doi:10.3772/j.issn.1002-0470.2020.05.002

物理层安全中无线信号强度的非均匀量化方案①

徐志江②[*,****] 王晓敏[*] 卢为党[*] 陈芳妮[**] 华惊宇[***] 贡 毅③[****]

([*]浙江工业大学信息工程学院 杭州 310023)

([**]浙江科技学院信息与电子工程学院 杭州 310023)

([***]浙江工商大学信息与电子工程学院 杭州 310018)

([****]南方科技大学电子与电气工程系广东省普通高校先进无线通信技术重点实验室 深圳 518055)

摘 要 利用无线信道的互易性和随机性来生成物理层安全密钥,以保护传输数据的安全性。在给定的无线信号强度高斯分布模型下,通过数值计算推导出了理论上均匀量化的密钥匹配率,指出均匀量化是一种失配率最高的量化方案。基于此,提出了一种非均匀量化方案,将信道测量的强度量化为多个比特值,并给出相应的密钥失配率。实验和仿真结果表明,所提出的非均匀量化方案优于均匀量化方案。

关键词 物理层安全;高斯分布;接收信号强度(RSS);非均匀量化;密钥失配率

0 引 言

传统上,数据是通过经典加密方案[1,2]来保证信息的安全传输。这些密码算法比较复杂,窃听者破解密码系统所要花费的时间成本很大,因此可以保证信息的安全性。然而,随着计算机软硬件技术的发展,这种基于计算的安全性可能会不成立。利用物理层的随机性来生成无线设备间的密钥,近年来引起了极大的关注。与传统的密码学不同,通过无线信道物理层产生的密钥可以保证通信双方之间的信道与其他信道不相关[3,4]。

Maurer[5]提出根据无线信道互易性的特性建立信道模型,大量研究工作致力于开发各种物理层安全技术。为了提高信息传输过程中的安全性,采用复杂的信号处理技术来提高保密能力是非常重要的,例如人工噪声[6]的辅助技术、面向安全的波束成形技术[7-9]、协作中继的安全方法[10]等。在物理层密钥生成过程中,合法通信双方提取合适的信道参数,如信道响应幅度[11]、相位差异[12]以及信道增益和延迟[13]等,再对测量的信道参数进行量化,以此获得通信双方共享密钥的初始比特串。无线信道的互易性定理保证了信道测量值在上下行信道上是一致的。然而,加性噪声、无线信道的半双工性质以及器件的差异性导致实际信道的非互易性,密钥生成过程中存在失配率问题。秦艳琳等人[14]通过对密钥协商协议的改进,且没有使用双线性对运算,因此在确保安全性的同时具有较高的运算效率。Ali等人[15]通过链路端点的识别,得出信道测量不一致的主要原因是非同时测量,提出了一种实用的过滤方案以提高通信双方的信号相关性。Ambekar等人[16]提出一种无线自组织网络的密钥管理系统,通过在量化之前对接收信号强度的预处理以改善信道的互易性。同时,采用多比特量化方案用来提高密钥生成率。多数研究已经通过使用信道模型分析来解决问题,瑞利、莱斯和高斯等统计信道衰落模型已经被应用。Tope等人[3]提出高斯统计信道模型。Patwari等人[11]提出一种多比特自适应的量化方法

① 国家自然科学基金(61871348,61601409)和深圳市科技计划(JSGG20180508151852303)资助项目。

② 男,1973年生,博士,副教授;研究方向:物理层安全;E-mail:zyfxzj@zjut.edu.cn

③ 通信作者,E-mail:gongy@sustech.edu.cn

(收稿日期:2019-01-25)

对信道测量值进行编码，并且在进行理论分析时把收发双方的接收信号强度（received signal strength，RSS）建模为零均值的联合高斯分布，其方案使得密钥失配率大大下降。

Liu 等人[17]使用了均匀量化的方法量化密钥。通过 Mathematica 的数值计算分析，发现均匀量化是密钥失配率最高的情况。本文提出了一种非均匀多比特量化方案，着重于测量信道信息幅度数据的量化，然后得出密钥序列。仿真及实验结果表明，非均匀多比特量化方法密钥失配率低于均匀多比特量化密钥失配率。

论文的结构安排如下。第 1 节介绍了系统模型及密钥的经典生成过程。第 2 节通过 RSS 累积分布函数具体阐述量化分割阈值得出的过程，然后用 Mathematica 数值计算，得出在给定 RSS 模型条件下，均匀量化是密钥失配率较高的一种量化方案。提出了一种非均匀的量化方法，给出了其失配率的理论公式。第 3 节通过实测验证了 RSS 模型的假设是合理的，通过实验和 Matlab 仿真，表明了所提出的非均匀量化方案失配率小于均匀量化的方案。第 4 节是结论。

