doi:10.11959/j.issn.1000-436x.2016177

均匀散射环境中物理层安全密钥容量分析

王旭，金梁，刘璐，李明亮，黄开枝
（国家数字交换系统工程技术研究中心，河南 郑州 450002）

摘 要：物理层安全密钥容量受信道测量时差、终端移动和加性噪声等因素影响，在均匀散射环境中定量分析了上述因素对密钥容量的影响。在分析含噪窄带信道参数的时域统计特性的基础之上，推导了密钥容量时域闭式解，并且分别在均匀散射和非均匀散射环境中验证了推导结果的正确性和适用性。
关键词：物理层安全；物理层安全密钥；密钥容量；均匀散射环境
中图分类号：TN918.91 **文献标识码**：A

Analysis of physical layer secret key capacity in the uniform scattering environment

WANG Xu, JIN Liang, LIU Lu, LI Ming-liang, HUANG Kai-zhi
(National Digital Switching System Engineering & Technological Research Center, Zhengzhou 450002, China)

Abstract: Physical layer secret key capacity was affected by time difference of channel sounding, mobility of terminals, and additive noise. Effects on the physical layer secret key capacity were quantitatively analyzed in the uniform scattering environment. Based on the time domain statistical characteristics of narrow band wireless channel parameters with noise, a closed-form solution to physical layer secret key capacity in the time domain was derived. Afterwards, simulations in the uniform and non-uniform scattering environment were carried out to demonstrate its validity and applicability, respectively.
Key words: physical layer security, physical layer secret key, secret key capacity, uniform scattering environment

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安全密钥，可用于密钥分发并辅助高层密钥加密机制实现安全增强。现有物理层安全密钥研究[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上界，具有重要理论研究价值。

Maurer[9]和 Csiszár[10,11]首先提出利用无线信道作为共享随机源提取密钥，并分析了密钥容量问题。物理层安全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。但是大量文献研究表明，信道测量时差、终端移动以及热噪声等因素破坏了信道互易条件，限制了密钥容量。Patwari[12]指出实际系统中信道测量时差破坏了互易条件。为了降低信道测量时差对物理层安全密钥提

收稿日期：2015-11-04；**修回日期**：2016-07-26
通信作者：金梁，liangjin@263.net
基金项目：国家高技术研究发展计划（“863”计划）基金资助项目（No.2015AA01A708）；国家自然科学基金资助项目（No.61171108, No.61471396）；中国博士后科学基金资助项目（No.2016M592990）
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (No.2015AA01A708), The National Natural Science Foundation of China (No.61171108, No.61471396); China Postdoctoral Science Foundation (No.2016M592990)

取的影响，Shehadeh [13]利用一段时间内多次信道采样的平均值增加信道信息的一致性。与此同时，Shehadeh[13,14]指出终端移动带来的信道快变丰富了信道参数的随机性。除此之外，Nitinawarat[15]和Chou[4]等指出加性噪声对互易条件的破坏作用也不容忽视，并定量分析了加性噪声对密钥容量的影响。上述文献只考虑某一因素对密钥容量的影响，而 Wu[16]在均匀散射环境[17]中，综合考虑终端移动和加性噪声 2 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。但是现有文献均只从部分因素入手分析密钥容量，未综合考虑信道测量时差、终端移动和加性噪声对密钥容量的影响。

针对上述问题，本文基于 Csiszár[10]提出的 Model S (source-type model)，在均匀散射环境中定量分析了上述 3 个因素对密钥容量的影响。首先介绍均匀散射环境，分析了含噪窄带信道参数的时域统计特性；随后将密钥容量计算转化为随机变量的互信息计算问题，推导出密钥容量时域闭式解；在均匀散射环境中验证推导结果的正确性，并且仿真验证该结论在非均匀散射环境中同样适用。仿真结果表明，在具有大量散射体的环境中利用无线信道参数提取物理层安全密钥是可行的。该结论能够分析在密集散射场景中提取物理层安全密钥时的密钥容量。

2 系统模型

考虑一个具有丰富散射体的 NLOS（无直达径）移动通信场景，单天线的基站 Alice 和移动终端 Bob 之间存在大量散射物。Bob 从 A 点出发，按照移动速度 v 向 B 点方向移动。设 Alice 到 Bob 之间的无线信道为下行信道，Bob 到 Alice 的信道为上行信道；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。由于建筑物或者其他人为或者自然散射体的存在，导致通信双方之间的电磁波（工作在超高频或者更高频段）产生大量的散射、反射、折射和衍射。均匀散射模型[17, 18]能够建模这一典型移动通信场景的无线信道参数，包括幅度、相位、空间相关性、频域相关性等特性。如图 1 所示，在该模型中散射体均匀分布在以终端为圆心的圆周上，以保证入射功率[18]（incoming power）来自各个方向。该模型假设终端周围有 N 个散射体，第 $n(n\leqslant N)$个散射体到达终端的角度为 $n\Delta\theta$，其中，相邻 2 个入射径的夹角为 $\Delta\theta=\dfrac{2\pi}{N}$，且假设从各个散射体到达终端的电磁波衰减相同。

