PHY-CRAM 物理层激励响应认证机制的性能分析

张 丹 吴晓富 颜 俊 朱卫平
(南京邮电大学通信与信息工程学院 南京 210003)

摘 要 物理层认证是利用物理层资源的特性识别通信用户身份,可以有效地阻止非法用户的接入与访问,加强无线网络的信息安全性。PHY-CRAM是最近提出的一种典型的物理层激励响应认证机制,目前其性能主要依赖于仿真。尝试对其认证性能进行理论分析,推导了成功认证概率和错误接收概率的解析表达式。推导结果表明:PHY-CRAM认证准则中的相关系数服从莱斯分布,成功认证概率和错误接收概率均可用Marcum Q函数来计算。进一步的计算机仿真结果显示:相关系数的概率密度曲线与莱斯分布的概率密度曲线相吻合,且认证使用的密钥越长,吻合性越好;接收操作特性(ROC)曲线的理论值和统计值是一致的。

关键词 激励响应认证,OFDM技术,接收操作特性曲线,理论分析
中图法分类号 TN918 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2016.2.041

Performance Analysis of PHY-CRAM Physical Layer Challenge Response Authentication Mechanism

ZHANG Dan WU Xiao-fu YAN Jun ZHU Wei-ping
(College of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract The physical layer authentication recognizes the identities of communication users by exploiting the characteristics of physical layer resources, which can effectively prevent illegal users from accessing the wireless network in order to enhance the information security of wireless network. PHY-CRAM proposed recently is a typical physical layer challenge response authentication mechanism, and its performance mainly depends on the simulation. So this paper attempted to theoretically analyze the authentication performance and derived the analytical expressions of successful authentication rate and false acceptance rate. The derived results show that the correlation coefficient of PHY-CRAM authentication standards obeys Rice distribution, and successful authentication rate and false acceptance rate can be calculated by Marcum Q function. The computer simulation results show that the probability density curve of correlation coefficient is coincident with that of Rice distribution, and the longer the secret key is, the better the fitness is. The theory value of receiver operating characteristic curve is identical with the statistical value.

Keywords Challenge response authentication, OFDM technology, Receiver operating characteristic curve, Theoretical analysis

1 引言

随着无线通信的飞速发展和基于移动终端业务的不断增长,保证无线通信的安全变得越来越重要。无线链路的开放特性决定了它比传统计算机网络更容易遭受窃听、篡改、伪造等各种攻击的威胁。受无线通信安全需求的驱动,近年来,国内外一些学者对物理层安全领域十分关注[1-5],利用物理层安全认证技术加强无线通信的安全成为了信息安全领域的研究热点。

无线物理层传输技术的持续发展对利用物理层资源特性来实现身份认证的研究起到推动作用[6-14]。文献[6]提出了一种物理层认证算法,该算法利用信道探测和假设检验来判决当前的通信与之前的通信是否由同一发送终端发起。根据信道的互易特性,如果来自同一发送端的两个数据帧间的时间间隔比信道相干时间小,那么这两数据帧的信道状态信息(CSI)必定高度相关,如果CSI不相关,则数据帧就是攻击端发出的。在无线通信中信道动态变化且通信环境无法精确预测,针对这样的信道状态,文献[7]提出了一种利用时变的载波频率偏置(CFO)进行身份认证的算法,该算法通过从接收到的信号中估计出CFO值,然后利用卡尔曼滤波器跟踪过去时刻CFO的变化来预测出此刻CFO值,最后在假设检验条件下将CFO的估计值与预测值进行比较,进而实现通信终端的身份认证。基于多载波传输系统,文献[11]提出了物理层相位激励响应认证方案(PHY-PCRAS),该方案利用信道相位响应的互易性和随机性把共享密钥信息调制到子载波相位上,进行用户身份的认证,仿真证明该算法具有很好的认证性能。

到稿日期:2015-02-05 返修日期:2015-06-08 本文受国家自然科学基金项目(61372123)资助。
张 丹(1989-),女,硕士生,主要研究方向为无线物理层安全认证,E-mail:zhangdany1989@126.com;吴晓富(1975-),男,博士,教授,主要研究方向为无线物理层安全技术、编码与信息论;颜 俊(1981-),男,博士,讲师,主要研究方向为通信信号定位;朱卫平(1962-),男,博士,教授,主要研究方向为语音信号处理、通信信号处理。

