DOI：10.7652/xjtuxb201406006

一种无线信道密钥容量求解方法

蔡文炳[1,2]，付红双[2]，张水莲[2]，孙有铭[2]，于大鹏[2]
（1.北京跟踪与通信技术研究所，100094，北京；2.信息工程大学信息系统工程学院，450002，郑州）

摘要：为了准确求解合法通信双方利用无线信道生成共享密钥的容量，借助于瑞利衰落统计模型和互易性对无线信道进行建模，得到合法双方接收信号的统计分布；通过对统计分布进行雅克比变换分别推导出双方包络的联合分布和相位的联合分布，进而通过互信息公式求解出相应的两个密钥容量表达式。利用窄带信道的互易性，提出了一种发送信号为非相干载波的密钥生成协议，合法双方在相干时间内以时分双工(TDD)方式对无线信道进行多载波探测，双方分别利用接收信号包络、相位信息生成密钥，将两密钥去除相关性后拼接起来作为最终的密钥以用于安全通信。该协议能够同时利用接收信号的包络和相位信息，且密钥容量与非相干载波的个数成正比。仿真结果表明：分别基于信号包络、相位信息生成的密钥存在相关性；仅由包络和相位信息生成密钥并未充分利用信道特性信息，当信噪比为 10 dB 时，利用接收信号包络、相位的密钥容量的数值求和比利用接收信号的密钥容量低 0.3 b/s。

关键词：无线信道；密钥生成；密钥容量；相干载波
中图分类号：TN911.2 **文献标志码**：A **文章编号**：0253-987X(2014)06-0031-06

A Solution of the Secret Key Capacity for Wireless Channel

CAI Wenbing[1,2], FU Hongshuang[2], ZHANG Shuilian[2], SUN Youming[2], YU Dapeng[2]
(1. Beijing Institute of Tracking and Telecommunication Technology, Beijing 100094, China;
2. Institute of Information System Engineering, Information Engineering University, Zhengzhou 450002, China)

Abstract: A model for wireless channel is established to evaluate accurately the capacity of the shared secret key generated by legitimate users in the channel. The building of the model is based on statistical models of Rayleigh fading and reciprocity from the statistical distribution of the received signals. The joint probability density functions of both the envelope and the phase at the legitimate users are respectively derived by using a Jacobi transform. The corresponding expressions of the two secret key capacities are then deduced by using the formula of mutual information. Then a protocol of secret key generation in which the transmitted signals are multi-carriers is presented by utilizing the reciprocity of the narrowband channel. The legitimate users implement the multi-carrier channel sounding in TDD mode within the coherence time, and exploit the information of envelope and phase in the received signals to generate secret keys. The keys are spliced together to realize secure communication by removing the correlation between them. The proposed protocol can use information of the envelope and the phase simultaneously, and the capacity of the secret key is proportional to the number of carriers. Simulation results show that correlation exists between the secret keys generated based on information of the

收稿日期：2013-10-16。 作者简介：蔡文炳(1988—)，男，硕士，工程师；张水莲(通信作者)，女，教授。 基金项目：国家"863 计划"资助项目(2009AA011205，2013AA013603)；国家自然科学基金资助项目(61271253)。
网络出版时间：2014-03-19 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20140319.1749.001.html

envelope and the phase, and that the numerical sum of key capacity that exploits information of the envelope and the phase is lower than that of received signals by 0.3 bit/s when the SNR is 10 dB. It can be concluded that legitimate users can utilize more information in the received signals to generate shared secret key.

Keywords: wireless channel; secret key generation; secret key capacity; coherent carriers

无线信道的广播特性使得信息的安全传输成为一个非常重要的问题。密码学是保障信息安全的重要工具之一。目前,广泛应用的密码体制大多依赖于没有严格证明的数学难题和计算复杂性,只能够实现计算安全,而基于无线信道特性的生成密钥并结合"一次一密"加密体制能够实现无条件安全。因此,基于无线信道特性的密钥生成方法由于其较强的理论性和良好的应用前景,近年来引起了人们的广泛关注,并成为了当前的一个研究热点。