1 RSS 模型及密钥生成过程

无线信道具有互易性、时变性和空变性等特点，这些特点保证了合法通信双方可以利用无线信道作为相关随机信源，提取并共享密钥。假设合法通信双方工作在时分双工（time division duplex，TDD）通信模式下，通信双方首先在相干时间内完成对无线信道特性的双向探测（如通过发送导频信号），然后利用接收信号对信道进行估计，随后通过量化、信息协商以及私密放大等步骤，生成用于加密通信的共享密钥比特串。

1.1 上下行信号强度

在 TDD 通信模式下 Alice、Bob、Eve 分别表示为合法发送方、合法接收方和窃听者。无线通信因为其固有的广播特性，在其信号覆盖范围内的任何用户都能接收，所以其安全问题显得尤为重要。利用无线信道的不可预测性和随机性为物理层加密方案提供了条件。在相干时间内，可以合理地假设无线信道的信息状态是不变的。根据信道互易性定理，只要通信双方在该时间段内完成测量，可以认为双方的信道信息状态是一致的。若通信双方相距为电磁波波长以上的距离，一般可以认为双方所对应的信道特征是完全独立不相干的。若窃听者 Eve 与合法通信双方 Alice 或 Bob 之间的距离大于波长的一半，就可以保证 Alice 和 Bob 之间的信道信息不会被窃取。

具体地，对于 Alice 和 Bob 的 RSS（单位为 dB）建模为正态分布，即 $R_i \sim N(\mu_i, \sigma_i^2)$，$i \in \{A, B\}$；其上下行信道的 RSS 具有互易性，建模为 2 维高斯分布，其联合概率密度函数为

$$f(R_A, R_B, \rho) = N(\mu_A, \mu_B, \sigma_A^2, \sigma_B^2, \rho) = \frac{1}{2\pi\sigma_A\sigma_B\sqrt{1-\rho^2}} \times \exp\left\{-\frac{1}{2(1-\rho^2)}\left[\frac{(R_A-\mu_A)^2}{\sigma_A^2} - \frac{2\rho(R_A-\mu_A)(R_B-\mu_B)}{\sigma_A\sigma_B} + \frac{(R_B-\mu_B)^2}{\sigma_B^2}\right]\right\} \tag{1}$$

其中，用于度量上下行信道关联程度的相关系数 ρ 定义为

$$\rho = \frac{E[R_A R_B] - E[R_A]E[R_B]}{\sigma_A\sigma_B} \tag{2}$$

这里 μ_i，σ_i^2，$i \in \{A, B\}$ 分别表示 Alice 和 Bob 接收到 RSS 的均值与方差。从理论上讲，无线链路的上下行信道测量应该是相同的。然而，由于信道噪声、无线信道的半双工性质以及物理器件的不一致性等因素造成测量值的不一致，从而存在密钥失配率问题。本文中，使用相关系数来表示互易程度的大小。当 $\rho = 0$ 表示上下行信道相互独立，不存在互易性；当 $\rho = 1$ 时表示上下行信道完全互易。

1.2 密钥生成过程

获取共享密钥的典型流程，主要包括以下 4 个步骤。

（1）信道测量：合法通信方 Alice 和 Bob 通过接收信号交替测量公共信道，进而获取两者之间的无线信道随着时间的变化值。

（2）量化：将测量值用不同的量化方法，转换成为一串二进制密钥比特。这是本文讨论的对象。

（3）信息调和：尽管可以采用信号预处理算法

来改善信道测量的互相关性,但量化后 Alice 和 Bob 之间仍然存在不一致的密钥比特。可以使用信息调和技术来纠正两端生成的密钥比特的差异。

(4) 隐私放大:由于一些信息在信息调和部分公开传输,导致窃听者也可以得到,可能会危及到密钥序列的安全性,所以要通过隐私放大加强密钥的安全性。

2 密钥失配率的理论分析

在 1.1 节给定的 RSS 模型条件下,推导出了 2 电平量化的理论失配率;以 4 电平量化为例,给出了以量化电平为变量的失配率函数,分析得到均匀量化是一种失配率最高的量化方法这一结论,然后提出了一种非均匀量化方法来降低密钥失配率。

2.1 均匀量化方法

随机过程理论指出,给定一个具有累积分布函数为 $F_X(x)$ 的随机变量 X, 构造函数 $g(x) = F_X(x)$, 使得随机变量 $Y = g(X)$ 服从[0,1]均匀分布,即 $Y = F_X(X) \sim U(0, 1)$。基于此,均匀量化方法是: 假定 RSS 的累积分布函数 $F_X(x)$ 已知,在[0, 1]上等间隔划分成 M 个区间,则对接收到的 RSS 进行均匀量化的端点为 $\{F_X^{-1}(k/M),\ k = 0,1,\cdots,M\}$, $F_X^{-1}(\cdot)$ 是累积分布函数的逆函数。在本文中,RSS 建模为高斯分布,因此构造函数为

$$g(x) = F(x) = \frac{1}{2}\mathrm{Erfc}\left(\frac{\mu - x}{\sqrt{2}\sigma}\right) \tag{3}$$