文献[13]提出的 PHY-CRAM 利用无线衰落信道的互易性、随机性和位置去相关等特性，采用 OFDM 技术把高层信息和共享密钥信息分别调制到子载波的相位和幅度上，通过在通信用户间相互传送激励响应信号来实现身份认证，该算法具有高成功认证率和低错误接收率。本文对 PHY-CRAM 的认证性能进行了理论推导分析，研究了该算法认证判决准则中相关系数的分布情况，并对成功认证概率和错误接收概率的理论值进行了计算与分析。

本文第 2 节介绍了 PHY-CRAM 认证机制；第 3 节对 PHY-CRAM 进行了理论研究；第 4 节是仿真结果与分析；最后总结全文。

2 PHY-CRAM 认证机制

2.1 PHY-CRAM 的原理

PHY-CRAM 利用无线衰落信道的互易性、随机性等特点，采用 OFDM 技术把共享密钥信息调制到子载波的幅度上。该认证机制不同于加密的激励响应型认证技术，它的共享密钥是非加密的，但共享密钥被信道衰落和随机数保护。合法用户根据信道互易性特点和对信号的逆处理操作可获知共享密钥，然而由于位置差异，攻击者很难获知共享密钥信息。与传统认证算法不同的是：对于采用 PHY-CRAM 的通信系统，其安全性取决于衰落信道的随机性以及合法用户与非法用户间的相对位置，而不是计算的复杂度。

PHY-CRAM 的实现是通过在通信双方间相互发送和接收一些数据帧信息，每一帧信息包含 (K_1+K_2) 个 OFDM 符号，前 K_1 个符号是流量信息，采用差分相移键控调制(DPSK)；后 K_2 个符号是 PHY-CRAM 信息，采用幅度调制(AM)。当 $K_1=1$ 时，PHY-CRAM 的帧结构如图 1 所示。

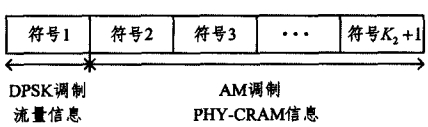


图 1 PHY-CRAM 的帧结构

PHY-CRAM 是一种主动认证机制，适用于若干个通信用户的单、双向认证，单向认证时需要一个共享密钥，双向认证时需要两个共享密钥。本文以两个合法用户和一个非法用户为通信模型描述 PHY-CRAM 认证过程。图 2 为主动认证机制模型，图 3 为通信模型，定义 Alice 和 Bob 是合法用户，Eve 为窃听用户。

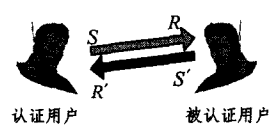


图 2 主动认证机制

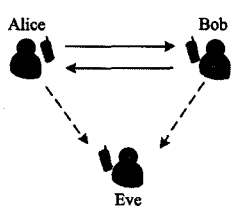


图 3 通信模型

若 Alice 和 Bob 进行互认证，则共享密钥表示为 $\{\boldsymbol{X}_A, \boldsymbol{X}_B\}$，其中 $\boldsymbol{X}_A=[X_{0,A},\cdots,X_{M-1,A}]^{\mathrm{T}}$，$X_{m,A}\in\{0,1\}$ 是第 $(m+1)$ 个比特，M 是密钥的长度，$\boldsymbol{X}_B$ 的定义与 $\boldsymbol{X}_A$ 相同；若 Alice 对 Bob 单向认证，则只需密钥 $\boldsymbol{X}_B$。图 4 是 Alice 对 Bob 的单向认证和互认证的示意图。

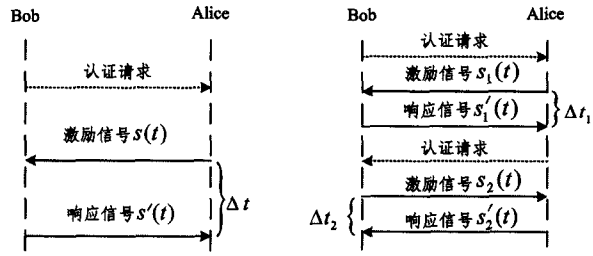


图 4 单向认证(左)和互认证(右)的示意图

PHY-CRAM 利用了信道互易性的特点，所以图 4 中的信号往返时间 Δt、Δt_1 和 Δt_2 均应小于信道的相干时间。从图 4 可看出，互认证包含两个单向认证，本质上单向认证和互认证的原理是一样的，本文就以 Alice 对 Bob 的单向认证为例来描述 PHY-CRAM 的具体实现过程。