Hershey 和 Maurer 等学者先后指出,无线信道可以作为一个公共随机源,并且这个公共随机源对窃听方来说是保密的[1-2]。当合法双方以时分双工(TDD)方式对无线信道进行探测时,信道的时变性使得合法双方能够生成具有噪声性质的真随机的密钥,互易性使得双方在生成密钥的同时实现了密钥分发[3],而无线信道的空变性能够实现密钥分发过程的物理安全性。因此,合法双方可以利用无线信道的这些特性生成共享密钥,从而实现安全通信的目标。

当合法通信双方以 TDD 方式对无线信道进行探测时,双方可以利用接收信号中包含的丰富信道特性信息来生成共享密钥。文献[4-6]利用接收信号包络来生成密钥;文献[7-8]指出可以通过观察接收信号相位来得到共享密钥;文献[9-10]给出了从相关复高斯信号中生成共享密钥的简便方法。可以看出,由于接收信号的包络、相位信息较易提取,使得目前的密钥生成实验常利用包络和相位信息来进行,因此研究给定模型下合法双方基于接收信号包络、相位信息的密钥容量将对实际的密钥生成过程具有重要的指导意义。本文首先对窃听信道进行建模,在此基础上,利用随机信号分析及信息论的相关理论,推导得到了基于接收信号包络、相位信息的最大密钥生成速率,即密钥容量的数学表达式,并对结果进行了仿真分析。最后,利用无线信道的互易性,提出了一种基于多载波的密钥生成协议,合法双方能够同时提取接收信号中的包络和相位信息以生成共享密钥,且密钥容量与探测信号中非相干载波的个数成正比。

1 基本的源模型

假定两个合法终端 Alice 和 Bob 分别对各自的信道输出 X、Y 进行 n 次独立观察,得到的序列分别记作 $\boldsymbol{X}=(X_1,\cdots,X_n)$、$\boldsymbol{Y}=(Y_1,\cdots,Y_n)$。Alice 和 Bob 能够通过一个无错(Error-Free)的公开讨论信道相互通信,记 V 为公开讨论信道上的所有通信内容。在任意给定的时刻,合法双方的观察(X_i,Y_i)是强相关的。基于双方各自的相关观察,Alice 能够生成密钥序列 $\boldsymbol{K}_1$,并且 $\boldsymbol{K}_1$ 是$(\boldsymbol{X},V)$的函数;Bob 能够生成密钥序列 $\boldsymbol{K}_2$,$\boldsymbol{K}_2$ 为$(\boldsymbol{Y},V)$的函数。

对于任意的 $\varepsilon>0$ 和足够大的 n,如果 $\boldsymbol{K}_1$ 和 $\boldsymbol{K}_2$ 满足

$$P(\boldsymbol{K}=\boldsymbol{K}_1=\boldsymbol{K}_2)\geqslant 1-\varepsilon \tag{1}$$

$$I(\boldsymbol{K};V)\leqslant \varepsilon \tag{2}$$

$$H(\boldsymbol{K})\geqslant \mathrm{lb}\,|\boldsymbol{K}|-\varepsilon \tag{3}$$

式中:$P(\cdot)$表示概率;$I(\cdot)$表示互信息;$H(\cdot)$表示信息熵。则,$\boldsymbol{K}_1$、$\boldsymbol{K}_2$ 称为 ε 密钥,$|\boldsymbol{K}|$是 $\boldsymbol{K}$ 的所有可能取值构成的集合的势。

式(1)保证了 Alice 和 Bob 能够以很高的概率生成相同的密钥;式(2)保证了所生成的密钥对能够观察到合法双方在公开讨论信道上进行信息交互的窃听方来说是保密的;式(3)保证了合法双方所生成的密钥接近均匀分布。

对于任意小的 $\varepsilon>0$ 和足够大的 n,如果 $\varepsilon-(\boldsymbol{K}_1,\boldsymbol{K}_2)$密钥是可达的,并且

$$\frac{1}{n}H(\boldsymbol{K}_1)\geqslant R_{\mathrm{key}}-\varepsilon \tag{4}$$

成立,则称 R_{key}为可达的密钥生成速率,所有可达的密钥生成速率的上界称为密钥容量,记作 C_{SK}。对于以上模型,由文献[2,11]可知

$$C_{\mathrm{SK}}=I(X;Y) \tag{5}$$

在上面定义的模型中,假定窃听方 Eve 可以观察到公开讨论信道上传输的信息,但是不能对其进行篡改,并且不能获得任何其他有用的边信息(边信息指窃听方通过窃听合法双方的信道探测过程而获得的信息)。虽然窃听方能够获得边信息的情形引起了学者们的广泛关注(如文献[2,12]),但是这种

