



文章编号:1001-9081(2019)06-1780-06

DOI:10.11772/j.issn.1001-9081.2018102120

基于通用软件无线电外设的 OFDM 信道物理密钥量化分析

丁 宁^{*}, 管新荣, 杨炜伟

(中国人民解放军陆军工程大学 通信工程学院, 南京 210007)

(* 通信作者电子邮箱 dingningmtn@163.com)

摘要:为了对比分析实测数据下单门限量化算法与双门限量化算法的性能差异,并通过优化量化参数改善物理密钥性能,采用通用软件无线电外设(USRP)搭建了正交频分复用(OFDM)系统,通过信道估计提取信道幅度特征作为密钥源(实测数据),从密钥一致性、密钥随机性和密钥剩余长度三个方面分析了两种量化算法的性能。基于实测数据得到了单门限量化和双门限量化下密钥一致性、密钥随机性和密钥剩余长度仿真结果。仿真结果表明:在单门限量化算法中,在给定密钥随机性约束下存在最优量化门限使得密钥不一致率最低;在双门限量化算法中,存在最优量化因子使得有效密钥长度最大化;结合 Cascade 密钥协商算法进行协商时,不同量化算法的密钥一致性与密钥生成速率存在折中关系。

关键词:物理层密钥;量化;通用软件无线电外设;正交频分复用系统

中图分类号: TP393.09 文献标志码:A

Quantitative analysis of physical secret key in OFDM channel based on universal software radio peripheral

DING Ning^{*}, GUAN Xinrong, YANG Weiwei

(College of Communications Engineering, Army Engineering University of PLA, Nanjing Jiangsu 210007, China)

Abstract: In order to compare and analyze the performance of single threshold quantization algorithm and double thresholds quantization algorithm on measured data and improve the performance of physical secret key by optimizing the quantization parameters, an Orthogonal Frequency Division Multiplexing (OFDM) system was built by Universal Software Radio Peripheral (USR). The channel amplitude feature was extracted as the key source through channel estimation and the performance of the two quantization algorithms was analyzed in terms of consistency, randomness and residual length of secret key. The simulation results of consistency, randomness and residual length of secret key under single threshold quantization and double thresholds quantization were obtained based on measured data. The results show that single threshold quantization algorithm has the optimal quantization threshold to minimize the key inconsistency rate under the given key randomness constraint, double thresholds quantization algorithm has the optimal quantization factor to maximize the effective secret key length, and when Cascade key negotiation algorithm is used for negotiation, there is a trade-off relation between secret key consistency and secret key generation rate in different quantization algorithms.

Key words: physical layer secret key; quantification; Universal Software Radio Peripheral (USR); Orthogonal Frequency Division Multiplexing (OFDM) system

0 引言

随着无线通信技术的发展,无线通信安全问题备受关注。由于无线信道的开放性使其易受到第三方的窃听和攻击。传统的安全加密方案面临诸多挑战,例如:在动态无线网络中对称加密面临密钥分发问题;在物联网(Internet of Things, IoT)设备中资源有限导致无法负担加密算法高计算成本的开销;此外,随着计算机计算能力的增强,使得应用于无线通信网络的诸如 A5/1 和 A5/3 算法可以在短时间内破解^[1-2]。另一方面,近年来物理层密钥技术受到广泛关注,相较于传统安全加密方案具有以下优势:1)由于信道的短时互易性,合法通

信双方独立在线地生成物理密钥,不需预先分发密钥,避免了传统密钥方案中的密钥预分发和管理问题。2)由于信道的空时唯一性,使得不同时间、不同空间位置的无线信道特征唯一不可复制,从而保证密钥的机密性。3)因物理密钥基于无线信道的动态随机性,而不依赖于计算问题的复杂性,可实现“一次一密”,确保通信的绝对安全。4)因物理密钥可直接从信道特征中提取生成,而不需复杂的加密算法,适用于资源受限的设备。

物理层密钥生成技术的理论研究可以追溯到 20 世纪 90 年代初期。1993 年,文献[3]提出了当合法用户的信道条件不如窃听者信道条件时,合法用户仍可以利用相关的随机源

收稿日期:2018-10-22;修回日期:2019-01-03;录用日期:2019-01-04。

基金项目:国家自然科学基金项目资助项目(61471393, 61501512);江苏省青年基金资助项目(BK20150718)。

作者简介:丁宁(1992—),男,江苏南京人,硕士研究生,主要研究方向:无线物理层安全; 管新荣(1987—),男,江西于都人,讲师,博士,主要研究方向:物理层安全、无线密钥生成、协同通信、认知无线电网络; 杨炜伟(1981—),男,四川名山人,副教授,博士,主要研究方向:正交频域复用系统、通信中的信号处理、协同通信、认知网络、网络安全。