2.2 PHY-CRAM 的实现步骤

PHY-CRAM 采用了 OFDM 技术，把 PHY-CRAM 信息调制到子载波的幅度上，则 PHY-CRAM 的详细步骤如图 5 所示。

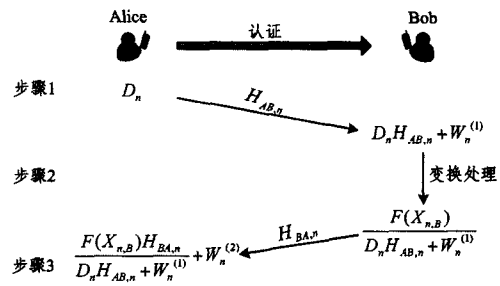


图 5 PHY-CRAM 的详细步骤

图 5 中符号及公式的含义如下。

D_n：Alice 向 Bob 发送的随机数；

$H_{AB,n}$：Alice 与 Bob 通信时第 n 个子信道的频率响应；

$H_{BA,n}$：Bob 与 Alice 通信时第 n 个子信道的频率响应；

$W_n^{(1)}$：Alice 与 Bob 通信时第 n 个子信道的加性复高斯白噪声；

$W_n^{(2)}$：Bob 与 Alice 通信时第 n 个子信道的加性复高斯白噪声；

$X_{n,B}$：Alice 和 Bob 的共享密钥信息；

$F(\cdot)$：星座映射函数；

$D_nH_{AB,n}+W_n^{(1)}$：Bob 的接收信号；

$\frac{F(X_{n,B})}{D_nH_{AB,n}+W_n^{(1)}}$：Bob 向 Alice 发送的响应信号；

$\frac{F(X_{n,B})H_{BA,n}}{D_nH_{AB,n}+W_n^{(1)}}+W_n^{(2)}$：Alice 的接收信号。

PHY-CRAM 的实现步骤如下。

步骤 1：Alice 用随机数 D_n 调制子载波的幅度，$D_n\in[K_3,K_4]$，$0<K_3<1<K_4$，K_3、K_4 的值根据 OFDM 系统子信道频域的幅值范围而定。然后把已调数据帧通过子信道传送给 Bob，该数据帧实际上等同于认证中的激励信号，随机数 D_n 用于防止攻击者探测信道。

步骤 2：Bob 接收到信号 $D_nH_{AB,n}+W_n^{(1)}$ 后，对其进行变换处理，向 Alice 发送响应信号 $\frac{F(X_{n,B})}{D_nH_{AB,n}+W_n^{(1)}}$，$F(\cdot)$ 是一个星座映射，它把二进制比特 0、1 映射为正实数，定义 $F(\cdot)$ 如下：

$$F(x)=\begin{cases}K_3, & x=0\\ K_4, & x=1\end{cases}$$

步骤 3：Alice 接收到 $\frac{F(X_{n,B})H_{BA,n}}{D_nH_{AB,n}+W_n^{(1)}}+W_n^{(2)}$ 后，根据此接收信号和共享密钥 $X_{n,B}$ 对 Bob 进行认证。

在以上整个认证过程中所用的时间必须少于信道的相干时间，由信道互易性特点则有 $H_{AB}=H_{BA}$。

3 PHY-CRAM 的理论研究

3.1 PHY-CRAM 的系统模型

本文 PHY-CRAM 的时域系统模型如图 6 所示，其中 $s(t)$ 为 Alice 发出的激励信号，$s'(t)$ 为 Bob 发出的响应信号，$r(t)$、$r'(t)$ 分别为 Bob 和 Alice 的接收信号。

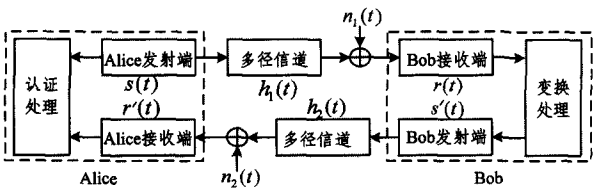


图 6 PHY-CRAM 的时域系统模型

本文基于 3GPP 标准[15]中的 Rural 信道模型建立多径信道，信道的脉冲响应记为：

$$h(t;\tau)=\sum_{l=1}^{L}h_l(t)\delta(\tau-\tau_l) \tag{1}$$

其中，$h_l(t)$、τ_l 分别为第 l 条径的信道增益和时延。信道脉冲响应基于改进的 Clarke's 模型[16]产生，第 l 条径的数学模型为：

$$h_l(t)=\sqrt{\frac{2}{M}}\{\sum_{n=1}^{M}\cos[w_dt\cos\alpha_{n,l}+\phi_{n,l}]+ j\sum_{n=1}^{M}\cos[w_dt\sin\alpha_{n,l}+\varphi_{n,l}]\} \tag{2}$$

