEE Transactions on Communications, 2020, DOI: 10.1109/TCOMM.2020.3040434.

[11] PENG Yuexing, WANG Peng, XIANG Wei, et al. Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels [J]. IEEE Transactions on Wireless Communications, 2017, 16(8): 5176-5186.

[12] 余训健, 吴晓富, 周雪倩. 无线密钥产生中的 Karhunen-Loève 变换去相关性研究[J]. 信号处理, 2016, 32(10): 1225-1232.
YU Xunjian, WU Xiaofu, ZHOU Xueqian. Decorrelation of Wireless Channel Coefficients for Secret Key Generation with Karhunen-Loève Transform[J]. Journal of Signal Processing, 2016, 32(10): 1225-1232. (in Chinese)

[13] ZHAN Furui, YAO Nianmin, GAO Zhenguo, et al. Efficient key generation leveraging wireless channel reciprocity for MANETs[J]. Journal of Network and Computer Applications, 2018, 103: 18-28.

[14] EL HAJJ SHEHADEH Y, ALFANDI O, HOGREFE D. Towards robust key extraction from multipath wireless channels[J]. Journal of Communications and Networks, 2012, 14(4): 385-395.

[15] 张孝甜, 赵生妹, 郑宝玉. 无线信道中的 Polar 码协商[J]. 信号处理, 2018, 34(7): 793-798.
ZHANG Xiaotian, ZHAO Shengmei, ZHENG Baoyu. Key Reconciliation Using Polar Code in Wireless Channel [J]. Journal of Signal Processing, 2018, 34(7): 793-798. (in Chinese)

[16] YULIANA M, WIRAWAN, SUWADI. An efficient key generation for the Internet of Things based synchronized quantization[J]. Sensors, 2019, 19(12): 2674.

[17] AONO T, HIGUCHI K, OHIRA T, et al. Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels[J]. IEEE Transactions on Antennas and Propagation, 2005, 53(11): 3776-3784.

[18] PREMNATH S N, JANA S, CROFT J, et al. Secret key extraction from wireless signal strength in real environments[J]. IEEE Transactions on Mobile Computing, 2013, 12(5): 917-930.

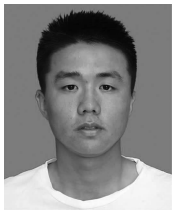
[19] XI Wei, DUAN M, BAI Xiuxiu, et al. KEEP: Secure and efficient communication for distributed IoT devices[J]. IEEE Internet of Things Journal, 2020, DOI: 10.1109/JIOT.2020.3011558.

[20] 袁瑞, 彭林宁, 李古月, 等. 不同环境下无线信道密钥生成性能研究[J]. 密码学报, 2020, 7(2): 261-273.
YUAN Rui, PENG Linning, LI Guyue, et al. On Key Generation Performance of Wireless Channel in Different Environments[J]. Journal of Cryptologic Research, 2020, 7(2): 261-273. (in Chinese)

## 作者简介

**郭登科** 男, 1996 年生, 山东临邑人。国防科技大学电子科学学院硕士研究生, 主要研究方向为无线物理层安全。
E-mail: guodengke18@nudt.edu.cn

**熊 俊** 男, 1987 年生, 江西丰城人。国防科技大学电子科学学院副研究员, 博士, 硕士生导师, 主要研究方向为通信信号处理与资源分配、物理层安全、认知无线电网络等。
E-mail: xj8765@nudt.edu.cn



**高玉威** 男, 1996 年生, 江西宜春人。国防科技大学电子科学学院硕士研究生, 主要研究方向为无线物理层安全。
E-mail: cruzgao@163.com

**曹 阔** 男, 1990 年生, 湖南汨罗人。国防科技大学电子科学学院讲师, 博士, 主要研究方向为协同通信、无线物理层安全等。
E-mail: caokuo90@sina.cn

**马东堂** 男, 1969 年生, 安徽灵璧人。国防科技大学电子科学学院教授, 博士, 博士生导师, 主要研究方向为宽带通信与网络、物理层安全、认知无线电与认知网络等。
E-mail: dongtangma@nudt.edu.cn