根据文献[19]，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

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

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；$\phi_n(t)$ 表示信道相位偏移。在均匀散射环境条件下 $\alpha_n(t)$ 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 $\sigma_h^2(t)$ 的高斯随机分布，即 $h(t)\sim\mathrm{CN}(0,\sigma_h^2(t))$。

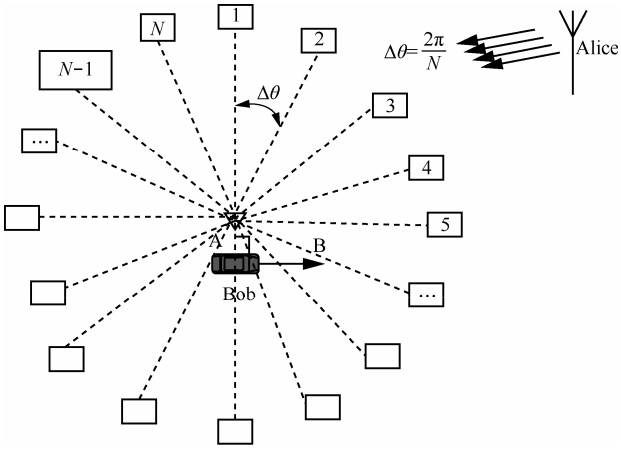


图 1 均匀散射环境

3 密钥容量分析

本文基于 Model S[10]进行研究，将无线信道作为共享随机源，Alice 和 Bob 通过测量获取具有一定相关性的信道信息。同时，Chen[20]指出当 Eve 到 Alice 和 Bob 距离大于几个波长时，可认为窃听信道（Eve 与 Alice 和 Eve 与 Bob 之间的信道）与合法信道（Alice 与 Bob 之间的信道）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，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]。本节首先分析均匀散射环境中含噪窄带信道参数的统计特性；随后推导利用信道参数提取密钥时，密钥容量的时域闭式解。

3.1 信道参数的统计特性

当 Alice 在 t 时刻对信道进行测量时，测得含噪

上行信道参数 $\hat{h}_u(t)$，其 I/Q 分量可表示为

$$\hat{h}_{u_{\mathrm{I}}}(t)=\sum_{n=1}^{N(t)}\alpha_n(t)\cos\phi_n(t)+n_{\mathrm{I}}(t)=h_{u_{\mathrm{I}}}(t)+n_{\mathrm{I}}(t) \quad (2)$$

$$\hat{h}_{u_{\mathrm{Q}}}(t)=\sum_{n=1}^{N(t)}\alpha_n(t)\sin\phi_n(t)+n_{\mathrm{Q}}(t)=h_{u_{\mathrm{Q}}}(t)+n_{\mathrm{Q}}(t) \quad (3)$$

其中，$h_{u_{\mathrm{I}}}(t)$、$h_{u_{\mathrm{Q}}}(t)$ 表示上行信道参数 $h_u(t)$的同相、正交分量，$n_{\mathrm{I}}(t)$、$n_{\mathrm{Q}}(t)$ 是均值为零、方差为 $\sigma_h^2(t)$ 的高斯噪声；$\phi_n(t)=2\pi f_{\mathrm{c}}\tau_n(t)-\phi_{\mathrm{Dn}}(t)$ 是相位偏移，f_{c} 为载波频率，$\tau_n(t)$ 为时延，且信道的时延拓展远小于发送信号带宽的倒数，$\phi_{\mathrm{Dn}}(t)=2\pi f_{\mathrm{Dn}}(\tau)$ 为多普勒频移产生的相偏，$f_{\mathrm{Dn}}=\dfrac{v}{\lambda}\cos n\Delta\theta$ 表示多普勒频移。因为 $h(t)\sim\mathrm{CN}(0,\sigma_h^2(t))$，所以上行信道 I/Q 分量的功率满足 $P_{u_{\mathrm{I}}}=P_{u_{\mathrm{Q}}}=\mathrm{E}\left(\left|h_{u_{\mathrm{I}}}(t)\right|^2\right)=\mathrm{E}\left(\left|h_{u_{\mathrm{Q}}}(t)\right|^2\right)=0.5P_{\mathrm{A}}$，期望 $\mathrm{E}(h_{u_{\mathrm{I}}}(t))=\mathrm{E}(h_{u_{\mathrm{Q}}}(t))=0$，其中，$P_{\mathrm{A}}=\sigma_{\hat{h}_u}^2(t)$ 为上行信道参数总功率，此时 $\hat{h}_{u_{\mathrm{I}}}(t)$、$\hat{h}_{u_{\mathrm{Q}}}(t)$ 为联合高斯分布。同一时刻接收信号的 I/Q 分量的信噪比相同，即 $\hat{h}_{u_{\mathrm{I}}}(t),\ \hat{h}_{u_{\mathrm{Q}}}(t)\sim N(0,\sigma_{\hat{h}_u}^2(t))$，其中，$\sigma_{\hat{h}_u}^2(t)=0.5P_{\mathrm{A}}\left(1+\dfrac{1}{SNR_{\mathrm{A}}(t)}\right)$，Alice 端接收信号信噪比 $SNR_{\mathrm{A}}(t)=\dfrac{\sigma_{\hat{h}_u}^2(t)}{\sigma_n^2(t)}$，即 $\hat{h}_{u_{\mathrm{I}}}(t)$、$\hat{h}_{u_{\mathrm{Q}}}(t)$ 服从均值为零、方差为 $\sigma_{\hat{h}_u}^2$ 的高斯分布。