其中 $M=\frac{N}{4}$，N 是入射波数目；$\alpha_{n,l}=\frac{2\pi n-\pi+\theta_l}{4M}(n=1,2,\cdots,M)$ 是入射波角度；$\phi_{n,l}$、$\varphi_{n,l}$ 为初始相位，$\phi_{n,l}$、$\varphi_{n,l}$ 和 θ_l 相互独立且均在 $[-\pi,\pi]$ 上服从均匀分布；$w_d=2\pi f_d$，f_d 为最大多普勒频移。无线多径信道的脉冲响应是式(2)产生的 l 条单径的叠加。

由于 PHY-CRAM 采用了 OFDM 技术，本文首先将时域的多径信道转化成频域的并行子信道，然后在频域对 PHY-CRAM 进行理论研究。对式(1)进行傅里叶变换，得到信道的频域时变冲激响应为：

$$\begin{aligned}H(t,f)&=\int_{-\infty}^{+\infty}h(t;\tau)e^{-j2\pi f\tau}d\tau\\&=\int_{-\infty}^{+\infty}\sum_{l=1}^{L}h_l(t)\delta(\tau-\tau_l)e^{-j2\pi f\tau}d\tau\\&=\sum_{l=1}^{L}h_l(t)e^{-j2\pi f\tau_l}\end{aligned} \tag{3}$$

再对式(3)在时域和频域分别以 T_s 和 $\Delta f(t=nT_s,f=k\Delta f)$ 采样得：

$$H(n,k)=\sum_{l=1}^{L}h_l(nT_s)e^{-j2\pi nk\Delta f\tau_l} \tag{4}$$

其中，T_s 表示时域上一个 OFDM 符号的长度，Δf 表示相邻子信道间的频率间隔。式(4)是第 n 个 OFDM 符号时间内第 k 个子信道的频率响应，则 OFDM 系统的等效频域系统如图 7 所示。

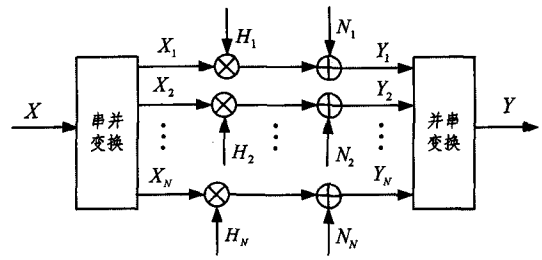


图 7 OFDM 系统的等效频域系统框图

由图 7 可知，接收信号在频域可表示为：

$$Y_k=X_kH_k+N_k,k=1,2,\cdots,N \tag{5}$$

其中，X_k、Y_k、N_k、H_k 分别表示第 k 个子信道上的发送信号、接收信号、噪声和频率响应。

3.2 PHY-CRAM 认证性能的理论分析

由 2.2 节内容知，Alice 在第 n 个子信道上的接收信号 $R_n=\frac{F(X_{n,B})H_{BA,n}}{D_nH_{AB,n}+W_n^{(1)}}+W_n^{(2)}$，则 $\boldsymbol{R}=[R_0,\cdots,R_{M-1}]^{\mathrm{T}}$，$M$ 为密钥长度。Alice 对 Bob 的认证判决准则如下：

$$\rho=\left|\frac{(\boldsymbol{R}\otimes\boldsymbol{D}-\overline{\boldsymbol{R}}_D)^H\cdot(F(\boldsymbol{X}_B)-\overline{F}(\boldsymbol{X}_B))}{\|\boldsymbol{R}\otimes\boldsymbol{D}-\overline{\boldsymbol{R}}_D\|\cdot\|F(\boldsymbol{X}_B)-\overline{F}(\boldsymbol{X}_B)\|}\right|>C_1 \tag{6}$$