提取密钥实现安全通信。通常,物理层密钥生成技术主要包括信道探测、量化、密钥协商和隐私放大四个步骤。考虑信道特征测量值的非互易性和冗余性等问题,还可以增加预处理和熵估计两个步骤。

1)信道探测,即采集 Alice 和 Bob 通信双方之间的信道特征信息,常用于物理层密钥生成的信道特征包括:信道状态信息(Channel State Information, CSI)^[4]、接收信号强度^[5]、相位^[6]以及多径时延^[7]等。

2)量化是通信双方将采集到的信道特征信息量化成比特序列。因此,量化的目的是在尽可能降低通信双方量化后比特序列不一致率的同时保证密钥生成速率。现有的文献研究主要通过设计不同的量化算法来增强密钥的一致性。文献[8]分析对比经典量化算法的性能包括均匀量化、等概量化及最小均方误差量化,并指出等概量化最终能生成更长的密钥长度,且量化输出的0、1比特等概分布,因而是一种简单而实用的方法。文献[9]采用单门限的量化方法且使用了LCA(Level Crossing Algorithm),使得每个信道测量值可以产生1bit密钥。单门限量化方法在门限值附近量化出错概率较高,且在信道变化缓慢时密钥随机性较差。为此,文献[4]采用双门限量化方法,将介于高阈值和低阈值之间的测量值舍弃。该方法以牺牲一定密钥生成速率为代价,换取了量化比特序列的高一致性。同时,文献[3]提出的多比特量化算法可提升密钥生成速率,但量化比特序列的一致性也相应下降。因此,文献[10]提出了带奇偶校验的多比特量化算法,其在校验位错误时,将舍弃量化后的比特序列,从而提高密钥的一致性。文献[11]研究了自适应量化方法,将一方的量化噪声在共有信道上共享从而另一方用在适应地调整量化门限。文献[12]研究了多维信息的矢量量化,该方法适用于多输入多输出及多用户通信系统的密钥生成过程。文献[13]针对矢量量化存在的量化边界问题进行研究。一般而言,量化过程中密钥不一致率和密钥生成速率之间不可调和的矛盾总是存在的。

3)经过量化后,密钥协商是进一步产生可用密钥的关键步骤。密钥协商的目的是纠正通信双方初始密钥中不一致的比特,使得 Alice 和 Bob 通信双方具有相同的密钥比特序列。文献[14]提出 Cascade 协议,合法双方通过交换密钥分组后的奇偶校验值并使用二分法进行查找纠错。由于二分法纠错过程需要合法双方多次进行信息交换,因而对网络延时等信道参数较为敏感^[15]。文献[16]提出 Winnow 协商算法,利用汉明码伴随式矩阵进行前向纠错,虽然降低协商信息交互次数,但纠错效率也相对降低。

4)隐私放大的目的是防止窃听者利用信息协商中泄露的部分信息推断出任何密钥信息。文献[17]最早提出了隐私放大的概念,并在窃听模型的基础上设计出了隐私放大的机制。该机制依赖于一个隐私放大函数的构建,即 $g: (0, 1)^n \rightarrow (0, 1)^r$ ($n > r$)。隐私放大函数通过将物理密钥长度由 n 压缩为 r 以消除在公开信道上泄露的信息。文献[17]基于通用 Hash 函数构造了隐私放大函数 g ,将 n 比特输入映射为 r 比特输出。文献[18]给出了隐私放大可行性的理论分析,并探讨了通用 Hash 函数在实际中的应用。

然而,从现有的文献观察,都是对各种量化算法进行仿真分析,缺乏对这些量化算法在实测数据下的性能进行分析和

比较。文献[19]通过通用软件无线电外设(Universal Software Radio Peripheral, USRP)平台实测数据提取密钥生成。文献[20]提出一种新的回环传输方案,并通过 USRP 平台验证此方案可以有效地消除用于密钥生成的 CSI 非互易性。本文采用 USRP 软件无线电设备,在 LabVIEW 平台下搭建正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)系统并编程实现 125 个子载波的信道状态信息提取^[21],对实际测量的 OFDM 幅度进行单门限量化包括等概量化和均匀量化与双门限量化,并根据密钥的一致性、密钥随机性和初始密剩余钥长度三个评价指标来综合评价量化算法的实际性能。仿真结果表明:单门限量化方法中,等概量化的密钥随机性优于均匀量化,但均匀量化相较于等概量化获得更低的密钥不一致率(Key Disagreement Rate, KDR),在给定密钥随机性约束条件下,根据密钥一致性最大化找出最优的量化门限;双门限量化方法比单门限量化方法获得更低的密钥不一致率,但生成密钥长度减小且受门限量化因子 α 影响较大。为了综合考虑密钥的一致性和密钥生成速率,文中定义了有效密钥长度 L 全面评价双门限量化因子 α 的影响,并根据有效密钥长度最大化找到最优的量化因子,进而结合密钥协商步骤中的 Cascade 算法综合考虑各量化算法在整个密钥生成过程中的实际性能。