情况下的容量求解依然是一个亟待解决的问题。

2　信道建模及密钥容量的求解

2.1　信道建模

对于窄带平坦衰落信道,合法双方 Alice 和 Bob 以 TDD 方式互发探测序列,并且双方的探测时间间隔小于信道的相干时间。发送信号 s 和接收信号 r 之间的关系可表示为 $r=Fs+n$(其中 F 为信道增益),当信道为瑞利信道时,F 为复高斯随机过程,n 为独立的加性噪声。由于收发双方通常都已知探测信号 s,所以在任意给定时刻,Alice 和 Bob 的信道输出 X、Y 可分别设为

$$\left.\begin{aligned} X &= h + N_{\mathrm{a}} \\ Y &= h + N_{\mathrm{b}} \end{aligned}\right\} \tag{6}$$

式中:h 为 Alice 和 Bob 之间的信道增益,且 $h\sim \mathrm{CN}(0,\sigma^2)$,为分析方便,假定信道探测过程中,合法双方之间的信道完全互易。N_{a}、N_{b} 为独立同分布的复高斯随机变量 $\mathrm{CN}(0,\sigma_{\mathrm{n}}^2)$,对应观测噪声。

将上述分布代入式(6)中,得到

$$\begin{bmatrix} X \\ Y \end{bmatrix} \sim \mathrm{CN}[\boldsymbol{0},\boldsymbol{B}_{XY}] \tag{7}$$

式中:$\boldsymbol{B}_{XY}$ 为信道输出 X、Y 的协方差矩阵,表达式为

$$\boldsymbol{B}_{XY} = \sigma_{\mathrm{n}}^2 \begin{bmatrix} 1+\gamma & \gamma \\ \gamma & 1+\gamma \end{bmatrix} \tag{8}$$

式中:定义 $\gamma=\sigma^2/\sigma_{\mathrm{n}}^2$ 为信道的输出信噪比,不失一般性,假定 $\sigma_{\mathrm{n}}^2=1$。

由于接收信号 X、Y 均为复高斯随机变量,故可表示成如下形式

$$\left.\begin{aligned} X &= A_1\exp(\mathrm{j}\phi_1) = A_{\mathrm{c1}} + \mathrm{j}A_{\mathrm{s1}} \\ Y &= A_2\exp(\mathrm{j}\phi_2) = A_{\mathrm{c2}} + \mathrm{j}A_{\mathrm{s2}} \end{aligned}\right\} \tag{9}$$

式中:A_1、A_2 分别为 X、Y 的包络;ϕ_1、ϕ_2 分别为 X、Y 的相位;A_{c1}、A_{s1} 分别为 X 的实部和虚部;A_{c2}、A_{s2} 分别为 Y 的实部和虚部。A_{c1}、A_{s1}、A_{c2} 和 A_{s2} 均为 0 均值、方差为 $\sigma_0^2=\sigma_X^2/2=\sigma_Y^2/2=(1+\gamma)/2$ 的高斯随机变量,σ_X^2、σ_Y^2 分别为 X、Y 的方差。A_{c1} 和 A_{c2} 的相关系数为

$$\rho = \frac{E(A_{\mathrm{c1}},A_{\mathrm{c2}})}{(E(A_{\mathrm{c1}}^2))^{1/2}(E(A_{\mathrm{c2}}^2))^{1/2}} = \frac{\gamma/2}{(1+\gamma)/2} = \frac{\gamma}{1+\gamma} \tag{10}$$

式中:$E(\cdot)$ 表示随机变量的期望。

2.2　密钥容量的求解

基于以上假设条件,得到包络和相位的四维联合概率密度 $p_4(\boldsymbol{A})$ 为

$$p_4(\boldsymbol{A}) = \frac{1}{(2\pi)^{n/2}\,|\,\boldsymbol{B}_{\boldsymbol{A}}\,|^{1/2}}\exp\left[-\frac{1}{n}\boldsymbol{A}^{\mathrm{T}}\boldsymbol{B}_{\boldsymbol{A}}^{-1}\boldsymbol{A}\right] \tag{11}$$