其中,互补误差函数定义为 $\mathrm{Erfc}(z) = \frac{2}{\sqrt{\pi}}\int_z^{\infty} e^{-t^2}\mathrm{d}t$。

2 电平量化的失配率推导如下。Alice 和 Bob 都以自己接收到的 RSS 的均值 μ 为量化分界线,也即量化区间为 $S_{0,i} = (-\infty, \mu_i]$, $S_{1,i} = (\mu_i, +\infty)$, $i = \{A, B\}$。以 Alice 和 Bob 的 RSS 构成的 2 维笛卡尔坐标系中,量化在 $(S_{0,A}, S_{1,B})$ 和 $(S_{1,A}, S_{0,B})$ 区间时,量化比特是失配的。失配的概率为

$$\begin{aligned}&\Pr(S_{0,A}, S_{1,B})\\ &= \Pr(S_{1,A}, S_{0,B}) = \Pr(R_A < \mu_A, R_B > \mu_B)\\ &= \Pr(R_A - \mu_A < 0, R_B - \mu_B > 0)\\ &\triangleq \Pr(R_{NA} < 0, R_{NB} > 0) = \int_0^{\infty}\int_{-\infty}^{0} \frac{1}{2\pi\sqrt{1-\rho^2}}\\ &\exp\left\{-\frac{1}{2(1-\rho^2)}[x^2 - 2\rho xy + y^2]\right\}\mathrm{d}x\mathrm{d}y\\ &\triangleq \int_0^{\infty}\int_{-\infty}^{0} g(x, y, \rho)\mathrm{d}x\mathrm{d}y = \frac{\arccos(\rho)}{2\pi}\end{aligned} \tag{4}$$

其中 R_{NA}、R_{NB} 是 R_A、R_B 经过标准正态分布处理后得到的,即:

$$R_{Ni} = \frac{R_i - \mu_i}{\sigma_i},\ i = \{A, B\} \tag{5}$$

因此 2 电平量化的密钥失配率为

$$\Pr(\rho, \sigma_A, \sigma_B) = \frac{\arccos(\rho)}{\pi} \tag{6}$$

对于多比特量化的情况,以 4 电平量化为例,推导量化分割阈值与失配率之间的关系。假设量化编码为格雷编码,即相邻区间相差 1 比特。相应的量化区间编码为 00、01、11 和 10。4 电平量化区间如图 1 所示,图中的 R_{NA} 和 R_{NB} 经过式(5)标准化处理,类比式(4)的计算过程可以得出,此时的量化区间的范围和均值 μ 是不相关的。本文的计算过程也验证了 Patwari 等人[11]将通信双方建模为零均值的联合高斯分布的原因。因此 4 量化电平的简洁示意图如图 1 所示。

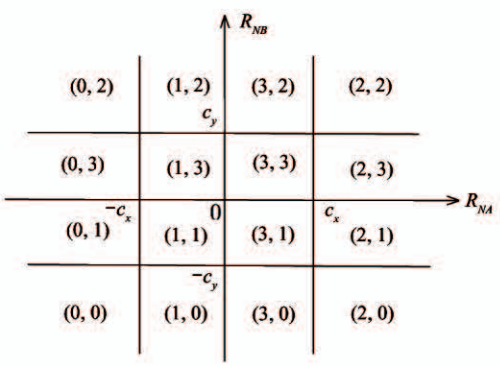

图 1 4 电平任意量化示意图

如果 $R_{NA} \in (-\infty, -c_x)$ 区间,则 Alice 编码为 00。此时,假设 $R_{NB} \in (-c_y, 0)$, Bob 编码为 01。Alice 和 Bob 只有一个量化比特不同,并且它们的对应概率是 Alice 和 Bob 的联合概率密度函数在该区间上的积分的一半。从图 1 中,可以比较直观地得出 4 电平量化的密钥失配率为