同理可得，Bob 在 $t+\tau$ 时刻进行信道测量的结果 $\hat{h}_d(t+\tau)$ 的 I/Q 分量 $\hat{h}_{d_{\mathrm{I}}}(t+\tau)$、$\hat{h}_{d_{\mathrm{Q}}}(t+\tau)$ 服从均值为零、方差为 $\sigma_{\hat{h}_d}^2(t+\tau)=0.5P_{\mathrm{B}}\left(1+\dfrac{1}{SNR_{\mathrm{B}}(t+\tau)}\right)$ 的高斯分布，其中，Bob 端接收信号信噪比 $SNR_{\mathrm{B}}(t+\tau)=\dfrac{P_{\mathrm{B}}}{\sigma_n^2(t+\tau)}$，下行信道参数总功率 $P_{\mathrm{B}}=\sigma_{\hat{h}_d}^2(t+\tau)$。假设无线介质各向同性且均匀，则由无线信道互易原理得，同一时刻通信双方之间的无线信道参数相同，即 $h_u(t)=h_d(t)$，$h_u(t+\tau)=h_d(t+\tau)$，其中，$h_d(t)$ 和 $h_d(t+\tau)$ 分别表示 t 和 $t+\tau$ 时刻下行无线信道参数信息。由上述分析可知，信道测量时差、终端移动及噪声确实降低了合法通信双方在不同时刻测量信道参数的相关性，而物理层安全密钥来源于测量信道参数的相关性，因此需要定量分析上述因素对 $\hat{h}_u(t)$ 与 $\hat{h}_d(t+\tau)$ 相关性的破坏程度，为物理层安全密钥提取提供理论参考。

3.2　密钥容量时域闭式解

由 3.1 节分析可知，合法通信双方测量的信道参数是具有相关性的复高斯随机变量，下面对利用具有一定相关性的信道参数提取密钥时的密钥容量进行分析。由于 I/Q 分量地位等价且分析方法相同，因此，在不失一般性的情况下选用 I 分量对密钥容量进行分析。又密钥容量 C_{S} 是双方测量信道参数的互信息，且高斯随机变量的互信息可通过相关系数表示[15, 21]。所以，利用 I 分量提取的物理层安全密钥容量 $C_{\mathrm{S_I}}$ 满足式(4)。

$$C_{\mathrm{S_I}}=I\left(\hat{h}_{u_{\mathrm{I}}}(t);\ \hat{h}_{d_{\mathrm{I}}}(t+\tau)\right)=-\frac{1}{2}\mathrm{lb}(1-\rho^2) \quad (4)$$

其中，ρ 表示双方测量信道参数的相关系数。

$$\rho=\rho_{\mathrm{I}}(v,\tau)=\frac{\mathrm{cov}\left(\hat{h}_{u_{\mathrm{I}}}(t),\ \hat{h}_{d_{\mathrm{I}}}(t+\tau)\right)}{\sigma_{\mathrm{A}}(t)\sigma_{\mathrm{B}}(t+\tau)}=\frac{\mathrm{cov}\left(\hat{h}_{u_{\mathrm{I}}}(t),\hat{h}_{d_{\mathrm{I}}}(t+\tau)\right)}{\mathrm{var}\left(\hat{h}_{u_{\mathrm{I}}}(t)\right)\mathrm{var}\left(\hat{h}_{d_{\mathrm{I}}}(t+\tau)\right)} \quad (5)$$

由于 $\mathrm{E}(\hat{h}_{u_{\mathrm{I}}}(t))=\mathrm{E}(\hat{h}_{u_{\mathrm{Q}}}(t))=0$，Alice 和 Bob 测量信道参数 $\hat{h}_{u_{\mathrm{I}}}(t)$ 与 $\hat{h}_{d_{\mathrm{I}}}(t+\tau)$ 的协方差可表示为

$$\mathrm{cov}(\hat{h}_{u_{\mathrm{I}}}(t),\ \hat{h}_{d_{\mathrm{I}}}(t+\tau))=\mathrm{E}\left(\left(\sum_{n=1}^{N(t)}\alpha_n(t)\cos\phi_n(t)\right)\left(\sum_{n=1}^{N(t+\tau)}\alpha_n(t+\tau)\cos\phi_n(t+\tau)\right)\right) \quad (6)$$