式中:$n=4$;$\boldsymbol{A}=[A_{\mathrm{c1}}\quad A_{\mathrm{s1}}\quad A_{\mathrm{c2}}\quad A_{\mathrm{s2}}]^{\mathrm{T}}$,其对应的协方差矩阵 $\boldsymbol{B}_{\boldsymbol{A}}$ 的表达式为

$$\boldsymbol{B}_{\boldsymbol{A}} = \begin{bmatrix} \frac{1+\gamma}{2} & 0 & \frac{\gamma}{2} & 0 \\ 0 & \frac{1+\gamma}{2} & 0 & \frac{\gamma}{2} \\ \frac{\gamma}{2} & 0 & \frac{1+\gamma}{2} & 0 \\ 0 & \frac{\gamma}{2} & 0 & \frac{1+\gamma}{2} \end{bmatrix} \tag{12}$$

其中$[\cdot]^{-1}$表示矩阵求逆。设 D 为矩阵 $\boldsymbol{B}_{\boldsymbol{A}}$ 的行列式,即 $D=|\boldsymbol{B}_{\boldsymbol{A}}|=[\sigma_0^4-(\gamma/2)^2]^2$,将 $\boldsymbol{B}_{\boldsymbol{A}}$ 代入式(11)得到

$$p_4(A_{\mathrm{c1}},A_{\mathrm{s1}},A_{\mathrm{c2}},A_{\mathrm{s2}}) = \frac{1}{4\pi^2 D^{1/2}}\cdot \exp\left\{-\frac{1}{2D^{1/2}}[\sigma_0^2(A_{\mathrm{c1}}^2+A_{\mathrm{s1}}^2+A_{\mathrm{c2}}^2+A_{\mathrm{s2}}^2)]+\frac{1}{2D^{1/2}}[\gamma(A_{\mathrm{c1}}A_{\mathrm{c2}}+A_{\mathrm{s1}}A_{\mathrm{s2}})]\right\} \tag{13}$$

因为

$$\left.\begin{aligned} A_{\mathrm{c1}} &= A_1\cos\phi_1; \quad A_{\mathrm{c2}} = A_2\cos\phi_2 \\ A_{\mathrm{s1}} &= A_1\sin\phi_1; \quad A_{\mathrm{s2}} = A_2\sin\phi_2 \end{aligned}\right\} \tag{14}$$

所以有

$$p_4(A_1,\phi_1,A_2,\phi_2) = |J|\,p_4(A_{\mathrm{c1}},A_{\mathrm{s1}},A_{\mathrm{c2}},A_{\mathrm{s2}}) = |J|\,p_4(A_1\cos\phi_1,A_1\sin\phi_1,A_2\cos\phi_2,A_2\sin\phi_2) \tag{15}$$

式中:J 为雅克比系数,对应的值为

$$J = \frac{\partial(A_{\mathrm{c1}},A_{\mathrm{s1}},A_{\mathrm{c2}},A_{\mathrm{s2}})}{\partial(A_1,\phi_1,A_2,\phi_2)} = A_1A_2 \tag{16}$$

将式(13)、(14)和式(16)代入式(15)中,得到包络和相位的四维联合概率密度 $p_4(A_1,\phi_1,A_2,\phi_2)$ 为

$$p_4(A_1,\phi_1,A_2,\phi_2) = \begin{cases} \dfrac{A_1A_2}{4\pi^2D^{1/2}}\exp\left\{-\dfrac{1}{2D^{1/2}}[\sigma_0^2(A_1^2+A_2^2]+\dfrac{\gamma}{2D^{1/2}}[A_1A_2\cos(\phi_1-\phi_2)]\right\}, & \begin{matrix} A_1,A_2\geqslant 0 \\ 0\leqslant\phi_1,\phi_2\leqslant 2\pi \end{matrix} \\ 0, \quad \text{其他} \end{cases} \tag{17}$$

对式(17)中的 ϕ_1 和 ϕ_2 进行积分,得到接收信号包络的二维联合概率密度 $p_2(A_1,A_2)$ 为

$$p_2(A_1,A_2) = \int_0^{2\pi}\int_0^{2\pi} p_4(A_1,\phi_1,A_2,\phi_2)\,\mathrm{d}\phi_1\,\mathrm{d}\phi_2 = \begin{cases} \dfrac{A_1A_2}{D^{1/2}}\mathrm{I}_0\left(\dfrac{A_1A_2\gamma}{2D^{1/2}}\right)\exp\left[-\dfrac{\sigma_0^2(A_1^2+A_2^2)}{2D^{1/2}}\right], & A_1,A_2\geqslant 0 \\ 0, & \text{其他} \end{cases} \tag{18}$$