其中，$\boldsymbol{D}=[D_0,\cdots,D_{M-1}]^{\mathrm{T}}$ 是 Alice 发送的随机数序列，$\boldsymbol{X}_B$ 为 Alice 和 Bob 的共享密钥，$\overline{\boldsymbol{R}}_D$ 和 $\overline{F}(\boldsymbol{X}_B)$ 分别为 $\boldsymbol{R}\otimes\boldsymbol{D}$ 和 $F(\boldsymbol{X}_B)$ 的均值。该判决准则可看作是 PN 码捕获，$C_1\in[0,1]$，如果相关系数 ρ 大于 C_1，则 Bob 认证通过；否则认证失败。

本文采用假设检验的方法研究 PHY-CRAM 的认证性能，分析相关系数 ρ 的分布情况，以及推导成功认证概率(合法用户通过认证的概率)和错误接收概率(非法用户通过认证的概率)的理论计算函数。假设检验如下：

$$\begin{aligned}&H_1:\boldsymbol{X}=\boldsymbol{X}_B\\&H_0:\boldsymbol{X}=\boldsymbol{X}_E\end{aligned} \tag{7}$$

其中，$\boldsymbol{X}$ 是被认证用户产生的密钥，$\boldsymbol{X}_B$ 和 $\boldsymbol{X}_E$ 分别为合法用户 Bob 和非法用户 Eve 产生的密钥，则有：

$$R_{H_i}=[\frac{F(X_{0,H_i})H_{BA,0}}{D_0H_{AB,0}+W_0^{(1)}}+W_0^{(2)},\cdots,\frac{F(X_{M-1,H_i})H_{BA,M-1}}{D_{M-1}H_{AB,M-1}+W_{M-1}^{(1)}}+W_{M-1}^{(2)}]^{\mathrm{T}} \tag{8}$$

$$\rho_{H_i}=\left|\frac{(\boldsymbol{R}_{H_i}\otimes\boldsymbol{D}-\overline{\boldsymbol{R}}_{H_iD})^H\cdot(F(\boldsymbol{X}_B)-\overline{F}(\boldsymbol{X}_B))}{\|\boldsymbol{R}_{H_i}\otimes\boldsymbol{D}-\overline{\boldsymbol{R}}_{H_iD}\|\cdot\|F(\boldsymbol{X}_B)-\overline{F}(\boldsymbol{X}_B)\|}\right\| \tag{9}$$

将相关系数 $\rho_{H_i}(i=0,1)$ 和阈值 C_1 进行比较，若 $\rho_{H_1}>C_1$，则为成功认证；若 $\rho_{H_0}>C_1$，则为错误接收。由于 ρ_{H_i} 是若干个复高斯变量之和的幅度值且通过直方图统计，则有 ρ_{H_1} 和 ρ_{H_0} 的概率密度函数均服从莱斯分布，记 ρ_{H_1} 和 ρ_{H_0} 的概率密度函数为：

$$f(\rho_{H_i})=\frac{\rho}{\sigma_{H_i}^2}\exp(-\frac{\rho^2+\bar{\rho}_{H_i}^2}{2\sigma_{H_i}^2})\cdot I_0(\frac{\rho\cdot\bar{\rho}_{H_i}}{\sigma_{H_i}^2}) \quad \rho\in[0,1],i=0,1 \tag{10}$$

其中 $\sigma_{H_i}^2=Var(\rho_{H_i})$，$\bar{\rho}_{H_i}=E(\rho_{H_i})$，$I_0(\cdot)$ 是改进的第一类零阶贝塞尔函数，ρ_{H_1} 和 ρ_{H_0} 的分布函数为：

$$F(\rho_{H_i})=1-Q(\frac{\bar{\rho}_{H_1}}{\sigma_{H_1}},\frac{C_1}{\sigma_{H_1}}),i=0,1 \tag{11}$$

其中，$Q(a,b)=\int_b^{+\infty}x\exp(-\frac{x^2+a^2}{2})I_0(ax)dx$，$Q(\cdot)$ 是 Marcum Q 函数。根据 $\rho_{H_i}(i=0,1)$ 的概率密度函数，则成功认证概率 β 为：