由于终端移动速度远小于光速，一次密钥提取过程中终端移动距离足够小，可认为在密钥提取时间内散射体数量 $N=N(t)=N(t+\tau)$、信道衰减 $\alpha_n=\alpha_n(t)=\alpha_n(t+\tau)$、终端移动速度 v 以及多普勒频移 f_{Dn} 保持不变。将 $\phi_n(t)=2\pi(f_c\tau_n-f_{\mathrm{Dn}}t)$（其中，$\tau_n$ 为传播时延）代入式(6)得到式(7)。

$$\begin{aligned}&\sum_{n=1}^{N}\mathrm{E}(\alpha_n^2)\mathrm{E}\left(\cos\phi_n(t)\cos\phi_n(t+\tau)\right)\\&=\sum_{n=1}^{N}\mathrm{E}(\alpha_n^2)\mathrm{E}\left(\cos(2\pi(f_{\mathrm{c}}\tau_n-f_{\mathrm{Dn}}t))\cdot\right.\\&\left.\cos(2\pi(f_{\mathrm{c}}\tau_n-f_{\mathrm{Dn}}\cdot(t+\tau)))\right)\end{aligned} \quad (7)$$

又由于 $f_{\mathrm{c}}\tau_n$ 变化程度远大于 $f_{\mathrm{Dn}}t$ 和 $f_{\mathrm{Dn}}\tau$，即 τ_n 变化很小就足以使接收信号的相位信息 2π 变化。故

可认为 $4\pi(f_c\tau_n - f_{Dn}t)+2\pi f_{Dn}\tau$ 在 $[0,2\pi]$ 范围内为均匀分布，所以 $\mathrm{E}(\cos(4\pi(f_c\tau_n - f_{Dn}t)+2\pi f_{Dn}\tau))=0$，进而有式(8)成立。

$$\begin{aligned}&\mathrm{E}(\cos(2\pi(f_c\tau_n - f_{Dn}t))\cos(2\pi(f_c\tau_n - f_{Dn}(t+\tau))))\\&=0.5\mathrm{E}(\cos(2\pi f_{Dn}\tau))\end{aligned} \tag{8}$$

因为均匀散射模型中各角度的入射功率相同且 $N = N(t)=N(t+\tau)$，假设 Alice 与 Bob 发射功率相同，则有 $P_A = \sigma^2_{h_u} = \sigma^2_{h_d} = P_B = P$，其中，$P$ 为接收端信道参数总功率。令 $N=\dfrac{2\pi}{\Delta\theta}$，则每条散射径的功率 $P_n = E(\alpha_n^2)=\dfrac{P}{N}$。结合式(7)和式(8)，式(6)可化简为

$$\begin{aligned}&\mathrm{cov}(\hat{h}_{u_\mathrm{I}}(t),\ \hat{h}_{d_\mathrm{I}}(t+\tau))\\&=\sum_{n=1}^{N}\frac{0.5P}{2\pi}\mathrm{E}\left(\cos\left(\frac{2\pi v\tau\cos(n\Delta\theta)}{\lambda}\right)\right)\Delta\theta\end{aligned} \tag{9}$$

当 $N\to+\infty$ 时，式(6)可进一步化简为

$$\begin{aligned}&\mathrm{E}(\hat{h}_{u_\mathrm{I}}(t)\ \hat{h}_{d_\mathrm{I}}(t+\tau))\\&=\frac{0.5P}{2\pi}\int\cos\left(\frac{2\pi v\tau\cos\theta}{\lambda}\right)\mathrm{d}\theta=0.5PJ_0\left(\frac{2\pi v\tau}{\lambda}\right)\end{aligned} \tag{10}$$

其中，$J_0(x)=\dfrac{1}{\pi}\int_0^{\pi}\exp(-\mathrm{j}x\cos\theta)\mathrm{d}\theta$ 是零阶贝塞尔函数。因此，$\hat{h}_{u_\mathrm{I}}(t)$ 与 $\hat{h}_{d_\mathrm{I}}(t+\tau)$ 的相关系数为

$$\rho_\mathrm{I}(v,\tau)=\frac{J_0\left(\dfrac{2\pi v\tau}{\lambda}\right)}{\sqrt{\left(1+\dfrac{1}{SNR_\mathrm{A}(t)}\right)\left(1+\dfrac{1}{SNR_\mathrm{B}(t+\tau)}\right)}} \tag{11}$$

同理可得 $\rho(v,\tau)=\rho_\mathrm{Q}(v,\tau)=\rho_\mathrm{I}(v,\tau)$。将式(11)代入式(4)，得到利用信道参数的 I 分量（或 Q 分量）提取密钥时的密钥容量 $C_{S_\mathrm{I}}(C_{S_\mathrm{Q}})$

$$C_{S_\mathrm{I}}=C_{S_\mathrm{Q}}=-\frac{1}{2}\mathrm{lb}\left(1-\frac{J_0\left(\dfrac{2\pi v\tau}{\lambda}\right)^2}{\left(1+\dfrac{1}{SNR_\mathrm{A}(t)}\right)\left(1+\dfrac{1}{SNR_\mathrm{B}(t+\tau)}\right)}\right) \tag{12}$$