式中：$I_0(x)=1/(2\pi)\int_0^{2\pi}\exp(x\cos\phi)\mathrm{d}\phi$ 为第一类零阶修正的贝塞尔函数。

对式(17)中的 A_1 和 A_2 进行积分，得到接收信号相位的二维联合概率密度 $p_2(\phi_1,\phi_2)$ 为

$$p_2(\phi_1,\phi_2)=\int_0^{\infty}\int_0^{\infty}p_4(A_1,\phi_1,A_2,\phi_2)\mathrm{d}A_1\mathrm{d}A_2=\begin{cases}\dfrac{D^{1/2}}{4\pi^2\sigma_0^4}\left[\dfrac{(1-\beta^2)^{1/2}+\beta(\pi-\cos^{-1}\beta)}{(1-\beta^2)^{3/2}}\right], & 0\leqslant\phi_1,\phi_2\leqslant 2\pi\\ 0, & \text{其他}\end{cases}\tag{19}$$

式中：$\beta=\gamma\cos(\phi_2-\phi_1)/2\sigma_0^2$。

式(18)、(19)分别给出了合法双方接收信号包络的联合分布和接收信号相位的联合分布。由式(5)可知，求解密钥容量可转化为相应的互信息的计算，其计算公式为[13]

$$I(X;Y)=\iint_{xy}p(x,y)\mathrm{lb}\frac{p(x,y)}{p(x)p(y)}\mathrm{d}x\mathrm{d}y=\iint_{xy}p(x,y)\mathrm{lb}\frac{p(x,y)}{\int_y p(x,y)\mathrm{d}x\int_y p(x,y)\mathrm{d}y}\mathrm{d}x\mathrm{d}y\tag{20}$$

式中：X 和 Y 为任意两个随机变量；$p(x)$、$p(y)$ 分别为 X、Y 的概率密度；$p(x,y)$ 为随机变量 X、Y 的联合概率密度。

将合法双方接收信号包络的联合概率密度 $p_2(A_1,A_2)$ 代入式(20)中，得到基于接收信号包络的密钥容量 C_{E} 为

$$C_{\mathrm{E}}=\mathrm{I}(A_1,A_2)=\int_0^{+\infty}\int_0^{+\infty}p_2(A_1,A_2)\cdot\mathrm{lb}\frac{p_2(A_1,A_2)}{\int_0^{+\infty}p_2(A_1,A_2)\mathrm{d}A_2\int_0^{+\infty}p_2(A_1,A_2)\mathrm{d}A_1}\mathrm{d}A_1A_2\tag{21}$$

将合法双方接收信号相位的联合概率密度 $p_2(\phi_1,\phi_2)$ 代入式(20)中，得到基于接收信号相位的密钥容量 C_{P} 为

$$C_{\mathrm{P}}=\mathrm{I}(\phi_1,\phi_2)=\int_0^{2\pi}\int_0^{2\pi}p_2(\phi_1,\phi_2)\cdot\mathrm{lb}\frac{p_2(\phi_1,\phi_2)}{\int_0^{2\pi}p_2(\phi_1,\phi_2)\mathrm{d}\phi_2\int_0^{2\pi}p_2(\phi_1,\phi_2)\mathrm{d}\phi_1}\mathrm{d}\phi_1\phi_2\tag{22}$$

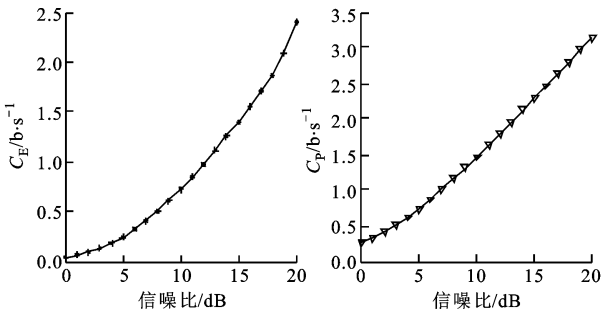
由 $p_4(A_1,\phi_1,A_2,\phi_2)$、$p_2(A_1,A_2)$ 和 $p_2(\phi_1,\phi_2)$ 的表达式可得

$$p_4(A_1,\phi_1,A_2,\phi_2)\neq p_2(A_1,A_2)p_2(\phi_1,\phi_2)\tag{23}$$

式(23)表明接收信号的包络和相位不是统计独立的随机过程，因此，从接收信号包络中生成的密钥和从接收信号相位中生成的密钥也存在一定相关性。此时，合法双方不能简单地将从包络、相位信息中生成的密钥直接拼接起来用于安全通信，而必须先去除密钥比特之间的相关性。合法双方可以通过通用 Hash 函数(Universal Hash Function)等密钥增强工具来去除两密钥比特串之间的相关性[14]，然后用于安全通信。

