基于无线信道参数的物理层安全密钥容量

王 旭 金 梁* 宋华伟 黄开枝
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：利用无线信道参数提取物理层安全密钥时，密钥容量受加性噪声、信道测量时差、终端移动速度、采样周期和采样点数等因素影响。针对这一问题，该文在均匀散射环境中利用单输入单输出无线信道定量分析密钥容量，推导了密钥容量的闭式解以确定最佳采样周期的约束条件。仿真分析表明该结论同样适用于非均匀散射环境，同时验证将物理层密钥提取技术应用于无线通信系统的可行性。

关键词：物理层安全；物理层密钥提取；密钥容量；无线信道参数；最佳采样周期
中图分类号： TN918.91 **文献标识码**：A **文章编号**：1009-5896(2016)10-2612-07
DOI: 10.11999/JEIT160032

Physical Layer Secret Key Capacity Based on Wireless Channel Parameters

WANG Xu JIN Liang SONG Huawei HUANG Kaizhi
(*National Digital Switching System Engineering & Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: Physical layer secret key capacity is affected by such factors as additive noise, the time difference of channel sampling, terminal's moving speed, sampling period, and the number of samples, whose effects on the physical layer secret key capacity are analyzed quantitatively using the single-input single-output wireless channel over the uniform scattering environment. Specifically, a closed-form solution to the secret key capacity is derived to determine the constraints on the optimal sampling period. Analysis and simulation results reveal that the results can also be applied to the nonuniform scattering environment. Furthermore, the feasibility to utilize the physical layer secret key extraction techniques in the mobile communication systems is verified.

Key words: Physical layer security; Physical layer secret key extraction; Secret key capacity; Wireless channel parameters; Optimal sampling period

1 引言

随着移动通信应用领域的拓展，安全问题逐渐成为制约其发展的主要瓶颈之一。现有移动通信安全依靠高层密钥加密机制，但是在资源受限的新兴网络(如物联网、传感器网络等)中高层密钥的分发和管理存在一定的安全隐患。而无线信道具有天然的密钥特征，通信双方通过测量同一无线信道提取相同的物理层密钥，实现密钥分发，并辅助高层加密机制实现安全增强。现有物理层密钥研究[1,2]主要分为密钥提取技术[3–8]和密钥容量分析[9–11]。其中，密钥容量分析为密钥提取技术提供理论指导，具有重要理论研究价值。

文献[9]和文献[10,11]首先提出利用无线信道作为共同随机源提取密钥，并引入信息论分析密钥容量。物理层密钥提取的前提是无线信道的互易性，当通信双方同时测量同一无噪信道时，能够得到完全相同的信道参数，此时密钥容量无限大。但是实际系统中加性噪声、信道测量时差、终端移动等因素破坏了无线信道的互易性[4,12–15]。文献[16]综合考虑了终端移动和噪声两个因素对密钥容量的影响，并给出了密钥容量的频域表达式。上述文献均只考虑利用单信道样值提取密钥时的密钥容量，但此时即使提取的密钥数达到密钥容量，其密钥数也难以满足需求。因此，需要研究多信道样值时的密钥容量问题，由此引入采样周期和采样点数。文献[17]在均匀散射环境[18]中分析了信道参数的空间和时间相关性对密钥容量的影响，同时指出存在最佳采样周期使得密钥容量最大。但没有给出综合信道测量时差、终端移动速度、加性噪声、采样周期、采样点数等因素的密钥容量的闭式解，也没有给出最佳

收稿日期：2016-01-11；改回日期：2016-06-06；网络出版：2016-08-26
*通信作者：金梁 liangjin@263.net
基金项目：国家 863 计划项目(2015AA01A708)，国家自然科学基金(61171108, 61471396)
Foundation Items: The National 863 Program of China (2015AA01A708), The National Natural Science Foundation of China (61171108, 61471396)

采样周期应该满足的约束条件。

针对上述问题，本文定量分析了上述 5 个因素对密钥容量的影响，确定最佳采样周期的约束条件以最大化物理层安全密钥数。首先在均匀散射环境中，分析没有直达径(NLOS)的单输入单输出(SISO)无线信道的统计特性，并给出信道采样方案；随后，提出一种利用任意维随机变量进行密钥提取时，密钥容量分析方案，推导更加普适的密钥容量闭式解；最后分别在均匀散射环境和非均匀散射环境中验证推导结果的正确性和适用性。推导与仿真结果表明通过合理控制上述因素可提升密钥数，能够指导物理层密钥提取方案中的参数设计。

2　系统模型

考虑一个散射丰富且没有直达径的移动通信场景，基站 Alice 位置固定，移动终端 Bob 以 v 沿着某一方向做直线运动，其中 Alice 和 Bob 均配置单天线，且 Bob 周围存在大量散射体。同时，假设系统中存在单天线被动窃听者 Eve，即 Eve 可以被动接收信号但是不能够发送信号干扰信息传输。由于人工或者自然散射体的散射、反射、折射、衍射等效应，导致工作在超高频或者更高频段的电磁波经历快衰落。均匀散射环境[18,19]能够较为准确建模这一典型移动通信场景的幅度、相位、空间相关性、频域相关性等特性。如图 1 所示[20]，在该模型中散射体密集分布在 Bob 四周，以保证入射功率(Incoming Power[19])来自各个方向，且该模型假设经各个散射体到达终端的电磁波幅度相同。设终端周围有 N 个散射体，则第 $n(n<N)$ 个散射体到达终端的角度为 $n\Delta\theta$，其中 $\Delta\theta=2\pi/N$。