1 量化算法

量化实质上就是一个模数转换的过程,目的是合法双方同时对估计的信道状态信息进行量化处理,从而使得合法双方得到一致比特序列。以下分别具体介绍了单门限量化算法中的均匀量化算法、等概量化算法和双门限量化算法。

1.1 均匀量化算法

均匀量化是把取值空间等间隔地分为多个区间,然后对相应的区间进行量化。假设量化器的输入信号为 x 的取值范围是 $x \in [a_L, a_M]$,其概率密度函数为 $p(x)$,于是:

$$\int_{a_L}^{a_M} p(x) dx = 1 \quad (1)$$

如图 1 所示,将量化器的阶数记为 J ,判决电平为 d_k ($k = 0, 1, \dots, J$)。当均匀量化器的输入满足 $d_k < x \leq d_{k+1}$ 时,则量化器的设计如下:

$$\begin{cases} \Delta = d_{k+1} - d_k \\ y_k = (d_{k+1} + d_k)/2 \end{cases}; \quad k = 0, 1, \dots, J-1 \quad (2)$$

其中: Δ 为区间间隔,均匀量化器的平均输出信噪比会随着量化阶数 J 的增加而增大。与此同时,如果给定输出电平 y_k 和判决电平 d_k ,则不同的输入信号会导致不一样的量化误差,当输入信号幅值较小时,对应的量化误差会增大,因此量化误差最小的量化器是非均匀的。

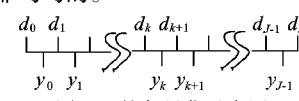


图 1 均匀量化示意图

Fig. 1 Schematic diagram of uniform quantization

1.2 等概量化算法

等概量化是根据待量化参数的统计特性来选择量化电平,使得采样值落在每个量化区间的概率相等,这种量化方式可以得到 0、1 等概的密钥比特序列。量化门限 $\{d_k; k = 0, 1, \dots, J\}$ 根据:



$$\int_{-\infty}^{d_k} p(x) dx = k/J \quad (3)$$

对于均值为0、方差为1的高斯分布, d_k 满足:

$$\int_{-\infty}^{d_k} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx = \frac{k}{J} \quad (4)$$

此外,当输入信号 x 服从均匀分布时,等概量化与均匀量化等价。

1.3 双门限量化算法

单门限量化方法在门限值附近量化出错概率较高,而双门限量化方法将上下门限之间的测量值舍弃,从而得到较高的一致率。

合法双方 Alice 和 Bob 分别对信道进行独立探测,得到随机序列 $X^A = (X_1, X_2, \dots, X_n), Y^B = (Y_1, Y_2, \dots, Y_n)$, 根据门限上下门限 q_+^i 和 q_-^i ($i \in (A, B)$) 形成双门限量化器:

$$\begin{cases} q_+^i = E(U) + \alpha \cdot \sigma(U) \\ q_-^i = E(U) - \alpha \cdot \sigma(U) \end{cases} \quad (5)$$

对于 Alice, 序列 $U = X^A$, q_+^i 和 q_-^i 分别为 Alice 进行量化时的上下门限; 对于 Bob, 序列 $U = Y^B$, q_+^i 和 q_-^i 分别为 Bob 进行量化时的上下门限。 $E(U)$ 和 $\sigma(U)$ 分别表示随机序列的均值和标准差, 量化因子 α 用来控制量化器的门限值。将序列 X^A 和 X^B 分别输入 Alice、Bob 的量化器进行量化:

$$\psi(x) = \begin{cases} 1, & x > q_+^i \\ 0, & x < q_-^i \\ e, & \text{其他} \end{cases} \quad (6)$$

式中: e 代表一个无效采样点对应的量化结果; 上标 i 代表用户。双方将位置索引的集合 $T_A = \{K: q_-^A \leq x_i \leq q_+^A\}$ 和 $T_B = \{K: q_-^B \leq x_i \leq q_+^B\}$ 在公开信道上交互, 删除 $T = T_A \cup T_B$ 对应位置的采样值, 将剩余 0、1 比特序列生成密钥。由此可见, 随着量化因子 α 的增大, 删除的采样值也增多, 从而导致密钥生成速率降低。