$$
\begin{aligned}
&2\Pr(Q_{RA} \neq Q_{RB}) \\
&= \int_{c_y}^{+\infty} \mathrm{d}y\left(\int_{-\infty}^{-c_x} g(x, y, \rho)\,\mathrm{d}x + 2\int_{-c_x}^{0} g(x, y, \rho)\,\mathrm{d}x\right. \\
&\quad \left. + \int_{0}^{c_x} g(x, y, \rho)\,\mathrm{d}x\right) + \int_{0}^{c_y} \mathrm{d}y\left(2\int_{-\infty}^{-c_x} g(x, y, \rho)\,\mathrm{d}x\right. \\
&\quad \left. + \int_{-c_x}^{0} g(x, y, \rho)\,\mathrm{d}x + \int_{c_x}^{\infty} g(x, y, \rho)\,\mathrm{d}x\right) \\
&\quad + \int_{-c_y}^{0} \mathrm{d}y\left(\int_{-\infty}^{-c_x} g(x,y,\rho)\,\mathrm{d}x + \int_{0}^{c_x} g(x, y, \rho)\,\mathrm{d}x\right. \\
&\quad \left. + 2\int_{c_x}^{\infty} g(x, y, \rho)\,\mathrm{d}x\right) + \int_{-\infty}^{-c_y} \mathrm{d}y\left(\int_{-c_x}^{0} g(x, y, \rho)\,\mathrm{d}x\right. \\
&\quad \left. + 2\int_{0}^{c_x} g(x, y, \rho)\,\mathrm{d}x + \int_{c_x}^{\infty} g(x, y, \rho)\,\mathrm{d}x\right) \qquad (7)
\end{aligned}
$$

对任意相关系数 ρ，根据正态分布的“3σ”原则令量化阈值 c 取值范围为[0,3]，再代入式(7)，通过 Mathematica 软件进行数值积分，得到如图 2 所示的一簇不同相关系数下的量化阈值与失配率之间的关系曲线。从图 2 中可以看出，随着量化阈值 c 的增加，密钥失配率增加。当 c 是某个值时，密钥失配率最大，然后随之减小。

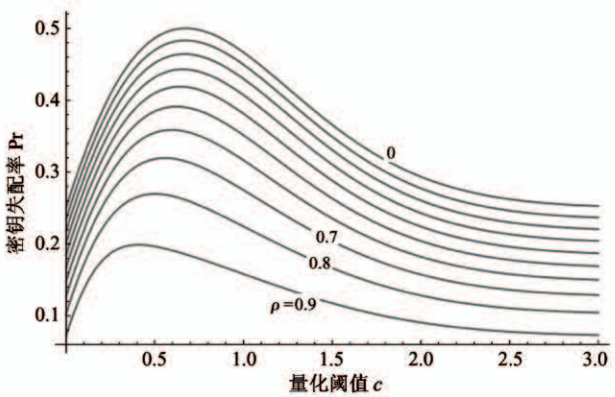

图 2　4 电平量化阈值系数与密钥失配率关系图

下面通过推导使得失配率最高的量化阈值 c，来说明均匀量化是一种失配率最高的量化方案。对于式(7)，密钥失配率对变量 c_x、c_y 分别求偏导，并令其为 0。经过整理后，得到：

$$
\begin{aligned}
&\frac{\partial \Pr(Q_{R_A} \neq Q_{R_B})}{\partial c_x} = 0 \\
&\Rightarrow \mathrm{Erfc}\left(\frac{c_x + c_y\rho}{\sqrt{2(1-\rho^2)}}\right) + \mathrm{Erfc}\left(\frac{c_y - c_x\rho}{\sqrt{2(1-\rho^2)}}\right) \\
&\quad - \mathrm{Erf}\left(\frac{c_x + c_y\rho}{\sqrt{2(1-\rho^2)}}\right) - \mathrm{Erf}\left(\frac{c_y - c_x\rho}{\sqrt{2(1-\rho^2)}}\right) = 0
\end{aligned} \qquad (8)
$$

和

$$
\begin{aligned}
&\frac{\partial \Pr(Q_{R_A} \neq Q_{R_B})}{\partial c_y} = 0 \\
&\Rightarrow \mathrm{Erfc}\left(\frac{c_x + c_y\rho}{\sqrt{2(1-\rho^2)}}\right) + \mathrm{Erfc}\left(\frac{c_x - c_y\rho}{\sqrt{2(1-\rho^2)}}\right) \\
&\quad - \mathrm{Erf}\left(\frac{c_x + c_y\rho}{\sqrt{2(1-\rho^2)}}\right) - \mathrm{Erf}\left(\frac{c_x - c_y\rho}{\sqrt{2(1-\rho^2)}}\right) = 0
\end{aligned} \qquad (9)
$$

根据对称性，如果式(8)和式(9)同时成立，则 $c_x = c_y = c$，因此得到

$$
\mathrm{Erfc}\left(\frac{c(1+\rho)}{\sqrt{2(1-\rho^2)}}\right) + \mathrm{Erfc}\left(\frac{c(1-\rho)}{\sqrt{2(1-\rho^2)}}\right) = 1 \qquad (10)
$$

对式(10)进行数值计算并进行拟合，其拟合方程为

$$
c = -2.3\rho^4 + 3.4\rho^3 - 1.9\rho^2 + 0.3\rho + 0.66 \qquad (11)
$$

结合图 2，式(11)表示不同相关系数下，最高失配率时的量化阈值 c。特别是当相关系数相对小时，失配率最高时的量化阈值基本在[0.6, 0.7]区域内，而均匀量化方案时的量化阈值 $\sqrt{2}\mathrm{Erfc}^{-1}(1/2) \backsimeq 0.67$ 落在此区间内，所以均匀量化是一种密钥失配率最高的量化方案。