3 仿真与分析

图 1 给出了合法双方基于接收信号包络、相位得到的密钥容量 C_{E} 和 C_{P} 随信噪比 γ 的变化曲线。可以看出，C_{E} 和 C_{P} 均随 γ 的增大而增大。这主要是因为信噪比增大时，合法双方接收信号的相关性也随之增大，因而接收信号之间的互信息也随之增大。因此，在实际的密钥生成过程中，合法双方应当尽量降低接收端的本地噪声，从而提高接收信噪比 γ，以增大密钥容量。



(a)基于包络 (b)基于相位

图 1 基于接收信号包络和相位的密钥容量

对于所建立的模型，合法双方基于接收信号的密钥容量[2] C_{R} 为

$$C_{\mathrm{R}}=I(X;Y)=H(X)+H(Y)-H(X,Y)=\mathrm{lb}\frac{|\boldsymbol{B}_X||\boldsymbol{B}_Y|}{|\boldsymbol{B}_{XY}|}=\mathrm{lb}\frac{1+2\gamma+\gamma^2}{1+2\gamma}\tag{24}$$

从式(24)可以看出，密钥容量 C_{R} 的取值也与信噪比 γ 有关。

图 2 为合法双方基于接收信号的密钥容量和基于接收信号包络、相位的密钥容量的对比曲线。可以看出，基于接收信号的密钥容量也随信噪比的增加而逐渐增大。此外，不仅基于接收信号包络、相位信息的密钥容量均小于基于接收信号的密钥容量，其数值求和也小于基于接收信号的密钥容量，从图 2 中可以看出，当信噪比为 10 dB 时，基于接收信号包络、相位的密钥容量的数值求和比基于接收信号的密钥容量低 0.3 b/s。这意味着分别基于信道响应的包络和相位生成密钥再合成处理成最终密钥的

密钥生成方式并不能够充分挖掘信道中所包含的全部信道特性信息。因此，合法双方还可以同时利用接收信号中包含的频率、时延等信息来生成共享密钥[15]。

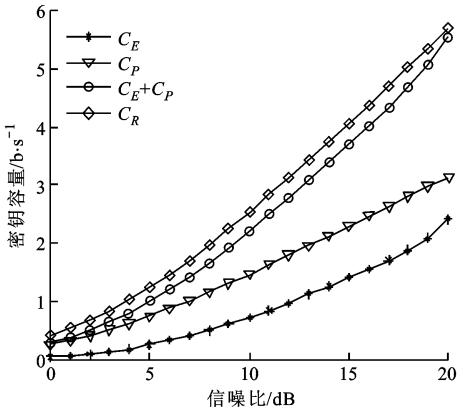


图 2　密钥容量的对比

4　密钥生成协议

密钥生成协议的基础为合法双方之间前向和后向发送的载波在相干时间内经历相同的信道变化[1,3]。

4.1　信道探测过程

每一轮的密钥生成过程都有 2 个时段，首先，Alice 向 Bob 发送 L 个持续时间为 T_1 的单位幅度且相互正交的正弦基信号

$$x_1(t)=\sum_{i=1}^{L}\exp[\mathrm{j}2\pi f_i(t-t_1)] \tag{25}$$

式中：$t\in[t_1,t_1+T_1)$；f_i 为载波频率，$1\leqslant i\leqslant L$；正弦信号的初始相位为 0。各载波之间的频率间隔大于信道的相干带宽，此时，接收端能够通过各个载波观察到相互独立的信道响应。为了叙述方便，假定 $t_1=0$，即协议开始时刻为 0。Bob 此时处于接收状态，记最短路径延时为 t_c，Alice 到 Bob 的信道响应 $h_{12}(t)$ 最终的时延扩展为 t_d。考虑信道多径丰富的情况，此时，可以认为 $h_{12}(t)$ 为复高斯随机过程，则在任意给定的时刻，$h_{12}(t)$ 的包络服从瑞利分布，相位服从均匀分布。为了使 Bob 能够很好地观察 $h_{12}(t)$ 以便于后续的包络、相位信息提取，需要满足 $T_1>t_d$。Bob 的接收信号可以表示为

$$y_{12}(t)=\sum_{i=1}^{L}a_{12,i}(t)\exp[\mathrm{j}(2\pi f_i t+\varphi_{12,i})]+\eta_{12}(t) \tag{26}$$