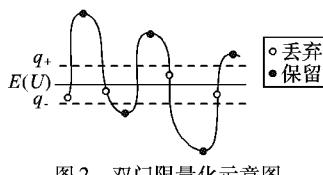


图 2 双门限量化示意图

Fig. 2 Schematic diagram of double thresholds quantization

2 基于 USRP 的 OFDM 系统搭建

USRP 是一款灵活的无线电设备, 它由一块主板和最多四块子板构成。USRP 包含母板和前端子板。母板主要完成信号从模拟到数字转换、基带信号的生成、与 PC 的通信功能, 它处理数字基带和中频信号。子板主要负责处理不同频带的射频信号, 并进行射频、中频信号之间的转换。

本文采用两台单天线 USRP 设备搭建 OFDM 通信系统, 不仅需要 USRP 驱动函数对 USRP 进行相关参数配置以设备与主机之间的通信, 还需要调用 LabVIEW 工具包构建数字通信的发射模块和接收模块。系统的配置参数如表 1 所示。其中载波频率参数选择是根据 USRP-2920 所支持的工作频段 (50 MHz ~ 2.2 GHz) 来设定的, 载波频率选择 2 GHz 可用于室内环境实验测量, 且最大的输出功率范围在 30 mW ~ 70 mW, 在室内环境下发送功率较小, 不影响其他设备的正常通信。

受 USRP 设备自身处理信号能力的影响, I/Q 符号速率设置为 500 KS/s, 如果设置采样速率过快, 则影响开发板的处理速度, 所以选择较为适中的 I/Q 采样速率。按照一帧 OFDM 符号的设计要求分别设置各项参数长度。发送天线和接收天线分别具有两个通道, 分别是 TX_1、TX_2 和 RX_1、RX_2。其中通道 1 既可以作为发送天线也可以作为接收天线使用, 而通道 2 只能作为接收天线使用。发送天线及通道号设置为 TX_1, 接收天线及通道号设置为 RX_1。

表 1 系统参数配置

Tab. 1 System parameter configuration

参数	设置	参数	设置
载波频率	2 GHz	FFT 变换长度	$FFT_size = 256$
I/Q 符号速率	500 KS/s	循环前缀长度	$CP_size = 64$
一帧 OFDM 符号数	$Nofdm_symbols = 20$	粗同步序列长度	$SIF_size = 160$
数据位长度	$Data_size = 1000$	精同步序列长度	$LTF_size = 160$
虚拟子载波数	$Null_tones = 106$	发射天线通道	TX_1
导频长度	$Pilot_size = 125$	接收天线通道	RX_1

2.1 程序流程

发送端和接收端流程如图 3 所示。配置 USRP 参数包括激活的 USRP 设备编号, 激活的天线和通道号等。在发送端, 信源经过正交振幅调制 (Quadrature Amplitude Modulation, QAM) 和串/并转换处理后, 进入 OFDM 调制阶段, 需要加入导频、虚拟子载波、快速傅里叶逆变换 (Inverse Fast Fourier Transform, IFFT)、加入循环前缀、加入同步序列, 调制后的并行数据流再经过并/串转换后送入 USRP, 同时驱动 USRP 发送信号。发射信号经过无线信道衰落后到达接收端, 在接收端驱动 USRP 接收信号, 对接收到的信号进行同步处理, 数据进入 OFDM 解调阶段, 即需要去除循环前缀、FFT、去除虚拟子载波、信道估计、信道均衡、QAM 解调, 接收端接收信号完毕并关闭 USRP。

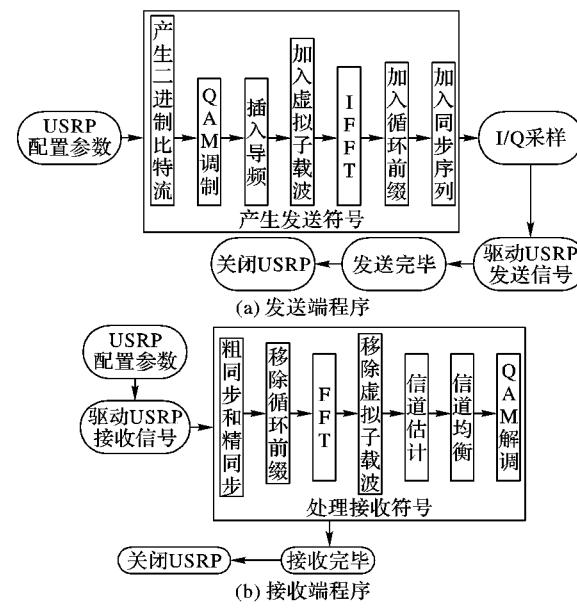


Fig. 3 Flow chart of OFDM transmitter and receiver

2.2 编程实现与数据采集

本系统基于 LabVIEW 软件, 搭建了通信发射链路和接收



链路模块。图4程序是对发送数据进行组包,随机序列发生器产生1000比特随机序列,经过4QAM调制后输出500符号映射,然后将500符号分20组,每组25个符号数据。