进一步，当 c 趋于无穷大时，4 电平量化失配率退化为 2 电平量化。由于格雷编码用于相邻的量化间隔，因此在 4 电平量化相邻间隔中一个比特总是相同的。失配率是 2 电平量化的一半，密钥失配率 $\Pr(Q_{RA} \neq Q_{RB})$ 为

$$
\Pr(Q_{RA} \neq Q_{RB}) = \frac{\arccos(\rho)}{2\pi}, \quad c \to \infty \qquad (12)
$$

这就是图 2 中各条曲线的极限值。

2.2　非均匀量化方法

从 2.1 节中的分析可以得出，均匀量化方法的密钥失配率是密钥失配率最高的情况。受到通信原理中 13 折线非均匀量化的启发，当 RSS 幅度较小时，容易受到信道噪声、收发双方元器件的不一致性等影响，量化后的比特是不可靠的，量化区间应当大一些；与此相反，当 RSS 幅度较大时，抗干扰能力强，量化后比特的匹配率比较高，量化区间可以小一些。基于此，为了提高密钥的匹配率和生成速率，提

出了一种非均匀量化方案。Alice 和 Bob 对接收到的 RSS 进行标准化处理之后,量化区间划分如图 3 所示,其中 $c_1 = \sqrt{2}\,\mathrm{Erfc}^{-1}(1/2) \backsimeq 0.67$, $c_2 = \sqrt{2}\,\mathrm{Erfc}^{-1}(1/4) \backsimeq 1.15$。

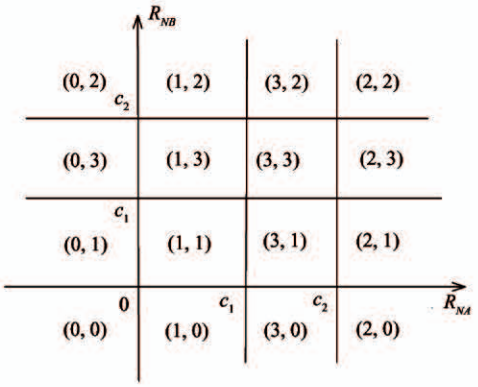

图 3　提出的非均匀量化示意图

本文所用的非均匀量化算法过程如算法 1 所示。

算法 1　非均匀量化算法

1. $F_X(x) = \Pr(X < x)$(一个实随机变量 x 的累积分布函数的定义)
2. $n_i = F_X^{-1}(1 - 1/2^i)$, $i = 1,2,\cdots, L-1$(L 为量化电平数)
3. $n_0 = -\infty$, $n_L = +\infty$
4. 在不同的量化区间 $[n_{i-1}, n_i]$ 构造对应的格雷编码

根据图 3,密钥失配率为

$$
\begin{aligned}
&2\Pr(Q_{RA} \neq Q_{RB}) \\
&= \int_{c_2}^{+\infty} \mathrm{d}y\Big(\int_{-\infty}^{0} g(x, y, \rho)\,\mathrm{d}x + 2\int_{0}^{c_1} g(x, y, \rho)\,\mathrm{d}x \\
&\quad + \int_{c_1}^{c_2} g(x, y, \rho)\,\mathrm{d}x\Big) + \int_{c_1}^{c_2} \mathrm{d}y\Big(2\int_{-\infty}^{0} g(x, y, \rho)\,\mathrm{d}x \\
&\quad + \int_{0}^{c_1} g(x, y, \rho)\,\mathrm{d}x + \int_{c_2}^{+\infty} g(x, y, \rho)\,\mathrm{d}x\Big) \\
&\quad + \int_{0}^{c_1} \mathrm{d}y\Big(\int_{-\infty}^{0} g(x, y, \rho)\,\mathrm{d}x + \int_{c_1}^{c_2} g(x, y, \rho)\,\mathrm{d}x \\
&\quad + 2\int_{c_2}^{+\infty} g(x, y, \rho)\,\mathrm{d}x\Big) + \int_{-\infty}^{0} \mathrm{d}y\Big(\int_{0}^{c_1} g(x, y, \rho)\,\mathrm{d}x \\
&\quad + 2\int_{c_1}^{c_2} g(x, y, \rho)\,\mathrm{d}x + \int_{c_2}^{+\infty} g(x, y, \rho)\,\mathrm{d}x\Big)
\end{aligned}
\tag{13}
$$

通过 Mathematica 计算了 4 电平量化密钥失配率的数值积分结果,如图 4 所示。从图 4 中可以看出,在相同相关系数的情况下,所提出的非均匀量化方法的密钥失配率低于均匀量化方法。