利用式(6)~式(10)的分析过程可得 $\mathrm{cov}(\hat{h}_{u_\mathrm{I}}(t),\ \hat{h}_{d_\mathrm{Q}}(t+\tau))=0$，即 $\hat{h}_{u_\mathrm{I}}(t)$ 与 $\hat{h}_{d_\mathrm{Q}}(t+\tau)$ 不相关，则高斯型随机变量 $\hat{h}_{u_\mathrm{I}}(t)$ 与 $\hat{h}_{d_\mathrm{Q}}(t+\tau)$ 相互独立。又由于可同时利用 I 和 Q 分量进行物理层安全密钥提取，因此均匀散射环境中密钥容量为

$$\begin{aligned}C_\mathrm{S}&=C_{S_\mathrm{I}}+C_{S_\mathrm{Q}}\\&=-\mathrm{lb}\left(1-\frac{J_0\left(\dfrac{2\pi v\tau}{\lambda}\right)^2}{\left(1+\dfrac{1}{SNR_\mathrm{A}(t)}\right)\left(1+\dfrac{1}{SNR_\mathrm{B}(t+\tau)}\right)}\right)\end{aligned} \tag{13}$$

特别地，当 $v\tau=0$ 时

$$\begin{aligned}C_\mathrm{S}&=-\mathrm{lb}\left(1-\frac{1}{\left(1+\dfrac{1}{SNR_\mathrm{A}(t)}\right)\left(1+\dfrac{1}{SNR_\mathrm{B}(t+\tau)}\right)}\right)\\&=\mathrm{lb}(1+SNR_\mathrm{eq})\end{aligned} \tag{14}$$

其中，

$$SNR_\mathrm{eq}=\left(\frac{1}{SNR_\mathrm{A}(t)}+\frac{1}{SNR_\mathrm{B}(t+\tau)}+\frac{1}{SNR_\mathrm{A}(t)SNR_\mathrm{B}(t+\tau)}\right)^{-1} \tag{15}$$

对比文献[4]可知，其密钥容量为本文式(12)在 $v\tau=0$ 时的特例。

由上述分析可知，在均匀散射环境中窄带无线信道参数近似服从复高斯分布。且利用无线信道参数提取物理层安全密钥时，密钥容量可由信道测量时差、终端移动速度和信噪比定量表示。

4 仿真分析

仿真条件采用 Fontán[22]给出的典型均匀散射环境（如图 2 所示）的仿真条件；仿真方法采用文献[23~25]给出的 Copula 熵估计算法，进行密钥容量估计；仿真数据通过 10^5 次独立的蒙特卡洛仿真实验得到。本节首先验证推导结果的正确性，并定量分析信道测量时差 τ、终端移动速度 v 和 SNR 对密钥容量的影响；随后在非均匀散射环境中验证推导结果的适用性（适用性指式(13)对于均匀散射环境和非均匀散射环境均适用）。

4.1 正确性验证

在图 2 所示的均匀散射仿真环境中，通过 10^5 次蒙特卡洛实验得到仿真数据。仿真条件如下。

1) Bob 的各角度入射功率相同，载波频率为 2 GHz，且 Alice 和 Bob 之间没有直达径。

2) $SNR\in[0, 20]$dB 且 $SNR_\mathrm{A}(t)= SNR_\mathrm{B}(t+\tau)$。

3) Bob 沿着 x 轴正向移动，速度 $v\in[0, 200]$ m/s，信道测量时差 $\tau\in[0, 200]$ μs。

4) 每次仿真中 Alice 位置固定，1 000 个散射点在以原点为圆心、半径为 200 m 的圆周上按照[0,2π]的均匀分布随机产生。

仿真步骤如下。

1) 如图 2 所示，在以原点为圆心，200 m 为半径的圆周上，按照[0, 2π]的均匀分布随机产生 1 000 个散射点。

2) 固定 Alice 位置在(−700, 700) m，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 t 和 $t+\tau$ 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) 利用仿真数据计算相关系数估计值，同时根据文献[25]处理仿真数据得到密钥容量估计值。