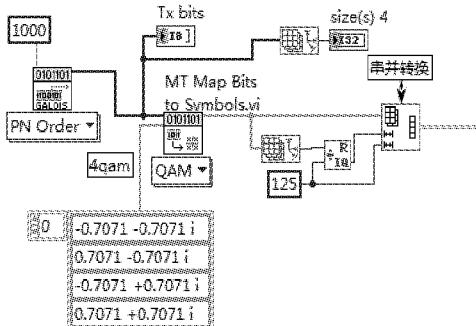


图4 数据组包
Fig. 4 Data package

图5是将125个导频按序插入每组数据后,添加106位虚拟子载波。紧接着做IFFT,变换到时域之后添加64位循环前缀。最后分别添加粗同步和精同步序列,经过并串转换形成一帧待发送的OFDM符号。

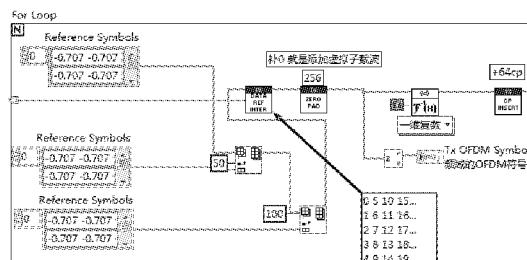


图5 OFDM帧符号设计
Fig. 5 OFDM frame symbol design

图6展示LabVIEW前面板接收端的显示界面,分别显示:接收端的接收参数、I/Q采样值、功率谱密度、均衡前后的星座图以及接收到的数据比特。

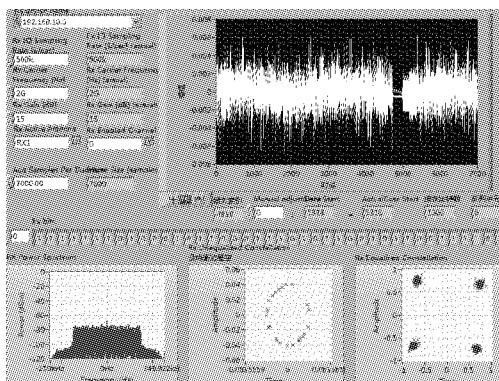
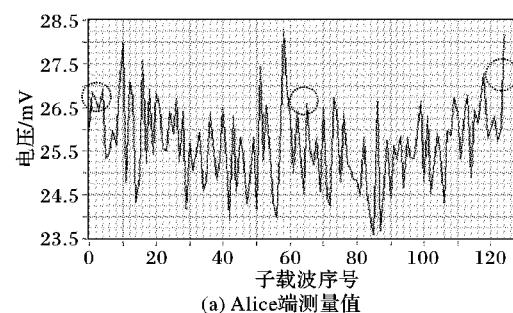


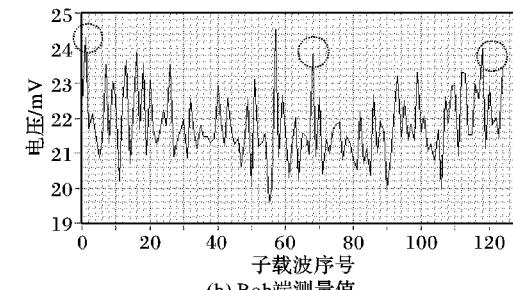
图6 接收面板显示
Fig. 6 Receive panel display

图7分别显示了Alice和Bob端在室内环境下的OFDM信道测量幅值。载波频率2 GHz,天线增益15 dB的参数条件下,由于受到非对称的硬件指纹和噪声等因素的影响,测量得到上下行的子载波幅值有所偏差,个别子载波幅值差异较大,在图中用圆圈标记处。

图8给出了上下行信道探测后归一化的幅值。由图8可知,合法双方提取的信道特征信息是强相关的,可以用于后续量化算法对比分析。



(a) Alice端测量值



(b) Bob端测量值

图7 信道上下行探测值
Fig. 7 Channel uplink and downlink detection value

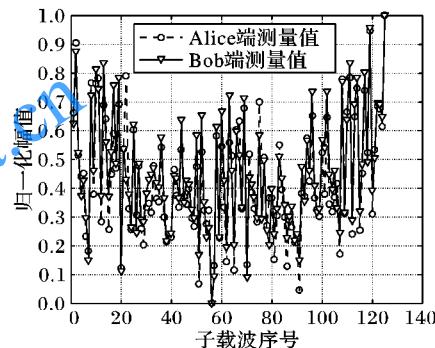


图8 归一化幅值

Fig. 8 Normalized amplitude value

3 性能比较

利用上述USRP平台下采集的OFDM系统的信道信息进行量化,单门限量化和双门限量化方法均采用1比特量化。采用初始密钥不一致率(记为 P_D)、初始密钥随机性(以0,1占比衡量,记为 R)和初始密钥剩余长度(记为 η)三个评价指标,综合评价各种量化算法优劣性。