式中：$t\in[t_c,t_c+T_1+t_d]$；$\eta_{12}(t)$ 为 Alice 到 Bob 的信道上的加性高斯白噪声；$a_{12,i}$ 和 $\varphi_{12,i}$ 分别为信道响应 $h_{12}(t)$ 中对应于第 i 个载波的信道增益和相位。Bob 利用接收信号得到各个载波的频率、包络及相位的估计，并分别记作 $\hat{f}_{12,i}$、$\hat{a}_{12,i}$ 及 $\hat{\varphi}_{12,i}$。

Alice 经过发收转换时间 t_{TR} 后处于接收时段，Bob 经过收发转换时间 t_{RT} 后，在时刻 $t_2=t_c+t_d+T_1+t_{RT}$ 发送同样的多载波正弦基信号 $x_2(t)$，且表达式为

$$x_2(t)=\sum_{i=1}^{L}\exp[\mathrm{j}2\pi f_i(t-t_2)] \tag{27}$$

式中：$t\in[t_2,t_2+T_2]$；载波频率为 f_i，$1\leqslant i\leqslant L$；正弦信号的初始相位为 0。基于信道互易性，仍然假定最短路径延时为 t_c，Alice 观察到的信道响应 $h_{21}(t)$ 最终的时延扩展为 t_d，为了便于 Alice 进行后续的包络、相位信息提取，同样需要满足 $T_2>t_d$。Alice 的接收信号 $y_{21}(t)$ 可以表示为

$$y_{21}(t)=\sum_{i=1}^{L}a_{21,i}\exp[\mathrm{j}(2\pi f_i t+\varphi_{21,i})]+\eta_{21}(t) \tag{28}$$

式中：$t\in[t_2+t_c,t_2+t_c+T_2+t_d]$；$\eta_{21}(t)$ 为从 Bob 到 Alice 的信道上的加性高斯白噪声；$a_{21,i}$ 和 $\varphi_{21,i}$ 分别为信道响应 $h_{21}(t)$ 中对应第 i 个载波的信道增益和相位。与 Bob 类似，Alice 通过接收信号得到各个载波的频率、包络和相位的估计，并分别记作 $\hat{f}_{21,i}$、$\hat{a}_{21,i}$ 及 $\hat{\varphi}_{21,i}$。

Bob 发送完毕后进入发收转换过程，转换时间同为 t_{TR}；Alice 接收完毕后进入收发转换过程，转换时间同为 t_{RT}，至此完成一个完整的收发探测周期。

4.2　密钥生成方法

合法双方分别对接收信号包络 $\hat{a}_{12,i}$、$\hat{a}_{21,i}$（$1\leqslant i\leqslant L$）进行 M_1 比特等概量化，在 R 个探测周期之后，双方分别得到长度为 LM_1R 的比特串 $\boldsymbol{K}_{A1}$、$\boldsymbol{K}_{A2}$，然后双方对分别得到的比特串采用二分法进行信息协商[16]，得到一致的比特串 $\boldsymbol{K}_A$；双方分别对接收信号的相位估计 $\hat{\varphi}_{21,i}$、$\hat{\varphi}_{12,i}$（$1\leqslant i\leqslant L$）进行 M_2 比特等概量化，在 R 个探测周期之后，双方分别得到长度为 LM_2R 的比特串 $\boldsymbol{K}_{\varphi 1}$、$\boldsymbol{K}_{\varphi 2}$，然后双方对分别得到的比特串 $\boldsymbol{K}_{\varphi 1}$、$\boldsymbol{K}_{\varphi 2}$ 同样采用二分法进行信息协商，得到一致的比特串 $\boldsymbol{K}_\varphi$。