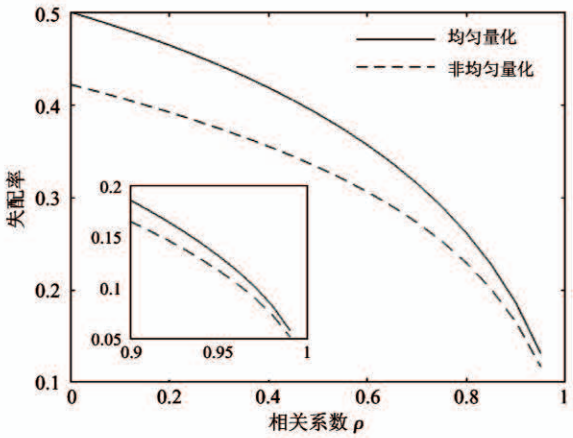

图 4　不同量化方法与相关系数 ρ 之间的关系

综上所述,本文提出的非均匀量化的方法计算密钥失配率的实现过程如下。

(1)首先建立一个通信双方的高斯通信模型。

(2)然后确定需要量化的电平数。

(3)画出非均匀量化的量化示意图。

(4)根据联合概率密度函数,计算出密钥失配的量化区间比特失配率的积分和。

(5)将比特失配率的积分和进行数值计算。

3　仿真结果与分析

通过 Intel 5300 网卡测量真实通信环境中收发节点链路之间的 RSS 数据,验证假设模型是合理的。进一步,将所提出的非均匀的量化方法与均匀量化方法在 Matlab 中进行仿真验证。

3.1　实际环境中通信情况

本文用 802.11 无线网卡测量 RSS。通过在 Linux Ubuntu (10.04-14.04 版本)系统上运行 csi-tools 工具[18]。利用它可以获取 Intel 5300 网卡测量真实通信环境中收发节点链路之间的 RSS 数据,来验证假设模型的合理性。

在测试数据收集过程中用到了 2 台台式电脑,分别命名为 Alice 和 Bob,测试环境如图 5 所示。用 ping 指令控制 Alice 向 Bob 发送 ICMP 报文,设定每 0.2 s发送一个 ICMP 报文; Bob 每收到一条 ICMP

报文都会记录数据，并且返回一个 ACK 给 Alice；Alice 收到 ACK 信号后，也会记录数据。在实验中，ICMP 报文传输的往返延时在 0 ~ 20 ms 之间，收集到的某个子载波 RSS 数据如图 6 所示。从图 6 可以看出，报文传输的往返延时小于信道的相干时间时，信道 RSS 是满足互易性的。图 7 为收集到的部分测量数据（图中符号“ + ”表示），用 Matlab 的 normplot( ) 函数来检验数据的正态性。从图中可看出，数据基本服从正态分布，因此第 3 节中的 RSS 假设模型是合理的。