3.1 量化性能对比

图9给出了在天线增益为15 dB情况下单门限量化的初始密钥不一致率和1比特所占比例曲线,图中分别标出了均匀量化门限值和等概量化门限值,等概量化门限值为0.3613,均匀量化门限值为0.5。可以看出:1)等概量化门限值小于均匀量化且等概量化得到的初始密钥不一致率比均匀量化高。从初始密钥不一致率 P_D 上看,均匀量化的一致性优于等概量化。2)等概量化输出的比特序列中0,1等概分布,而均匀量化得到比特序列中1比特占比较少,即等概量化的随机性比均匀量化要好。

在选择最优门限的时候,既要考虑量化输出密钥比特序列的一致率,也要考虑输出比特序列的随机性。可以将这个问题建模为:

$$\min(P_D)$$



$$\text{s. t. } 0.5 - \Delta \leq R \leq 0.5 + \Delta \quad (7)$$

即在随机性满足约束条件下,最小化初始密钥不一致率 P_D 。当 Δ 取值较小时,认为初始密钥比特序列的随机性较好。如图 9 所示,当 Δ 设定为 0.1,也就是要求 $0.4 \leq R \leq 0.6$ 时,初始密钥不一致率 P_D 单调递减,当 $R = 0.6$ 时取得最小值。此时所对应的门限值就是最优门限值,最优门限为 0.4210 取得的位置。不难发现,等概量化和均匀量化均不是最优量化门限,最优门限在等概门限和均匀门限之间。

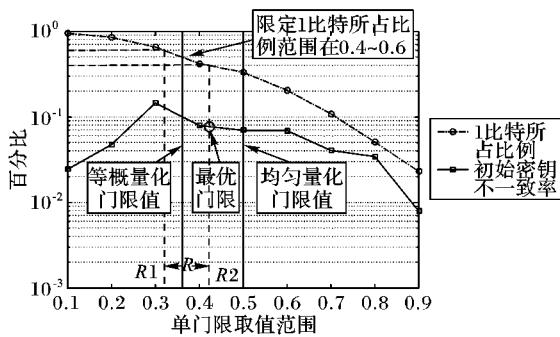


图 9 单门限量化对比

Fig. 9 Comparison of single threshold quantization

各种量化方式下初始密钥不一致率如图 10 所示。首先,各种量化方式的初始密钥不一致率 P_D 均随着天线增益增大而减小。其次,双门限量化得到初始密钥不一致率明显低于单门限量化方法,表明双门限量化方法可以进一步降低初始密钥不一致率 P_D 。最后正如前文所述,双门限量化得到初始密钥不一致率 P_D 随着门限量化因子 α 的增大而减小。

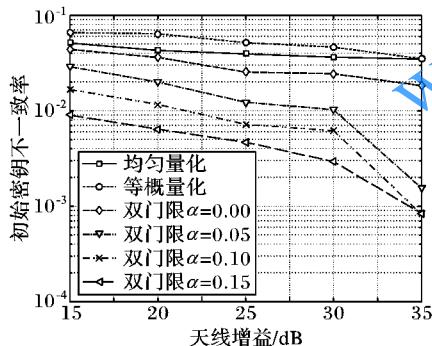


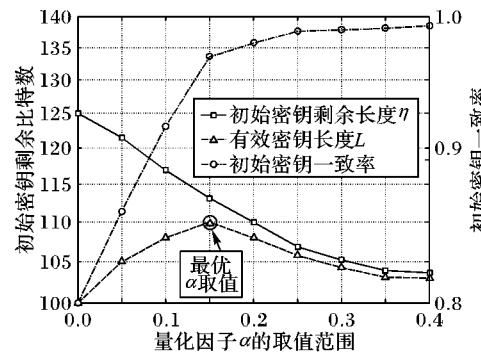
图 10 不同量化方式下初始密钥不一致率

Fig. 10 Initial key inconsistency rate in different quantization modes

在双门限量化过程中,门限的选择尤为关键,门限的选择影响到最终的量化性能。不能仅为了降低初始密钥不一致率 P_D 而不断增大门限量化因子 α 。当量化因子 α 增大,其中无效采样点也增多,使生成密钥比特数量减少,从而导致密钥生成速率降低。因此,有必要对双门限量化过程中的量化因子 α 进行讨论研究。图 11 给出了初始密钥剩余比特数和初始密钥一致率随着量化因子 α 的变化情况。如图 11 所示,随着量化因子 α 值的不断增大,初始密钥的一致率在不断增高,与此同时,初始密钥剩余比特数也在不断降低。这是因为,随着量化因子 α 的增加,合法双方进行量化时需要同时删除更多的采样值,因此长度会减小。由于双方删除了量化时容易产生不一样的采样值,所以量化后的比特序列的一致率会更高。为了综合评价双门限量化因子同时对初始密钥不一致率和初始密钥长度的影响,本文定义了有效密钥长度 L 来评价量化性能,则双方采样值能够生成的有效密钥长度 L 为:

$$L = \eta \times (1 - P_D) \quad (8)$$

由图 11 可以看出,选择不同的量化因子 α 对应不同的 L 和 P_D ,这样初始密钥剩余长度 η 和初始密钥不一致率 P_D 之间就会存在折中最优问题。图 11 中,有效密钥长度 L 随着量化因子 α 先增大后减小;在量化因子 α 取值为 0.15 时,有效密钥长度 L 取得最大值,即此时 α 为最优量化因子。

图 11 量化性能随 α 的变化情况Fig. 11 Changes of quantization performance with α

3.2 采用 Cascade 协商算法的性能对比

采用 Cascade 密钥协商算法^[14]可以进一步降低初始密钥不一致率 P_D ,通过多轮反复的纠正错误比特实现。主要步骤包括:第一轮通过二分法进行纠错,把所有含有奇数个错误比特的分组都纠正一个错误,确保每个分组都不含有错误比特或者含有偶数个错误比特;在之后的第 $i > 1$ 轮中, Alice 和 Bob 对密钥按随机序列打乱分组,再次比较每组的奇偶校验值并用二分法进行纠错,此时若发现了一个新错误比特,则在之前一轮中对应的分组内必会含有奇数个错误比特,对该分组再次进行二分法纠错,使得纠正的比特数倍增,提高密钥协商效率。

图 12 给出了协商后的密钥不一致率随着协商次数的变化情况。如图 12 所示,采用 Cascade 协商算法,分别给出量化因子 α 为 0.05、0.10 和 0.15 下对应的协商次数与不一致率。随着 α 的增加,协商次数不断减少。如: α 取值为 0.15 时,Alice 和 Bob 双方只需要 3 次协商就能达到生成的密钥完全一致;而 α 取值为 0.10 时双方需要 4 次协商;当 α 为 0.05 时,则需要多于 4 次的协商次数,虽然此时初始密钥有效长度 L 较大,但是双方不一致率 P_D 较高而导致协商阶段交互次数增加,从而导致双方在交互同时泄露更多的信息量,并且安全性和时间开销的增加。

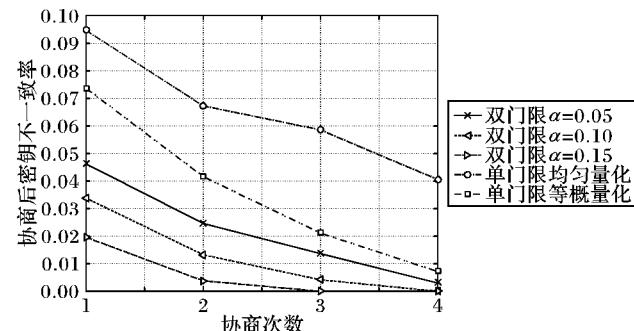


图 12 协商次数对不一致率的影响

Fig. 12 Impact of number of negotiations on inconsistency rate

综上所述,在评价双门限量化方法时,不仅需要从量化整体性能去考虑量化因子 α 的取值,还需要结合协商步骤综



合考虑对最终密钥生成效率的影响,根据不同的场景选择相应的量化因子 α 。例如:在IoT应用场景中,低能耗的特点要求生成密钥不一致率 P_D 较低,而低速率的特点则对应低的密钥生成速率。此时,可以选择较大的双门限量化因子 α ,使得生成密钥具有较低的不一致率 P_D ,不仅减少了后续协商次数,还节省了发射功率。

4 结语

本文利用USRP设备搭建了OFDM系统并进行信道估计,将采集的信道幅度测量值用于量化算法分析;分析对比单门限量化方法中均匀量化和等概量化方法的性能,针对双门限量化提出有效密钥长度 L 指标并结合协商步骤,全面评价量化因子对密钥生成的影响。本文仅选择较为常用的量化算法对比分析OFDM信道幅度特征,后续可以用OFDM信道相位特征对比分析,还可以考虑其他量化算法的应用性能。

参考文献(References)