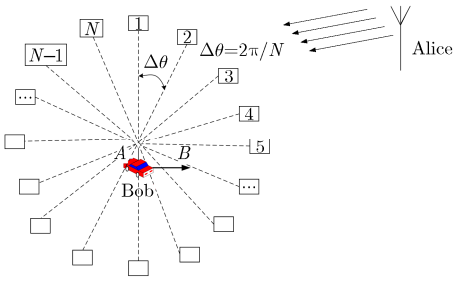

图 1　密集散射环境[20]

根据文献[20]附录 A，在 t 时刻，Alice 和 Bob 之间的窄带无线信道 $h(t)$ 可用其等效复基带表示。

$$h(t)=\sum_{n=1}^{N(t)}\alpha_n(t)\mathrm{e}^{-\mathrm{j}\phi_n(t)}=\sum_{n=1}^{N(t)}\alpha_n(t)\cos\left(\phi_n(t)\right)+\mathrm{j}\sum_{n=1}^{N(t)}\alpha_n(t)\sin\left(\phi_n(t)\right)=h_{\mathrm{I}}(t)+\mathrm{j}h_{\mathrm{Q}}(t)\quad(1)$$

其中，$h_{\mathrm{I}}(t)$，$h_{\mathrm{Q}}(t)$ 表示信道参数的同相/正交(I/Q)分量；$N(t)$ 表示 t 时刻散射体数量；$\alpha_n(t)$ 为信道衰减；$\phi_{\mathrm{D},n}(t)=\int_t 2\pi f_{\mathrm{D},n}(\tau)\mathrm{d}\tau$ 为多普勒频移产生的相偏，$f_{\mathrm{D},n}(\tau)=v/\lambda\cos(n\Delta\theta)$ 表示多普勒频移。在均匀散射环境中，$\alpha_n(t)$ 与 $\phi_n(t)$ 相互独立，由中心极限定理可得，当 $N(t)$ 足够大时，$h(t)$ 服从零均值方差为 $\sigma_h^2(t)$ 的复高斯随机分布，即 $h(t)\sim\mathrm{CN}(0,\sigma_h^2(t))$。由无线信道的互易性可知，信道参数可以作为共同随机源为信道两端的通信双方提供密钥。定义 t 时刻信道功率与噪声功率的比值为信噪比 $\mathrm{SNR}(t)=\sigma_h^2(t)/\sigma_z^2(t)$，由于加性噪声 $z(t)=z_{\mathrm{I}}(t)+\mathrm{j}z_{\mathrm{Q}}(t)\sim\mathrm{CN}\left(0,\sigma_z^2(t)\right)$ 的存在，t 时刻测量的信道参数为

$$\hat{h}(t)=\left(h_{\mathrm{I}}(t)+z_{\mathrm{I}}(t)\right)+\mathrm{j}\left(h_{\mathrm{Q}}(t)+z_{\mathrm{Q}}(t)\right)=\hat{h}_{\mathrm{I}}(t)+\mathrm{j}\hat{h}_{\mathrm{Q}}(t)\quad(2)$$

且 $\hat{h}(t)\sim\mathrm{CN}\left(0,\sigma_h^2(t)+\sigma_z^2(t)\right)$。

为提升密钥数，双方可利用多次信道采样增加双方共享的随机性，此处采用固定采样周期增加采样点数的采样方案。如图 2 所示，假设 Alice 与 Bob 的信道测量时差为 τ，从 0 时刻开始，Alice 和 Bob 以 T 为采样周期进行 K 次信道采样，一般情况下 $\tau\ll T$。

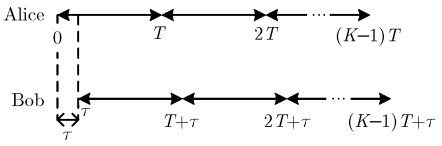

图 2　Alice 和 Bob 采样示意图

记 $\{\hat{h}_{\mathrm{u}}(kT)\}$ 和 $\{\hat{h}_{\mathrm{d}}(kT+\tau)\}$ 分别为 Alice 和 Bob 在 kT 和 $kT+\tau$，$k=0,1,\cdots,K-1$ 时刻测量的无线信道参数。由互易原理得 $h(kT)=h_{\mathrm{u}}(kT)=h_{\mathrm{d}}(kT)$，$h(kT+\tau)=h_{\mathrm{u}}(kT+\tau)=h_{\mathrm{d}}(kT+\tau)$，则 Alice 和 Bob 测量的信道参数可表示为

$$\left.\begin{aligned}\hat{h}_{\mathrm{u}}(kT)&=h(kT)+z(kT)=\hat{h}_{\mathrm{I}}(kT)+\mathrm{j}\hat{h}_{\mathrm{Q}}(kT)\\\hat{h}_{\mathrm{d}}(kT+\tau)&=h(kT+\tau)+z(kT+\tau)\\&=\hat{h}_{\mathrm{I}}(kT+\tau)+\mathrm{j}\hat{h}_{\mathrm{Q}}(kT+\tau)\end{aligned}\right\}\quad(3)$$

特别地，在均匀散射环境中 $\{\hat{h}_{\mathrm{u}}(kT)\}$ 和 $\{\hat{h}_{\mathrm{d}}(kT+\tau)\}$ 为相关的复高斯随机矢量。

从上述分析可以看出，利用信道参数提取物理层安全密钥时，密钥容量受到信道测量时差、终端移动速度、加性噪声、采样周期、采样点数等 5 个因素影响。为了提高物理层密钥数、衡量密钥提取方法的有效性，需要定量分析上述因素对密钥容量的影响。