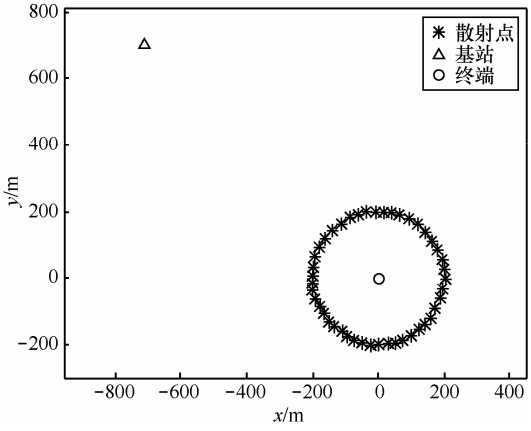


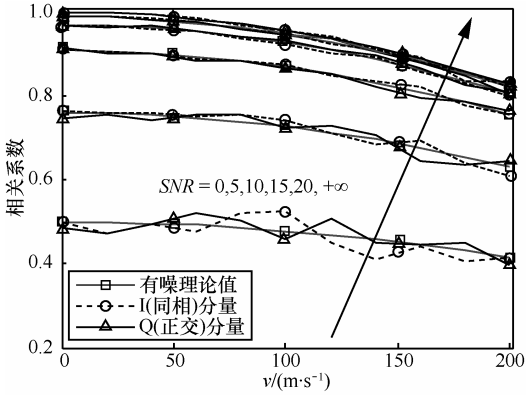
图 2　均匀散射环境仿真示意

在图 2 所示的均匀散射模型中进行仿真。图 3(a)、图 4(a)分别为 $\tau=100$ μs 条件下信道参数相关系数、密钥容量与移动速度和 *SNR* 关系；图 3(b)、图 4(b)为 $v=100$ m/s 条件下信道参数相关系数、密钥容量与测量时间差和 *SNR* 关系。

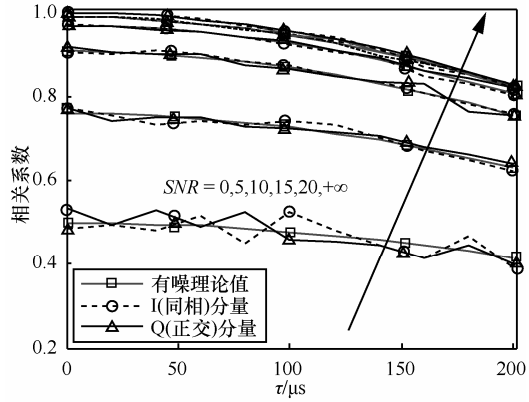
随着箭头指向，对应的 6 组曲线的 *SNR* 分别为 0 dB、5 dB、10 dB、15 dB、20 dB 和+∞ dB（下同），图 3 中有噪理论值指式(11)计算的 I(Q)分量的相关系数；I(Q)分量指在仿真条件下，利用仿真数据估计的 I(Q)分量相关系数估计值。

图 4 中有噪理论值指式(12)计算的 I(Q)分量的密钥容量理论值；I(Q)分量指在仿真条件下，利用仿真数据得到的 I(Q)分量密钥容量的估计值。

由图 3 可知，随着 *SNR* 的提高，信道参数的相关系数逐渐提高；且随着 *SNR* 的提高，利用仿真数据估计的相关系数与式(11)计算的理论值一致性逐

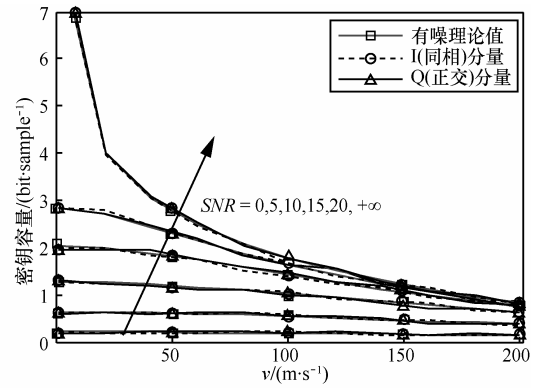


(a) 信道参数相关系数与移动速度和*SNR*关系

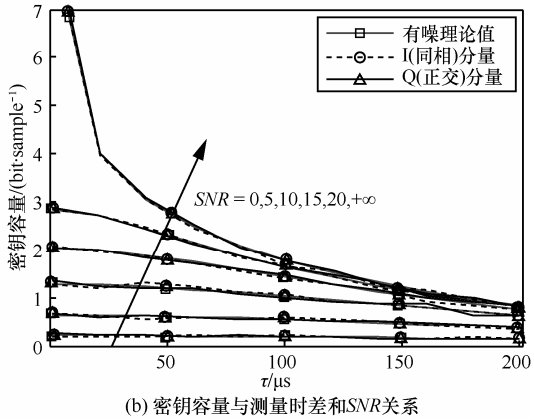


(b) 信道参数相关系数与测量时差和*SNR*关系

图 3　均匀散射环境中信道参数相关系数变化曲线



(a) 密钥容量与移动速度和*SNR*关系



(b) 密钥容量与测量时差和*SNR*关系

图 4　均匀散射环境中密钥容量变化曲线

渐增强。由图 4 可知，随着 *SNR* 提高，密钥容量逐渐提升。特别地，当 *SNR* 趋近于无穷大且 Alice 和 Bob 位置保持不动时，密钥容量趋于无穷大。