- [1] 李古月. 无线通信物理层安全理论与方法研究[D]. 南京: 东南大学, 2017: 18–22. (LI G Y. Research on physical layer security theory and method in wireless communication [D]. Nanjing: Southeast University, 2017: 18–22.)
- [2] BIRYUKOV A, SHAMIR A, WAGNER D. Real time cryptanalysis of A5/1 on a PC [C]// FSE 2000: Proceedings of the 7th International Workshop on Fast Software Encryption, LNCS 1978. Berlin: Springer, 2000: 1–18.
- [3] MAURER U M. Secret key agreement by public discussion from common information [J]. IEEE Transactions on Information Theory, 1993, 39(3): 733–742.
- [4] MATHUR S, TRAPPE W, MANDAYAM N, et al. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel [C]// MobiCom 2008: Proceedings of the 14th Annual International Conference on Mobile Computing and Networking. New York: 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 environment [C]// MobiCom 2009: Proceedings of the 15th Annual International Conference on Mobile Computing and Networking. New York: ACM, 2009: 321–332.
- [6] HASSAN A A, STARK W E, HERSHY J E, et al. Cryptographic key agreement for mobile radio [J]. Digital Signal Processing, 1996, 6(4): 207–212.
- [7] 周百鹏. 基于无线信道特征提取的密钥生成技术研究[D]. 郑州: 信息工程大学, 2011: 21–29. (ZHOU B P. Research on secret key generation utilizing the wireless channel characteristics [D]. Zhengzhou: Information Engineering University, 2011: 21–29.)
- [8] 蔡文炳. 基于无线信道特性生成密钥的理论限及量化方法研究[D]. 郑州: 信息工程大学, 2013: 35–43. (CAI W B. Research on theoretical limit and quantization methods in secret key generation based on characteristics of wireless channel [D]. Zhengzhou: Information Engineering University, 2013: 35–43.)
- [9] PAWAR S, EL ROUAYHEB S, RAMCHANDRAN K. Securing dynamic distributed storage systems against eavesdropping and adversarial attacks [J]. IEEE Transactions on Information Theory, 2011, 57(10): 6734–6753.
- [10] ALI S T, SIVARAMAN V, OSTRY D. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices [J]. IEEE Transactions on Mobile Computing, 2014, 13(12): 2763–2776.
- [11] DAI Q, LIANG J, HUANG K Z. Adaptive key generation based on quantization of channel characteristics [C]// Proceedings of the 2013 IEEE Third International Conference on Information Science and Technology. Piscataway, NJ: IEEE, 2013: 1512–1517.
- [12] SUNG C K, SUZUKI H, COLLINGS I B. Channel quantization using constellation based codebooks for multiuser MIMO-OFDM [J]. IEEE Transactions on Communications, 2014, 62(2): 578–589.
- [13] HONG Y W P, HUANG L M, LI H T. Vector quantization and clustered key mapping for channel-based secret key generation [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(5): 1170–1181.
- [14] BRASSARD C, SALVAIL L. Secret key reconciliation by public discussion [C]// EUROCRYPT 1993: Proceedings of the 1993 Workshop on the Theory and Application Of Cryptographic Techniques on Advances in Cryptology, LNCS 765. Berlin: Springer, 1994: 410–423.
- [15] MARTINEZ-MATEO J, ELKOUSS D, MARTIN V. Key reconciliation for high performance quantum key distribution [J]. Scientific Reports, 2013, 3(4): Article 1576.
- [16] ZHAO F, FU M X, WANG F Q, et al. Error reconciliation for practical quantum cryptography [J]. Optik, 2007, 118(10): 502–506.
- [17] BENNETT C, BRASSARD G, ROBERT J. Privacy amplification by public discussion [J]. SIAM Journal on Computing, 1988, 17(2): 210–229.
- [18] BENNETT C H, BRASSARD G, CREPEAU C, et al. Generalized privacy amplification [J]. IEEE Transactions on Information Theory, 1995, 41(6): 1915–1923.
- [19] 程伟, 谢非佚, 张腾月, 等. 基于USRP与OFDM信道响应的密钥提取实现[J]. 通信技术, 2017, 50(3): 513–519. (CHENG W, XIE F Y, ZHANG T Y, et al. Realization of key extraction based on USRP and OFDM channel response [J]. Communication Technology, 2017, 50(3): 513–519.)
- [20] PENG L N, LI G Y, HU A Q. Channel reciprocity improvement of secret key generation with loop-back transmissions [C]// Proceedings of the 2017 IEEE International Conference on Communication Technology. Piscataway, NJ: IEEE, 2017: 193–198.
- [21] PENG Y X, WANG P, XIANG W, 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.

This work is partially supported by the National Natural Science Foundation of China (61471393, 61501512), the Jiangsu Youth Fund Project (BK20150718).

DING Ning, born in 1992, M. S. candidate. His research interests include mobile cloud wireless physical layer security.

GUAN Xinrong, born in 1987, Ph. D., lecturer. His research interests include physical layer security, wireless key generation, cooperative communication, cognitive radio network.

YANG Weiwei, born in 1981, Ph. D., associate professor. His research interests include orthogonal frequency multiplexing system, signal processing in communication, cooperative communication, cognitive network, network security.