3 密钥容量分析

根据文献[17]可得当 Eve 距离 Alice 和 Bob 足够远时(大于几个波长)，可近似认为 Eve 和 Alice(或 Bob)之间信道参数与 Alice 和 Bob 之间的信道参数相互独立，此时 Eve 利用信道相关性窃取的密钥数可以忽略。因此本文假设 Eve 与 Alice 和 Bob 距离均超过几个波长，此时可以利用 Alice 与 Bob 测量信道参数间的互信息，代替存在 Eve 被动窃密时的条件互信息计算密钥容量[9,10]。本节首先扩展了文献[17]提出的密钥容量表达式；随后定量分析各项因素对密钥容量的影响，得到密钥容量的闭式解；并据此确定最佳采样周期满足的约束条件以最大化物理层安全密钥容量。本文中密钥容量指的是以 K 个周期性信道采样值为一个样本整体，能够提取的有效密钥位数的上界。

3.1 密钥容量分析方案

由第 2 节分析可知，均匀散射环境中通信双方测量的信道参数是相关的复高斯随机矢量。本小节提出一种利用高斯随机矢量提取物理层安全密钥时密钥容量的分析方案。由于 I/Q 分量分析思路相同，因此在不失一般性的前提下选用 I 分量对密钥容量进行分析。

为表示方便记 $X_k=\hat{h}_{\mathrm{I}}(kT)$，$Y_k=\hat{h}_{\mathrm{I}}(kT+\tau)$，$k=0,1,\cdots,K-1$，则 Alice 和 Bob 测量的信道参数可分别表示为 $\boldsymbol{X}=\left[X_0\ X_1\cdots X_{K-1}\right]$，$\boldsymbol{Y}=\left[Y_0\ Y_1\cdots Y_{K-1}\right]$。因此利用同相分量提取密钥时的密钥容量可以表示为式(4)。

$$\begin{aligned}C_{\mathrm{I}}&=\mathrm{I}(\boldsymbol{X};\boldsymbol{Y})=\mathrm{I}\left(X_0\ X_1\cdots X_{K-1};Y_0\ Y_1\cdots Y_{K-1}\right)\\&=\mathrm{H}(\boldsymbol{X})+\mathrm{H}(\boldsymbol{Y})-\mathrm{H}(\boldsymbol{X},\boldsymbol{Y})\end{aligned}\tag{4}$$

其中，$\mathrm{I}(\boldsymbol{X};\boldsymbol{Y})$ 表示 $\boldsymbol{X},\boldsymbol{Y}$ 的互信息，$\mathrm{H}(\boldsymbol{X})$ 表示 $\boldsymbol{X}$ 的熵。记 $\boldsymbol{Z}=\left[\boldsymbol{X}\ \boldsymbol{Y}\right]=\left[X_0\ X_1\cdots X_{K-1};Y_0\ \ Y_1\cdots\ \ Y_{K-1}\right]$，因为 $\boldsymbol{X},\boldsymbol{Y}$ 为高斯随机矢量，则 $\boldsymbol{Z}$ 也是高斯随机矢量。由文献[15,21]可知，高斯随机矢量的熵可通过协方差矩阵表示。噪声和信道测量时差使得 $\boldsymbol{X}\neq\boldsymbol{Y}$，又 $\left|\boldsymbol{R}_{\boldsymbol{X}}\right|\cdot\left|\boldsymbol{R}_{\boldsymbol{Y}}\right|\cdot\left|\boldsymbol{R}_{\boldsymbol{Z}}\right|\neq 0$，则由分块矩阵运算法可得 $\left|\boldsymbol{R}_{\boldsymbol{Z}}\right|$。

$$\left|\boldsymbol{R}_{\boldsymbol{Z}}\right|=\begin{vmatrix}\boldsymbol{R}_{\boldsymbol{X}} & \boldsymbol{R}_{\boldsymbol{XY}}\\ \boldsymbol{R}_{\boldsymbol{YX}} & \boldsymbol{R}_{\boldsymbol{Y}}\end{vmatrix}=\left|\boldsymbol{R}_{\boldsymbol{X}}\right|\left|\boldsymbol{R}_{\boldsymbol{Y}}-\boldsymbol{R}_{\boldsymbol{YX}}\boldsymbol{R}_{\boldsymbol{X}}^{-1}\boldsymbol{R}_{\boldsymbol{XY}}\right|\tag{5}$$

因此，利用信道参数 I 分量提取的物理层安全密钥容量 C_{I} 可表示为式(6)。

$$\begin{aligned}C_{\mathrm{I}}&=\mathrm{H}(\boldsymbol{X})+\mathrm{H}(\boldsymbol{Y})-\mathrm{H}(\boldsymbol{Z})\\&=\frac{1}{2}\log_2\frac{\left|\boldsymbol{R}_{\boldsymbol{Y}}\right|}{\left|\boldsymbol{R}_{\boldsymbol{Y}}-\boldsymbol{R}_{\boldsymbol{YX}}\boldsymbol{R}_{\boldsymbol{X}}^{-1}\boldsymbol{R}_{\boldsymbol{XY}}\right|}\end{aligned}\tag{6}$$

同理，利用式(4)～式(6)的分析步骤可得利用 Q 分量提取的物理层安全密钥容量 $C_{\mathrm{Q}}=C_{\mathrm{I}}$。需要说明的是，虽然式(6)由周期性采样所得的信道参数推导出，但是适用于利用两组任意维高斯矩阵提取密钥的场景。例如，对于 $N_1\times N_2\times\cdots\times N_{nn}$ 维的高斯随机矩阵 $\boldsymbol{X},\boldsymbol{Y}$，其密钥容量分析过程只需增加一步矩阵按列矢量化过程，即将 $\boldsymbol{X},\boldsymbol{Y}$ 变成 $N_1N_2\cdots N_{nn}\times 1$ 维的高斯随机矢量，之后重复式(4) ～式(6)即可。