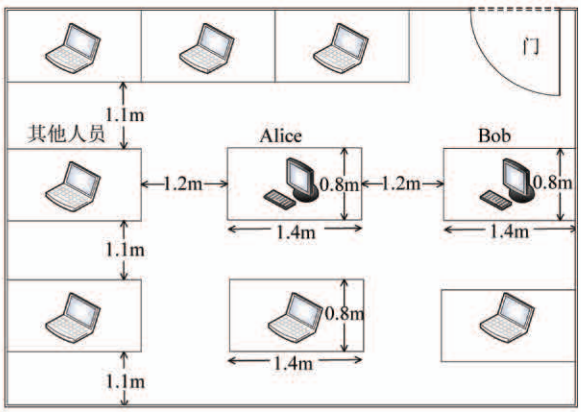

图 5　实测示意图

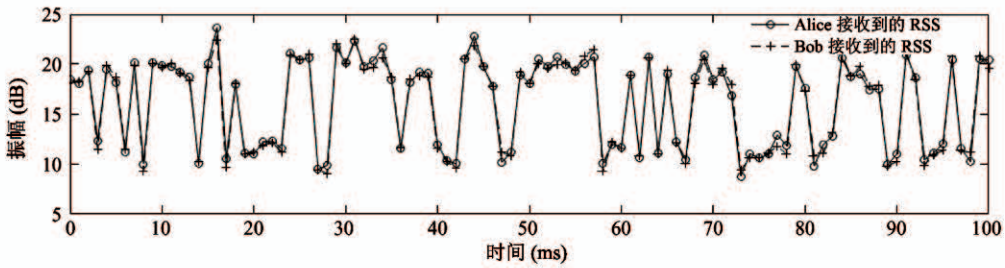

图 6　发射机和接收机的 RSS 随时间变化的测量结果比较图

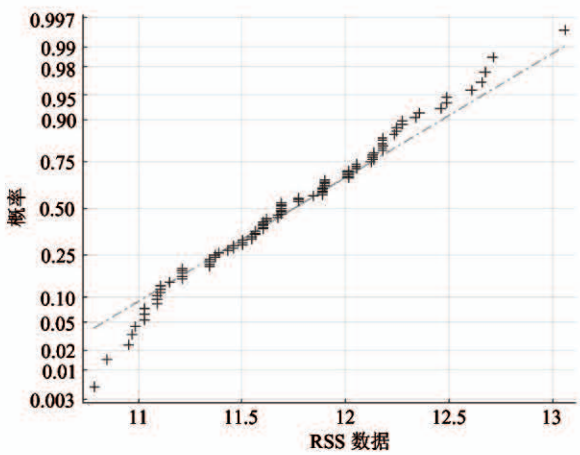

图 7　测量数据的正态性检验图

由于真实环境中不可预测的因素，Alice 和 Bob 两者之间的互易性并不总是很好。这也说明了需要考虑发送和接收双方之间相关系数的必要性。从测量数据中随机选择几组数据，计算相关系数，采用均匀量化和所提出的非均匀量化方案，得到如表 1 所示的密钥失配率。

表 1　4 电平量化的实测失配率

相关系数	4 电平均匀量化	4 电平非均匀量化
0.8292	0.2426	0.2030
0.9141	0.1623	0.1347

3.2　仿真数据结果

本文以 4 电平量化为例，选取不同的相关系数，对均匀量化和非均匀量化利用 Matlab 仿真得到相应的失配率，结果如表 2 所示。结合图 4 和表 2，可以看出表 2 中的仿真结果与图 4 所示的数值积分数据是一致的。

表 2　4 电平量化仿真失配率

相关系数	4 电平均匀量化	4 电平非均匀量化
0.70	0.3149	0.2726
0.75	0.2899	0.2525
0.80	0.2611	0.2290
0.85	0.2271	0.2004
0.90	0.1856	0.1649
0.95	0.1309	0.1167
0.98	0.0826	0.0737

相同条件下,本文也对比了文献[19]中提到的利用 RSS 的均值和方差来确定量化区间的量化方法。该量化方法是将信道信息分为 4 个量化区间 $\left[-\infty, \mu-\frac{1}{2}\sigma\right]$、$\left[\mu-\frac{1}{2}\sigma, \mu\right]$、$\left[\mu, \mu+\frac{1}{2}\sigma\right]$、$\left[\mu+\frac{1}{2}\sigma, +\infty\right]$,区间对应的格雷编码分别是 00、01、11、10。本文同时对该算法进行了数值积分的计算以及仿真实验。数值计算结果与仿真结果是一致的,仿真结果如表 3 所示。从表 3 中可以看出,本文所提出的非均匀量化方法与均匀量化方法和文献[19]的量化方法相比,具有较低密钥失配率的优点。

表 3　不同量化方法仿真失配率比较

相关系数	文献[19]方法	本文方法
0.70	0.3183	0.2726
0.75	0.2959	0.2525
0.80	0.2629	0.2290
0.85	0.2376	0.2004
0.90	0.1966	0.1649
0.95	0.1397	0.1167
0.98	0.0880	0.0737

使用格雷编码可以很好地降低密钥不匹配率。“0”,“1”等概率是确保实际应用中随机性的重要特征。所提出的非均匀量化方法不能保证“0”,“1”的等概率。在密钥生成的下一个信息调和步骤中,可以使用散列函数[20, 21]来解决此问题。

4　结　论

本文针对无线物理层无线通信密钥提取过程中由于加性噪声、无线信道的半双工性质及器件的差异性导致实际信道的非互易性,密钥生成过程中存在密钥失配率的问题,在指定的无线信号强度高斯分布模型下,通过对以往量化方法的分析,提出一种非均匀的密钥比特量化方法。该量化方法考虑到 RSS 幅度较小时,容易受到信道的不一致性等影响,量化后的比特是不可靠的,量化区间应当大一些;与此相反,当 RSS 幅度较大时,抗干扰能力强,量化后比特的匹配率较高,量化区间小一些,从而降低密钥失配率。该量化方法首先将合法通信双方即 Alice 和 Bob 的 RSS 建模为具有相关系数的 2 维高斯分布模型。然后,使用 RSS 的累积分布函数来获得量化的分隔阈值。最后,量化阈值被映射到随机变量上,并且通过使用格雷编码获得一系列密钥比特。通过数值计算结果的拟合分析,得出均匀量化的密钥失配率是最高的情况之一。仿真以及实验数据结果都验证了所提出的非均匀量化的方法降低了密钥失配率。但是在 RSS 指定分布模型下的分析在实际中有一定的局限性,验证其他场景下的密钥失配率情况将是下一步重点研究方向。

参考文献

[1] Hodjat A, Verbauwhede I. Area-throughput trade-offs for fully pipelined 30 to 70 Gbits/s AES processors [J]. *IEEE Transactions on Computers*, 2006, 55(4):366-372