$$\beta=\int_{C_1}^{+\infty} f(\rho_{H_1})\mathrm{d}\rho$$
$$=\int_{C_1}^{+\infty}\frac{\rho}{\sigma_{H_1}^2}\exp\left(-\frac{\rho^2+\bar{\rho}_{H_1}^2}{2\sigma_{H_1}^2}\right)\cdot I_0\left(\frac{\rho\cdot\bar{\rho}_{H_1}}{\sigma_{H_1}^2}\right)\mathrm{d}\rho$$
$$=\int_{\frac{C_1}{\sigma_{H_1}}}^{+\infty}\frac{\rho}{\sigma_{H_1}}\exp\left(-\frac{(\frac{\rho}{\sigma_{H_1}})^2+(\frac{\bar{\rho}_{H_1}}{\sigma_{H_1}})^2}{2}\right)\cdot I_0\left(\frac{\bar{\rho}_{H_1}}{\sigma_{H_1}}\cdot\frac{\rho}{\sigma_{H_1}}\right)\mathrm{d}\left(\frac{\rho}{\sigma_{H_1}}\right)$$
$$=Q\left(\frac{\bar{\rho}_{H_1}}{\sigma_{H_1}},\frac{C_1}{\sigma_{H_1}}\right)\tag{12}$$

错误接收概率 α 为：

$$\alpha=\int_{C_1}^{+\infty} f(\rho_{H_0})\mathrm{d}\rho$$
$$=\int_{C_1}^{+\infty}\frac{\rho}{\sigma_{H_0}^2}\exp\left(-\frac{\rho^2+\bar{\rho}_{H_0}^2}{2\sigma_{H_0}^2}\right)\cdot I_0\left(\frac{\rho\cdot\bar{\rho}_{H_0}}{\sigma_{H_0}^2}\right)\mathrm{d}\rho$$
$$=Q\left(\frac{\bar{\rho}_{H_0}}{\sigma_{H_0}},\frac{C_1}{\sigma_{H_0}}\right)\tag{13}$$

由以上推导知，在给定阈值 C_1 的情况下，可通过 Marcum Q 函数计算出成功认证概率和错误接收概率。

4 仿真结果与分析

本文采用具有 10 径的 Rural 信道模型对理论研究结果进行仿真验证，通信系统载频 $f_c=2.4$GHz，信道带宽 $W=20$MHz，子载波间隔 $\Delta f=15$kHz，子载波个数 $N=1200$。首先给出每个子信道频响的幅度值，然后给出 PHY-CRAM 认证判决准则中相关系数 ρ 的概率密度函数曲线，最后将 PHY-CRAM 的 ROC 曲线的理论值与统计值进行对比分析。

实际无线信道的每径时延在$[0,\tau_{\max}]$内随机均匀分布，每径的功率时延谱(PDP)服从指数 $\mathrm{e}^{-\frac{\tau}{\tau_{rms}}}$ 分布，其中 $\tau_{\max}$、τ、τ_{rms} 分别为最大时延、每径的时延和时延均方根，通常情况下取 $\tau_{rms}\approx\frac{1}{4}\tau_{\max}$。每个子信道频响的幅度瞬时值如图 8 所示。

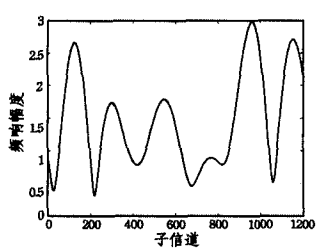
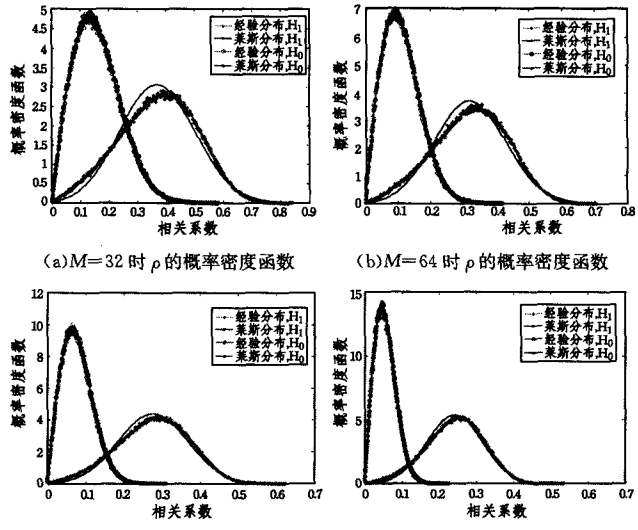


图 8 子信道的频响幅度值

由图 8 可知，子信道频响幅度值基本上在$[0.5,3]$内，所以在对 PHY-CRAM 的理论研究结果进行仿真验证时，取 $K_3=0.5$，$K_4=3$。认证准则中相关系数 ρ 的概率密度曲线如图 9 所示。