3.2 密钥容量推导

由 3.1 节分析可得，利用信道参数序列提取物理层安全密钥时，密钥容量由 Alice 和 Bob 测量的信道参数的协方差矩阵决定，而协方差矩阵代表序列之间的相关性。因此本小节将定量分析信道参数相关性的影响因素，推导密钥容量的闭式解，进而确定最佳采样周期的约束条件。

假设采样过程中 Bob 移动距离远小于 Alice 经过散射物到达 Bob 的路径长度，且采样过程中障碍物的位置保持不变。则可认为 Alice 发射的信号经过第 n 个散射点到达 Bob 的路径损耗保持不变。又均匀散射环境中假设入射功率相同，所以 $N=N(rT)=N(sT+\tau)$，$\alpha_n=\alpha_n(rT)=\alpha_n(sT+\tau)$，终端移动速度 v 及多普勒频移 $f_{\mathrm{D},n}$ 保持不变，其中 $r,s=0,1,\cdots,K-1$。相位偏移为 $\phi_n(t)=2\pi\left(f_c\tau_n-f_{\mathrm{D},n}t\right)$，其中 f_c 为载波频率，τ_n 为从 Alice 发射且经过第 n 个散射点到达 Bob 的电磁波的传输时延。则当 $r\neq s$ 时，有式(7)成立。

$$\begin{aligned}\boldsymbol{R}_{\boldsymbol{XY}}(r,s)=\sum_{n=1}^{N}E\left(\alpha_n^2\right)E\Big(&\cos\left(2\pi\left(f_c\tau_n-rT\cdot f_{\mathrm{D},n}\right)\right)\\&\cdot\cos\left(2\pi\left(f_c\tau_n-(sT+\tau)\cdot f_{\mathrm{D},n}\right)\right)\Big)\end{aligned}\tag{7}$$

又 $f_c\tau_n\gg(sT+\tau)f_{\mathrm{D},n}$，$f_c\tau_n\gg rTf_{\mathrm{D},n}$，所以 $4\pi f_c\tau_n-2\pi\left(((r+s)T+\tau)\cdot f_{\mathrm{D},n}\right)$ 在 $[0,2\pi]$ 范围内近似服从均匀分布。所以 $E\left(\cos\left(4\pi\left(f_c\tau_n-f_{\mathrm{D},n}t\right)+2\pi f_{\mathrm{D},n}\tau\right)\right)=0$。均匀散射模型中各角度的入射功率相同且 $N=2\pi/\Delta\theta$，则 $E\left(\alpha_n^2\right)=P/N$，其中 P 为无线信道的总功率，此时式(7)可化简为式(8)。

$$\begin{aligned}&\boldsymbol{R}_{\boldsymbol{XY}}(r,s)\\&=\sum_{n=1}^{N}\frac{0.5P}{2\pi}E\left(\cos\left(2\pi v\left((s-r)T+\tau\right)\cos(n\Delta\theta)/\lambda\right)\right)\Delta\theta\end{aligned}\tag{8}$$

因为零阶贝塞尔函数满足式(9)。

$$\begin{aligned}J_0(x)&=\frac{1}{\pi}\int_0^{\pi}\exp(-\mathrm{j}x\cos\theta)\mathrm{d}\theta\\&=\frac{1}{\pi}\int_0^{\pi}\left(\cos(x\cos\theta)\right)\mathrm{d}\theta\end{aligned}\tag{9}$$

所以，当 $N\to\infty$ 时，式(8)可进一步化简为

$$\boldsymbol{R}_{\boldsymbol{XY}}(r,s)=0.5PJ_0\left(2\pi v\left((s-r)T+\tau\right)/\lambda\right) \tag{10}$$

由式(10)可得，信道参数 I 分量的自相关函数只依赖于信道采样时间差，因此信道参数的 I 分量是宽平稳随机过程，因此有 $\sigma_h^2(rT)=\sigma_h^2(sT+\tau)=\sigma_h^2=P$，$r,s=0,1,2,\cdots,K-1$。同理可得式(11)的结论。

$$\left.\begin{aligned}\boldsymbol{R}_{\boldsymbol{X}}(r,s)=\boldsymbol{R}_{\boldsymbol{Y}}(r,s)=0.5PJ_0\left(2\pi v(r-s)T/\lambda\right)\\ \boldsymbol{R}_{\boldsymbol{YX}}(r,s)=0.5PJ_0\left(2\pi v\left((s-r)T-\tau\right)/\lambda\right)\end{aligned}\right\} \tag{11}$$

特别地，当 $r=s$ 时有式(12)成立。

$$\begin{aligned}\boldsymbol{R}_{\boldsymbol{X}}(r,r)&=0.5\left(\sigma_h^2(t)+\sigma_n^2(t)\right)\\&=0.5P\left(1+1/\mathrm{SNR}(t)\right)\end{aligned} \tag{12}$$

因为 $E\left(\hat{h}_{\mathrm{I}}(t)\hat{h}_{\mathrm{Q}}(t+\tau)\right)=0$，且 $\hat{h}_{\mathrm{I}}(t),\hat{h}_{\mathrm{Q}}(t+\tau)$ 均为高斯随机变量，所以 $\hat{h}_{\mathrm{I}}(t),\hat{h}_{\mathrm{Q}}(t+\tau)$ 相互独立。综合 3.1 节和 3.2 节分析可知，密钥容量 C 为

$$C=C_{\mathrm{I}}+C_{\mathrm{Q}}=\log_2\frac{\left|\boldsymbol{R}_{\boldsymbol{Y}}\right|}{\left|\boldsymbol{R}_{\boldsymbol{Y}}-\boldsymbol{R}_{\boldsymbol{YX}}\boldsymbol{R}_{\boldsymbol{X}}^{-1}\boldsymbol{R}_{\boldsymbol{XY}}\right|} \tag{13}$$