[2] Stinson R D 著, 冯登国译. 密码学原理与实践[M]. 广州:电子工业出版社, 2009: 303-326

[3] Tope M A, Mceachen J C. Unconditionally secure communications over fading channels[C]//Proceedings of the 2001 Communications for Network Centric Operations: Creating the Information Force, McLean, USA, 2001: 54-58

[4] Azimi-Sadjadi B, Kiayias A, Mercado A, et al. Robust key generation from signal envelopes in wireless networks [C]//Proceedings of the 2007 ACM Conference on Computer and Communications Security, Virginia, USA, 2007: 401-410

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

[6] Zhang L, Cai Y, Champagne B, et al. Non-linear transceiver design for secure communications with artificial noiseassisted MIMO relay [J]. *IET Communications*, 2017, 11(6):930-935

[7] Wu J, Chen J. Multiuser transmit security beamforming in wireless multiple access channels[C]//Proceedings of the 2012 IEEE International Conference on Communications, Ottawa, Canada, 2012: 903-906

[8] Wang H M, Yin Q, Xia X G. Distributed beamforming for physical-layer security of two-way relay networks[J]. *IEEE Transactions on Signal Processing*, 2012, 60(7): 3532-3545

[9] Lv L, Chen J, Yang L, et al. Improving physical layer security in untrusted relay networks: cooperative jamming and power allocation[J]. *IET Communications*, 2017, 11

(3):393-399

[10] Zou Y, Wang X, Shen W. Optimal relay selection for physical-layer security in cooperative wireless networks [J]. *IEEE Journal on Selected Areas in Communications*, 2013,31(10): 2099-2111

[11] 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*, 2009,9(1):17-30

[12] Sayeed A, Perrig A. Secure wireless communications: secret keys through multipath[C]//Proceedings of the 2008 International Conference on Acoustics, Speech and Signal Processing, Las Vegas, USA, 2008: 3013-3016

[13] Ye C, Reznik A, Sternberg G, et al. On the secrecy capabilities of ITU channels[C]//Proceedings of the 6th IEEE Vehicular Technology Conference, Baltimore, USA,2007: 2030-2034

[14] 秦艳琳, 吴晓平. 对两种密钥协商协议的分析与改进[J]. 小型微型计算机系统,2017,38(5):1007-1012

[15] 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

[16] Ambekar A, Hassan M, Schotten H D. Improving channel reciprocity for effective key management systems[C]//Proceedings of the 2012 International Symposium on Signals, Systems, and Electronics, Potsdam, Germany, 2012: 1-4

[17] Liu H, Wang Y, Yang J, et al. Fast and practical secret key extraction by exploiting channel response[C]//Proceedings of the 2013 IEEE International Conference on Computer Communications, Turin, Italy, 2013: 3048-3056

[18] Halperin D, Hu W, Sheth A, et al. 802.11 with multiple antennas for dummies[J]. *ACM SIGCOMM Computer Communication Review*,2010,40(1):19-25

[19] Ambekar A, Hassan M, Schotten H D. Improving channel reciprocity for effective key management systems[C]//Proceedings of the 2012 International Symposium on IEEE Signals, Systems, and Electronics, Potsdam, Germany, 2012: 1-4

[20] Zhang J, Kasera S K, Patwari N. Mobility assisted secret key generation using wireless link signatures[C]//Proceedings of the 2010 IEEE International Conference on Computer Communications, San Diego, USA, 2010: 1-5

[21] 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

A non-uniform quantization scheme for wireless signal strength in physical layer security

Xu Zhijiang[*,****], Wang Xiaomin[*], Lu Weidang[*], Chen Fangni[**], Hua Jingyu[***], Gong Yi[****]

([*] College of Information Engineering, Zhejiang University of Technology, Hangzhou 310023)

([**] School of Information and Electronic Engineering, Zhejiang University of Science and Technology, Hangzhou 310023)

([***] School of Information and Electronic Engineering, Zhejiang Gongshang University, Hangzhou 310018)

([****] University Key Laboratory of Advanced Wireless Communications of Guangdong Province Department of Electrical and Electronic Engineering, Southern University of Science and Technology, Shenzhen 518055)

Abstract

The reciprocity and randomness of wireless channel are employed to generate the security key of physical layer to protect the security of transmission data. Under the given Gaussian distribution model of wireless signal strength, the uniform quantized key mismatch rate of uniform quantization scheme is derived theoretically by numerical calculation in the paper. Moreover, it is pointed out that the uniform quantization is a quantization scheme with the highest mismatch rate. To alleviate this problem, a non-uniform quantization scheme is proposed to quantize the strength of the channel measurement into multiple bit values and its corresponding mismatch rate is also given. The experimental and simulation results show that the proposed non-uniform quantization scheme is superior to the counterpart of the uniform quantization.

Key words: physical layer secure, Gaussian distribution, received signal strength (RSS), non-uniform quantization, key mismatch rate