由文中结论可知，合法双方基于接收信号包络得到的密钥比特串 $\boldsymbol{K}_A$ 和基于接收信号相位得到的密钥比特串 $\boldsymbol{K}_\varphi$ 存在一定相关性，双方首先利用通用 Hash 函数去除 $\boldsymbol{K}_A$ 和 $\boldsymbol{K}_\varphi$ 之间的相关性，得到 $\boldsymbol{K}'_A$ 和 $\boldsymbol{K}'_\varphi$，此时双方可以将所得到的两个密钥比特串 $\boldsymbol{K}'_A$ 和 $\boldsymbol{K}'_\varphi$ 拼接起来作为最终的密钥 $\boldsymbol{K}$ 并用于安全

通信。

5 结 论

鉴于现有的实验通常是利用接收信号中包含的信道响应包络信息和相位信息生成密钥,因此在窃听方无法获得合法双方边信息的情况下,对合法双方基于接收信号包络、相位信息的密钥容量进行了推导,并进行了仿真分析,得到如下2个结论:一是合法双方基于信道响应包络信息生成的密钥和基于信道响应相位信息生成的密钥存在一定的相关性;二是信道响应中包含的包络和相位信息并不能完整地表征信道的变化情况。值得注意的是,本文是在假定合法双方信道完全互易的情况下探讨密钥容量的,信道不完全互易的情况可以通过在式(6)的信道响应 h 中引入相关系数来描述。实际可行的密钥生成方案的设计将是今后的一个研究方向;此外,所提密钥生成方案的性能及如何缩小密钥生成速率与密钥容量之间的差距值得进一步深入研究。

参考文献:

[1] HERSHEY J E, HASSAN A A, YARLAGADDA R. Unconventional cryptographic keying variable management [J]. IEEE Transactions on Communications, 1995, 43(1): 3-6.

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

[3] SMITH G S. A direct derivation of a single-antenna reciprocity relation for the time domain [J]. IEEE Transactions on Antenna and Propagation, 2004, 52(4): 1568-1577.

[4] 尚昭辉. 无线物理层密钥生成方法的研究 [D]. 西安:西安电子科技大学, 2013.

[5] LIU Y, DRAPER S C, 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.

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

[7] YE Chunxuan, MATHUR S, REZNIK A, et al. Information-theoretically secret key generation for fading wireless channels [J]. IEEE Transactions on Information Forensics and Security, 2010, 5(2): 240-254.

[8] WANG Qian, XU Kaihe, REN Kui. Cooperative secret key generation from phase estimation in narrowband fading channels [J]. IEEE Journal on Selected Areas in Communications, 2012, 30(9): 1666-1674.

[9] KHISTI A, DIGGAVI S N, WORNELL G W. Secret-key generation using correlated sources and channels [J]. IEEE Transactions on Information Theory, 2012, 58(6): 652-670.

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

[11] CSISZAR I, NARAYAN P. Secrecy generation for multiaccess channel models [J]. IEEE Transactions on Information Theory, 2013, 59(1): 17-31.

[12] ZAFER M, AGRAWAL D, SRIVATSA M. Limitations of generating a secret key using wireless fading under active adversary [J]. IEEE/ACM Transactions on Information Theory, 2012, 20(5): 1440-1451.

[13] 邹永魁, 宋立新. 信息论基础 [M]. 北京:科学出版社, 2010: 73-97.

[14] MAURER U, WOLF S. Secret key agreement over unauthenticated public channels: part III privacy amplification [J]. IEEE Transactions on Information Theory, 2003, 49(4): 839-851.

[15] 周百鹏, 黄开支, 金梁, 等. 一种基于多径相对时延的密钥生成方法 [J]. 计算机应用研究, 2011, 28(6): 2196-2198.
ZHOU Baipeng, HUANG Kaizhi, JIN Liang, et al. Scheme of key generation based on multipath relative-delay [J]. Application Research of Computers, 2011, 28(6): 2196-2198.

[16] 孙牛牛, 张水莲, 辛刚, 等. 基于LDPC码和二分法的联合信息协商算法 [J]. 信息工程大学学报, 2013, 14(2): 207-212.
SUN Niuniu, ZHANG Shuilian, XIN Gang, et al. Joint information reconciliation algorithm based on LDPC codes and BINARY [J]. Journal of Information Engineering University, 2013, 14(2): 207-212.

(编辑 刘杨)