由图 3 和图 4 可得仿真估计值与式(11)和式(12)一致性较好，验证了推导结果的正确性。对比图 3(a)和图 3(b)、图 4(a)和图 4(b)可知，测量时间差 τ 与移动速度 v 对相关系数以及密钥容量的贡献相同。这是由于移动距离 $s=v\tau$，即 v 和 τ 共同作用，改变终端的空间位置，进而影响信道状态。

4.2　适用性验证

如图 5 所示，在非均匀散射环境中进行密钥容量估计，通过与式(12)计算的密钥容量理论值比较，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。

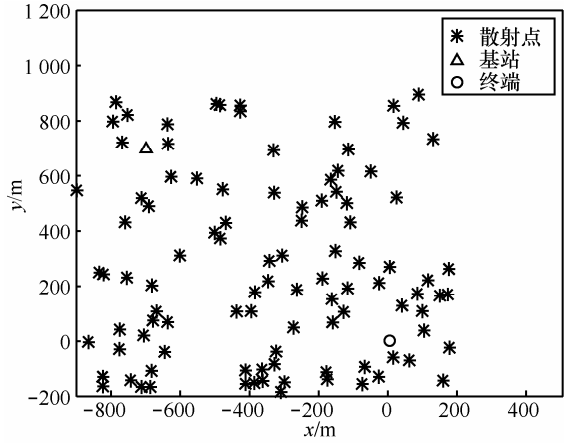


图 5　非均匀散射环境仿真示意

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 之间没有直达径，载波频率为 2 GHz。

2) $SNR\in[0, 20]$ dB，且 $SNR_{\mathrm{A}}(t)= SNR_{\mathrm{B}}(t+\tau)$。

3) Bob 沿着 x 轴正向移动，速度 $v\in[0, 200]$ m/s，信道测量时差 $\tau\in[0, 200]$ μs。

4) 每次仿真中 Alice 位置固定，100 个散射点在 $x\in[-900, 200]$ m，$y\in[-200, 900]$ m 内均匀产生。

仿真步骤如下。

1) 在 $x\in[-900, 200]$ m，$y\in[-200, 900]$ m 的矩形区域内，按照均匀分布产生 100 个散射点。

2) 固定 Alice 位置在(−700,700)m，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 t 和 $t+\tau$ 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) 利用仿真数据计算相关系数估计值，同时根据文献[25]得到密钥容量估计值。

图 6(a)、图 6(b)分别为在图 5 所示非均匀散射仿真环境中，当 $v=100$ m/s 时，信道参数相关系数、密钥容量与信道测量时差和 *SNR* 关系。

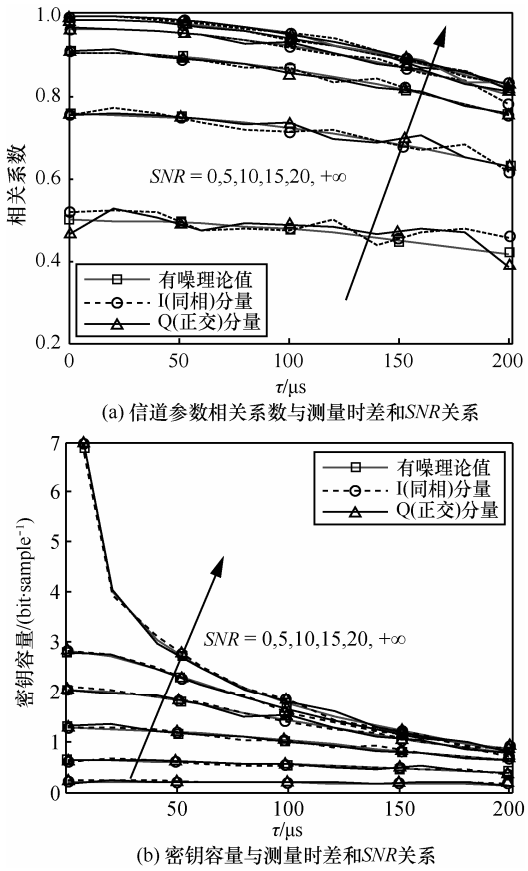


图 6　非均匀散射环境中信道参数相关系数和密钥容量变化曲线

由图 6 可知，在图 5 所示的非均匀散射环境中，利用仿真数据估计的信道参数相关系数以及密钥容量，与分别利用式(11)和式(12)计算的信道参数相关系数和密钥容量较为吻合。这是由大数定理保证的，具体地，是因为密集分布的散射体能够保证 Alice 和 Bob 之间的信道参数仍可近似为复高斯分布。进而保证推导结果并不局限于均匀散射环境，对于存在大量散射体的非均匀散射环境依然适用。

综合 4.1 节和 4.2 节可知，利用式(13)能够分析在有大量散射体的环境中，利用无线信道参数提取物理层安全密钥时的密钥容量。

5　结束语

本文在均匀散射环境中，推导了利用无线信道参

数提取物理层安全密钥时，密钥容量的时域闭式解，能够定量分析信道测量时差、终端移动和加性噪声对密钥容量的影响。本文首先分析了均匀散射环境中含噪信道参数的时域统计特性；随后将密钥容量计算问题转化为随机变量的互信息计算问题，推导了密钥容量时域闭式解；最后通过蒙特卡洛仿真，分别在均匀散射和非均匀散射环境中验证了推导结果的正确性和适用性。仿真结果表明，在有大量散射体的环境中，根据给定的信道测量时差、终端移动速度和信噪比可近似确定密钥容量。该结论可以为在散射丰富的移动通信环境中，提取物理层安全密钥提供理论参考。

参考文献：

[1] SHEHADEH Y E H, HOGREFE D. A survey on secret key generation mechanisms on the physical layer in wireless networks [J]. Security and Communication Networks, 2015, 8(2): 332-41.