图 9 是在信噪比 $SNR=5$dB 时，密钥长度 M 分别为 32、64、128 和 256 情况下相关系数 ρ 的概率密度函数曲线。仿真结果表明：相关系数 ρ 服从莱斯分布，其概率密度函数与理论莱斯分布相吻合。比较图 9 中的 4 幅子图可以得出：在信噪比相同的情况下，密钥的长度越长，相关系数 ρ 的经验分布与理论莱斯分布吻合得越好。在相关系数 ρ 服从莱斯分布的基础上，推导出成功认证概率和错误接收概率的理论计算公式。图 10 为 PHY-CRAM 的 ROC 理论值和统计值。



(a)$M=32$ 时 ρ 的概率密度函数　(b)$M=64$ 时 ρ 的概率密度函数

(c)$M=128$ 时 ρ 的概率密度函数　(d)$M=256$ 时 ρ 的概率密度函数

图 9 不同密钥长度情况下相关系数 ρ 的概率密度函数

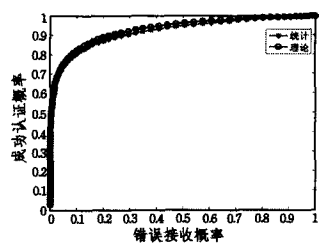


图 10 $M=64$ 时 PHY-CRAM 的 ROC 曲线

图 10 是在 $SNR=5$dB 和密钥长度 $M=64$ 情况下的 ROC 曲线。ROC 曲线对应的成功认证概率和错误接收概率的理论值均用 Marcum Q 函数计算。由图 10 得出，ROC 曲线的统计值和理论值基本上一致，存在的误差在可接受范围之内，因为在密钥长度 $M=64$ 情况下，相关系数 ρ 的经验分布与理论莱斯分布本身就存在稍微的误差，这对 ROC 曲线的统计值和理论值造成了影响。

结束语 本文针对 3GPP 中的 Rural 信道模型，采用 OFDM 技术对 PHY-CRAM 的认证性能进行了理论推导研究，并进行了仿真验证。推导及仿真结果表明：认证准则中的相关系数服从莱斯分布，其概率密度曲线与莱斯分布的概率密度曲线相吻合，且密钥越长，吻合性越好。PHY-CRAM 的成功认证概率和错误接收概率均可用 Marcum Q 函数计算，并且 ROC 曲线的理论值和统计值是一致的。

参 考 文 献

[1] Yu P L, Baras J S, Sadler B M. Physical-layer authentication[J]. IEEE Trans. Inf. Forensics Security, 2008, 3(1): 38-51

[2] Lin Tong, Huang Kai-zhi, Luo Wen-yu. A Multicarrier-based Physical Layer Security Scheme for the Multicast Systems[J]. Journal of Electronics & Information Technology, 2013, 35(6): 1338-1343(in Chinese)
林通，黄开枝，罗文宇. 一种基于多载波的多播系统物理层安全方案[J]. 电子与信息学报，2013，35(6)：1338-1343

[3] Baracca P, Laurenti N, Tomasin S. Physical layer authentication over MIMO fading wiretap channels[J]. IEEE Trans. Wireless Commun., 2012, 11(7): 2564-2573

(下转第 223 页)

National Computer Conference. 2009:499-507(in Chinese)
韩喆,陈世鸿. 跳转语句跟随域分析与程序依赖图构造算法[C]// 中国计算机大会. 2009:499-507

[5] Weiser M D. Program slices: formal, psychological, and practical investigations of an automatic program abstraction method[D]. Ann Arbor, MI: University of Michigan, 1979

[6] Shan Yong-ming. An automatic method for generation control flow graph from source program[J]. Journal of Chinese Computer Systems, 1996, 17(10): 45-49(in Chinese)
单永明. 一种源程序到控制流图的自动生成方法[J]. 小型微型计算机系统, 1996, 17(10): 45-49

[7] Wang Wen-yong, Wang Xue-dong, Xiang Yu, et al. Research on automatic construction of program flow graph for assembley embedded software[J]. Computer Science, 2005, 32(2): 173-175(in Chinese)
汪文勇, 王学东, 向渝, 等. 汇编嵌入式软件程序流程图自动生成的研究[J]. 计算机科学, 2005, 32(2): 173-175