式(13)计算的密钥容量是在 τ,SNR,v,K,T 给定条件下，以 K 个采样值作为一个样本整体，进行物理层安全密钥提取时，所能够提取的密钥数上界(单位为 bit/K samples)，此时 τ,SNR,v,K,T 是相互独立的变量。特别地，当 $K=1/T$ 时，或者利用总时间 $K\cdot T$ 对式(13)进行归一化处理之后，由式(13)计算的密钥容量的单位为 bps。为了充分研究各个因素对密钥容量的影响，本文中选用 bit/K samples 为单位。

比较文献[17]式(7)可知，其表达式为本文式(13)在 $h(rT)=h(rT+\tau),r=0,1,2,\cdots,K-1$ 时的特例。实际系统中 τ 由系统决定，SNR 受无线信道环境制约，而 K,T,v 是可控的。给定 v,K,τ,SNR 时，式(13)为 T 的函数，据此可确定出最佳采样周期的约束条件。

4　仿真分析

本节首先在均匀散射环境中验证密钥容量的正确性，并分析信噪比 SNR，采样点数 K，采样周期 T，移动速度 v，信道测量时差 τ 等因素对密钥容量的影响；随后在非均匀散射环境中验证推导结论的适用性(适用性指式(13)不仅适用于均匀散射环境，也适用于非均匀散射环境)。其中，I/Q 分量的密钥容量仿真值通过文献[22–24]给出的互信息估计算法得到。

4.1 正确性验证

如图 3 所示，在文献[25]给出的典型均匀散射仿真环境中，验证推导结果正确性。仿真结果通过 10^5 次蒙特卡洛实验得到，仿真条件如下：

(1)各角度入射功率相同且 Alice 与 Bob 之间没有直达径，每经历一个波长相位变化 2π，载波频率为 2 GHz，且 $\mathrm{SNR}=\mathrm{SNR}(t)=\mathrm{SNR}(t+\tau)$；

(2)Alice 位置固定，Bob 以速度 v 从原点沿着 X 轴正向移动；每次仿真中 1000 个散射点在以原点为圆心、半径为 200 m 的圆周上按照 $[0,2\pi]$ 的均匀分布随机产生；

(3)信道参数为 Alice 与 Bob 之间经过一次散射的电磁波的叠加。

仿真步骤如下：

(1)在以原点为圆心，200 m 为半径的圆周上，按照 $[0,2\pi]$ 的均匀分布随机产生 1000 个散射点；

(2)在 Bob 以速度 v 从原点沿着 X 轴正向移动过程中，Alice 和 Bob 分别在 kT 和 $kT+\tau$，$k=0,1,\cdots,K-1$ 时刻测量无线信道，得到无线信道参数的一组仿真数据；

(3)重复步骤(1)和步骤(2) 10^5 次，得到 10^5 组无线信道参数的仿真数据；

(4)根据文献[24]的式(16)～式(20)，利用仿真数据进行互信息估计。

图 4 为 $K=10$, $v=5$ m/s, $T=15$ ms, SNR = 10 dB 条件下，密钥容量随 $\lg(\tau)$ 的变化图。

图 4 中，$\lg(\cdot)$ 为以 10 为底的对数运算；“I/Q 理论值”指利用式(13)计算的密钥容量的一半；“I(Q)仿真值”指利用仿真数据估计的 I(Q)分量密钥容量的仿真值(图 5～图 8，图 10～图 12 中图例含义与此处相同)。如图 4 所示，当 $\tau<10^{-3}$ s 时，密钥容量近似保持不变；当 $10^{-3}\ \mathrm{s}\le\tau<10^{-1.4}$ s 时，密钥容量呈波浪状递减；当 $10^{-1.4}\ \mathrm{s}\le\tau<10^{-0.8}$ s 时，密钥容量迅速下降；当 $10^{-0.8}\ \mathrm{s}\le\tau$ 之后密钥容量近似为 0。这是由于信道测量时差以及终端移动导致 Alice 和 Bob 测量的无线信道发生变化，破坏了 Alice 和 Bob 采样信道的相关性。随着信道采样时间差的增加，信道参数的相关性在 Alice 和 Bob 采样时刻波浪递减。当 Alice 与 Bob 信道采样时间差 τ 足够长时，双方采样信道相互独立，双方所能提取的密钥容量近似为 0。

图 5 为 $K=10$, $v=15$ m/s, $\tau=15\,\mu$s, SNR = 10 dB 条件下，密钥容量随 $\lg(T)$ 的变化图。图 6 为 $K=10$, $T=5$ ms, $\mathrm{SNR}=10$ dB, $\tau=10\,\mu$s 条件下，密钥容量随 v 的变化图。

如图 5 所示，当 $10^{-2.35}\ \mathrm{s}\le T$ 时随着 T 增加，密钥容量增长缓慢；在 $T=10^{-2.35}$ s (相邻两次信道测量过程中，终端移动距离约为 0.5λ)处取得第 1 个波峰，此时密钥容量 $C_{\mathrm{I}}\approx12.2348$ bit/10 samples，而在仿真条件下，$\lim\limits_{T\to\infty}C_{\mathrm{I}}\approx12.6321$ bit

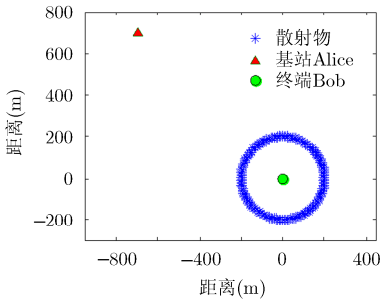

图 3 均匀散射环境仿真示意图[25]