[2] WANG T, LIU Y, VASILAKOS A V. Survey on channel reciprocity based key establishment techniques for wireless systems [J]. Wireless Networks, 2015, 21(6): 1835-46.

[3] THAI C D T, LEE J, QUEK T Q. Physical-layer secret key generation with colluding untrusted relays [J]. IEEE Transactions on Wireless Communications, 2016, 15(2): 1517-30.

[4] CHOU T H, DRAPER S C, SAYEED A M. Key generation using external source excitation: capacity, reliability, and secrecy exponent[J]. IEEE Transactions on Information Theory, 2012, 58(4): 2455-74.

[5] PFENNIG S, FRANZ E, ENGELMANN S, et al. End-to-end key establishment with physical layer key generation and specific attacker models [M]. Physical and Data-Link Security Techniques for Future Communication Systems. Springer, 2016: 93-110.

[6] 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): 917-30.

[7] TSOURI G R, WAGNER D M. Threshold constraints on symmetric key extraction from rician fading estimates [J]. IEEE Transactions on Mobile Computing, 2013, 12(12): 2496-506.

[8] 戴峤, 宋华伟, 金梁. 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): 1580-92.
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.

[9] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-42.

[10] AHLSWEDE R, CSISZÁR I. Common randomness in information theory and cryptography. part I: secret sharing [J]. IEEE Transactions on Information Theory, 1993, 39(4): 1121-32.

[11] AHLSWEDE R, CSISZÁR I. Common randomness in information theory and cryptography part II: CR capacity [J]. IEEE Transactions on Information Theory, 1998, 44(1): 225-40.

[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.

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

[14] SHEHADEH Y E H, ALFANDI O, HOGREFE D. Towards robust key extraction from multipath wireless channels [J]. Journal of Communications and Networks, 2012, 4(14): 385-95.

[15] NITINAWARAT S, NARAYAN P. Secret key generation for correlated Gaussian sources[J]. IEEE Transactions on Information Theory, 2012, 58(6): 3373-3391.

[16] WU X, SONG Y, ZHAO C, et al. Secrecy extraction from correlated fading channels: an upper bound[C]//IEEE International Conference on Wireless Communications & Signal Processing. Nanjing, China, 2009.

[17] CLARKE R. A statistical theory of mobile‐radio reception [J]. Bell System Technical Journal, 1968, 47(6): 957-1000.

[18] JAKES W C, COX D C. Microwave mobile communications [M]. New Jersey, USA: Wiley-IEEE Press, 1994.

[19] GOLD S A. Wireless communications[M]. Cambridge, UK: Cambridge University Press, 2005.

[20] CHEN C, JENSEN M. Secret key establishment using temporally and spatially correlated wireless channel coefficients[J]. IEEE Transactions on Mobile Computing, 2011, 10(2): 205-215.

[21] COVER T M, THOMAS J A. Elements of information theory [M]. New Jersey, USA: John Wiley & Sons, 2012.

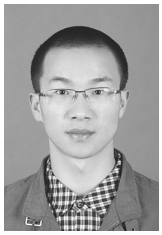
[22] FONTÁN F P, ESPIÑEIRA P M. Modelling the wireless propagation channel: a simulation approach with matlab [M]. New Jersey, USA: John Wiley & Sons, 2008.

[23] ZENG X, DURRANI T. Estimation of mutual information using copula density function [J]. Electronics Letters, 2011, 47(8): 493-494.

[24] MA J, SUN Z. Mutual information is copula entropy [J]. Tsinghua Science & Technology, 2011, 16(1): 51-4.

[25] 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.
HAN M,LIU X X. Mutual information estimation based on copula entropy[J]. Control Theory & Applications, 2013, 30(7): 875-879.

作者简介：



王旭（1990-），男，河南郑州人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线通信网络与信息安全等。

金梁（1969-），男，北京人，博士，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为无线通信安全等。

刘璐（1988-），男，安徽宿州人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线通信网络与信息安全等。

李明亮（1988-），男，河南周口人，国家数字交换系统工程技术研究中心博士生，主要研究方向为无线通信网络与信息安全等。

黄开枝（1973-），女，安徽滁州人，博士，国家数字交换系统工程技术研究中心教授、博士生导师，主要研究方向为无线通信安全等。