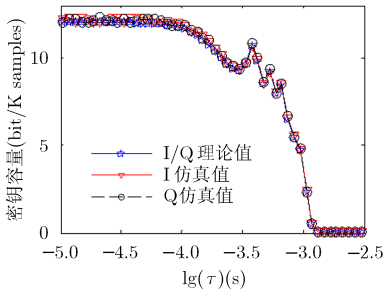

图 4 密钥容量随 $\lg(\tau)$ 变化图

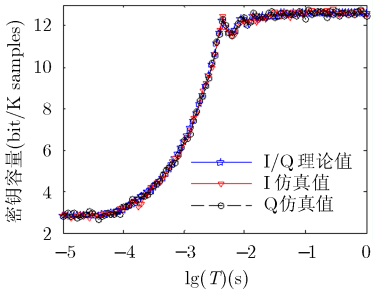

图 5 密钥容量随采样周期变化图

/10 samples ($T\to\infty$ 时，相邻两次信道测量值相互独立)，误差为 3.15% 。这是由于 $vT\geq 0.5\lambda$ 以后，可以认为 K 次采样值之间相互独立，使得信道随机性得到充分利用[20]。考虑到密钥更新效率，在图 5 的仿真环境中最佳采样周期为 $10^{-2.35}$ s。同理，根据任意给定的 τ,SNR, K, v 可以确定出相应的最佳采样周期 T，进而在保证时间效率的条件下最大化物理层安全密钥数量。如图 6 所示，当 $v<12$ m/s 时随着移动速度的增加，密钥容量近似按照线性规律迅速增长； $v\geq 12$ m/s 之后，呈波浪状缓慢增长，最后密钥容量趋于平稳。图 5 和图 6 的本质原因是空间位置的变化改变了 Alice(或 Bob)测量的信道采样值之间的相关性。

图 4~图 6 中的波浪现象是由于贝塞尔函数的特性造成的。由图 4~图 6 可得，由系统误差引起的信道测量时差 τ 与加性噪声和终端移动共同作用，确定了 Alice 和 Bob 第 k 次信道测量值 $h(kT)$ 和 $h(kT+\tau)$ 之间的相关性，进而确定了利用单次信道采样提取密钥的密钥容量。周期性采样的时延 T 能够降低 Alice(或 Bob)第 k 次和第 $k+1$ 次信道测量值 $h(kT)$ 和 $h\big((k+1)T\big)$ 之间的相关性。当 $vT\geq 0.5\lambda$ 以后，可近似认为第 k 次和第 $k+1$ 次信道测量值相互独立，以 K 次信道测量值为一个整体提取的密钥数约为单独利用一次信道测量值进行密钥提取时的 K 倍。因此，本文利用周期性采样增加采样点数(即增加共享随机性)的方法，解决信道测量时差和加性噪声降低信道相关性的问题。

图 7 为 $K=10$, $v=10$ m/s , $T=15$ ms , $\tau=10\,\mu$s 条件下，密钥容量随 SNR 增加的变化图。图 8 为 $v=5$ m/s , $T=15$ ms , $\tau=10\,\mu$s, SNR $=10$ dB 条件下，密钥容量随采样点数 K 的变化图。

如图 7 所示，当 SNR ≤ 60 dB 时，随着 SNR 增加，密钥容量近似线性增长； SNR >60 dB 后，密钥容量近似保持不变。这是由于随着 SNR 增加信道采样值之间的相关性得到提升，当 SNR $>$ 60 dB 可认为不存在加性噪声，此时密钥容量受给定量 τ,K,T,v 的制约而保持不变。实际通信系统中，SNR 通常在 0 ~ 30 dB 之间变化，此时密钥容量随着 SNR 增加近似按照线性增加。因此，为提升密钥容量需要注重噪声消除技术研究。如图 8 所示，密钥容量随着 K 的增加，呈线性增长；直线斜率代表平均每样值所能够提取的密钥数量。由图 8 可得，通过增加采样点数的方法可线性提升物理层安全密钥容量。

由图 4~图 8 可知，利用式(13)计算的密钥容量理论值与密钥容量仿真值一致性较好，从而论证了密钥容量推导结果的正确性。

4.2 适用性验证

如图 9 所示，改变仿真环境使得不再满足均匀散射环境条件，通过与式(13)比较论证推导结果的适用性。仿真结果通过 10^5 次蒙特卡洛实验得到，仿真条件如下：

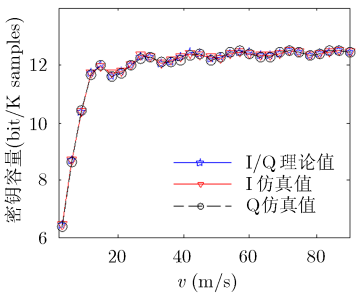

图 6 密钥容量随移动速度变化图

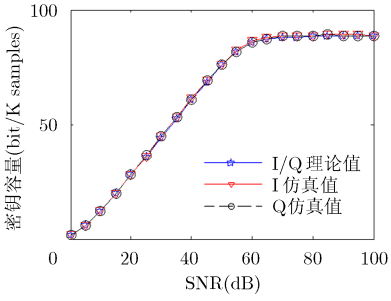

图 7 密钥容量随 SNR 变化图

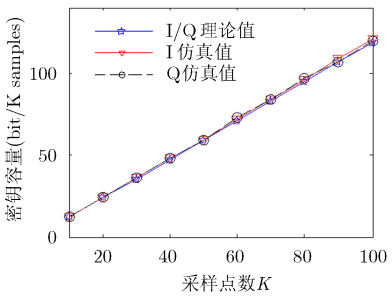

图 8 密钥容量随采样点数变化图

(1)电磁波衰减遵循自由空间路径损耗规律，每经历一个波长相位变化2π，Alice和Bob之间存在一条直达径，载波频率为 2 GHz，且$\mathrm{SNR}=\mathrm{SNR}(t)=\mathrm{SNR}(t+\tau)$；

(2)Alice位置固定，Bob以速度v从原点沿着X轴正向移动；每次仿真中 99 个散射点在$x\in[-900,200], y\in[-200,900]$平面内均匀产生；

(3)信道参数为 Alice 与 Bob 之间经过一次散射的电磁波的叠加。

仿真步骤如下：

(1)在$x\in[-900,200], y\in[-200,900]$平面内均匀产生 99 个散射点；

(2)在 Bob 以速度v从原点沿着X轴正向移动过程中，Alice 和 Bob 分别在kT和$kT+\tau$，$k=0,1,\cdots,K-1$时刻测量无线信道，得到无线信道参数的一组仿真数据；

(3)重复步骤(1)和步骤(2)10^5次，得到10^5组无线信道参数的仿真数据；

(4)根据文献[24]的式(16)~式(20)，利用仿真数据进行互信息估计。

图 10 为$x\in[-900,200]$, $y\in[-200,900]$, $K=10$, $v=15$ m/s, $T=15$ ms, SNR = 10 dB 条件下，密钥容量随$\lg(\tau)$的变化图。分别改变 99 个散射点的分布范围为$x\in[-600,200]$, $y\in[-200,600]$和$x\in[-1100,400]$, $y\in[-400,1100]$其余条件保持不变，重复步骤(1)~步骤(4)，得到图 11 和图 12。

由图 10~图 12 可得，该环境下仿真结果与理论值存在差异，但是变化趋势相同。这是由于密集分布的散射体依然能够保证 Alice 与 Bob 之间的信道参数近似服从高斯分布，从而使得推导结论依然具有适用性。商用 4 G TD-LTE 信道测量时差[26]为 143.8 μs。作为 5 G 移动通信研究热点的同时同频全双工(CCFD)技术，其信道测量时差来自于系统授时时差，而当前授时系统(如：GPS、北斗等)的最大授时时差为 10 μs。由图 10~图 12 可知，其信道测量时差对工作于 TD-LTE 和 CCFD 系统中的通信双方提取密钥的影响不大，从而验证物理层密钥提取技术可应用于 4G 和 5G 通信系统中。

5　总结

该文在均匀散射环境中，推导了利用信道参数提取物理层安全密钥时密钥容量的闭式解。可定量分析加性噪声、信道测量时差、终端移动速度、采样周期和采样点数等因素对密钥容量的影响。首先分析了均匀散射环境中 NLOS SISO 信道的统计特性，并介绍了信道采样方案。随后，给出了利用两个任意维高斯随机矩阵提取物理层安全密钥时，密钥容量的分析方法，并推导了密钥容量的闭式解。最后，仿真验证了推导结果的正确性和适用性。该结论可确定最佳采样周期的约束条件，指导实际采样方案的设计。除此之外，该文利用 TD-LTE 和 CCFD 参数验证了将物理层密钥提取技术应用于移动通信系统的可行性。

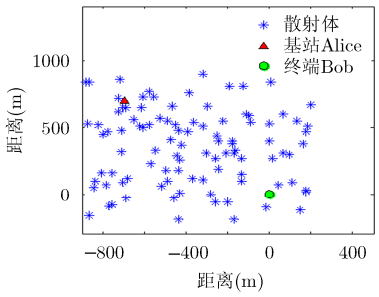

图 9 非均匀散射仿真环境示意图

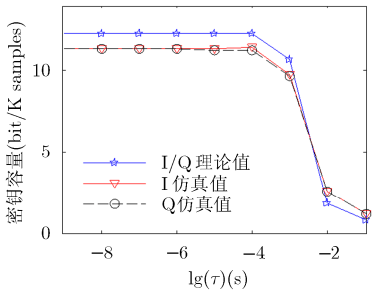

图 10 密钥容量随$\lg(\tau)$增加变化图$x\in[-900,200], y\in[-200,900]$

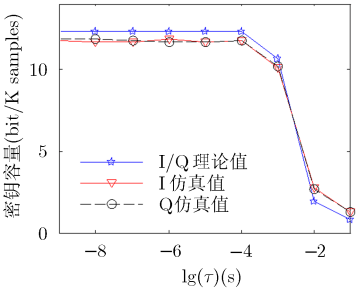

图 11 密钥容量随$\lg(\tau)$增加变化图
$x\in[-600,200], y\in[-200,600]$

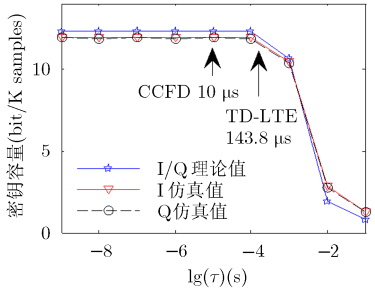

图 12 密钥容量随$\lg(\tau)$增加变化图
$x\in[-1100,400], y\in[-400,1100]$

参 考 文 献

[1] SHEHADEH Y E H and HOGREFE D. A survey on secret key generation mechanisms on the physical layer in wireless networks[J]. *Security and Communication Networks*, 2015, 8(2): 332–341. doi: 10.1002/sec.973.

[2] WANG T, LIU Y, and VASILAKOS A V. Survey on channel reciprocity based key establishment techniques for wireless systems[J]. *Wireless Networks*, 2015, 21(6): 1835–1846. doi: 10.1007/s11276-014-0841-8.

[3] 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. doi: 10.1109/TMC.2012.63.

[4] CHOU T H, DRAPER S C, and SAYEED A M. Key generation using external source excitation: capacity, reliability, and secrecy exponent[J]. *IEEE Transactions on Information Theory*, 2012, 58(4): 2455–2474. doi: 10.1109/TIT.2011.2176311.

[5] LIU Y, DRAPER S C, and SAYEED A M. Exploiting channel diversity in secret key generation from multipath fading randomness[J]. *IEEE Transactions on Information Forensics and Security*, 2012, 7(5): 1484–1497. doi: 10.1109/TIFS.2012.2206385.

[6] WALLACE J W and SHARMA R K. Automatic secret keys from reciprocal MIMO wireless channels: Measurement and analysis[J]. *IEEE Transactions on Information Forensics and Security*, 2010, 5(3): 381–392. doi: 10.1109/TIFS.2010.2052253.

[7] TSOURI G R and WAGNER D M. Threshold constraints on symmetric key extraction from rician fading estimates[J]. *IEEE Transactions on Mobile Computing*, 2013, 12(12): 2496–2506. doi: 10.1109/TMC.2012.226.

[8] 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: 信息科学, 2014, 44(12): 1580–1592. doi: 10.1360/N112013-00041.

DAI Q, SONG H W, JIN L, *et al*. Physical-layer authentication and key distribution mechanism based on equivalent channel[J]. *Scientia Sinica Informationis*, 2014, 44(12): 1580–1592. doi: 10.1360/N112013-00041.

[9] MAURER U M. Secret key agreement by public discussion from common information[J]. *IEEE Transactions on Information Theory*, 1993, 39(3): 733–742. doi: 10.1109/18.256484.

[10] AHLSWEDE R and CSISZ R I. Common randomness in information theory and cryptography. Part I: Secret sharing[J]. *IEEE Transactions on Information Theory*, 1993, 39(4): 1121–1132. doi: 10.1109/18.243431.

[11] AHLSWEDE R and CSISZ R I. Common randomness in information theory and cryptography. Part II: CR capacity[J]. *IEEE Transactions on Information Theory*, 1998, 44(1): 225–240. doi: 10.1109/18.651026.

[12] 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. doi: 10.1109/TMC. 2009.88.

[13] SHEHADEH Y E H, ALFANDI O, and HOGREFE D. On improving the robustness of physical-layer key extraction mechanisms against delay and mobility[C]. Proceedings of International Wireless Communications and Mobile Computing Conference, Limassol, Cyprus, 2012: 1028–1033. doi: 10.1109/IWCMC.2012.6314347.

[14] SHEHADEH Y E H, ALFANDI O, and HOGREFE D. Towards robust key extraction from multipath wireless channels[J]. *Journal of Communications and Networks*, 2012, 14(4): 385–395. doi: 10.1109/JCN.2012.6292245.

[15] NITINAWARAT S and NARAYAN P. Secret key generation for correlated Gaussian sources[J]. *IEEE Transactions on Information Theory*, 2012, 58(6): 3373–3391. doi: 10.1109/TIT.2012.2184075.

[16] WU X F, SONG Y, ZHAO C, *et al*. Secrecy extraction from correlated fading channels: an upper bound[C]. Proceedings of International Conference on Wireless Communications & Signal Processing, Nanjing, China, 2009: 1–3. doi: 10.1109/WCSP.2009.5371757.

[17] CHEN C and JENSEN M. Secret key establishment using temporally and spatially correlated wireless channel coefficients[J]. *IEEE Transactions on Mobile Computing*, 2011, 10(2): 205–215. doi: 10.1109/TMC.2010.114.

[18] CLARKE R. A statistical theory of mobile-radio reception [J]. *Bell System Technical Journal*, 1968, 47(6): 957–1000. doi: 10.1002/j.1538-7305.1968.tb00069.x.

[19] JAKES W C and COX D C. Microwave Mobile Communications[M]. New Jersey: Wiley-IEEE Press, 1994: 13–39.

[20] GOLDSMITH A. Wireless Communications[M]. Cambridge: Cambridge University Press, 2005: 63–76.

[21] COVER T M and THOMAS J A. Elements of Information Theory[M]. New York: John Wiley & Sons, 2012: 247–252.

[22] ZENG X and DURRANI T. Estimation of mutual information using copula density function[J]. *Electronics Letters*, 2011, 47(8): 493–494. doi: 10.1049/el.2011.0778.

[23] MA J and SUN Z. Mutual information is copula entropy[J]. *Tsinghua Science & Technology*, 2011, 16(1): 51–54. doi: 10.1016/S1007-0214(11)70008-6.

[24] 韩敏, 刘晓欣. 基于 Copula 熵的互信息估计方法[J]. 控制理论与应用, 2013, 30(7): 875–879. doi: 10.7641/CTA.2013.21262.

HAN M and LIU X X. Mutual information estimation based on Copula entropy[J]. *Control Theory & Applications*, 2013, 30(7): 875–879. doi: 10.7641/CTA.2013. 21262.

[25] FONT N F P and ESPI EIRA P M. Modelling the Wireless Propagation Channel: a Simulation Approach with Matlab [M]. New York: John Wiley & Sons, 2008: 105–111.

[26] STEFANIA S, ISSAM T, and MATTHEW B. LTE, the UMTS Long Term Evolution: from Theory to Practice[M]. New York: John Wiley & Sons, 2009: 430–453.

王 旭： 男，1990 年生，博士生，研究方向为无线通信网络与信息安全.

金 梁： 男，1969 年生，教授，博士生导师，研究方向为移动通信网络与信息安全.

宋华伟： 男，1978 年生，副研究员，研究方向为移动通信安全.