[8] Mou Zhan-sheng, Zhang Hong-jun, Hu Li-fang. Research and Realization on the Automatic-converting Algorithm from Source Program to Flowchart[J]. Computer Development & Applications, 2008, 21(7): 28-30(in Chinese)
牟占生, 张红军, 胡丽芳. 源程序到流程图自动转换算法的研究与实现[J]. 电脑开发与应用, 2008, 21(7): 28-30

[9] Song Y, Peng X, Xing Z, et al. Automatic adaptation of software applications to database evolution by graph differencing and AOP-based dynamic patching[C] // 2012 IEEE 36th Annual Computer Software and Applications Conference (COMPSAC). IEEE, 2012: 111-118

[10] Ottenstein K J, Ottenstein L M. The program dependence graph in a software development environment[J]. ACM Sigplan Notices, 1984, 19(5): 177-184

[11] Ambler S W, Sadalage P J. Refactoring databases: Evolutionary database design[M]. Pearson Education, 2006

[12] Maule A, Emmerich W, Rosenblum D S. Impact analysis of database schema changes[C]// Proceedings of the 30th international conference on Software engineering. ACM, 2008: 451-460

[13] Curino C A, Moon H J, Zaniolo C. Graceful database schema evolution: the prism workbench[J]. Proceedings of the VLDB Endowment, 2008, 1(1): 761-772

[14] Curino C A, Moon H J, Ham M, et al. The PRISM Workwench: Database Schema Evolution without Tears[C]// IEEE 25th International Conference on Data Engineering, 2009 (ICDE'09). IEEE, 2009: 1523-1526

[15] Curino C, Moon H J, Zaniolo C. Automating Database Schema Evolution in Information System Upgrades[C]// Proceedings of International Workshop on Hot Topics in Software Upgrades. 2009: 1-5

[16] Curino C, Moon H J, Deutsch A, et al. Automating the database schema evolution process[J]. The VLDB Journal, 2013, 22(1): 73-98

[17] Gobert M, Maes J, Cleve A, et al. Understanding Schema Evolution as a Basis for Database Reengineering[C]// 2013 29th IEEE International Conference on Software Maintenance (ICSM). 2013: 472-475

[18] Chytil M, Polák M, Nečcaský M, et al. Evolution of a Relational Schema and Its Impact on SQL Queries[J]. Studies in Computational Intelligence, 2014, 511(2): 5-15

[19] Cleve A, Gobert M, Meurice L, et al. Understanding database schema evolution: A case study[J]. Science of Computer Programming, 2015, 97: 113-121

(上接第 191 页)

[4] Li Wei, Chen Bin, Wei Ji-bo, et al. Secure Communications via Sending Artifical Noise by the Receiver: Ergodic Secure Region Analysis[J]. Journal of Signal Processing, 2012, 28(9): 1314-1320(in Chinese)
李为, 陈彬, 魏急波, 等. 基于接收机人工噪声的物理层安全技术及保密区域分析[J]. 信号处理, 2012, 28(9): 1314-1320

[5] Li Xiang-yu, Jin Liang, Huang Kai-zhi, et al. A Physical Layer Security Transmission Mechanism of Relay System Based on Joint Channel Characteristics[J]. Chinese Journal of Computers, 2012, 35(7): 1439-1406(in Chinese)
李翔宇, 金梁, 黄开枝, 等. 基于联合信道特征的中继物理层安全传输机制[J]. 计算机学报, 2012, 35(7): 1439-1406

[6] Xiao L, Greenstein L, Mandayam N, et al. Using the physical layer for wireless authentication in time-variant channels[J]. IEEE Trans. Wireless Commun., 2008, 7(7): 2571-2579

[7] Hou Wei-kun, Wang Xian-bin, Jean Y C, et al. Physical layer authentication for mobile systems with time-varying carrier frequency offsets[J]. IEEE Trans. Commun., 2014, 62(5): 1658-1667

[8] Dai Qiao, Song Hua-wei, Jin Liang, et al. Physical-layer Authentication and Key Distribution Mechanism Based on Equivalent Channel[J]. Science China, 2014, 44(12): 1580-1592(in Chinese)
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, 2014, 44(12): 1580-1592

[9] Zeng K, Govindan K, Mohapatra P. Non-cryptographic authentication and identification in wireless networks[J]. IEEE Trans. Wireless Commun., 2010, 17(5): 56-62

[10] Liu Y, Ning P. Enhanced wireless channel authentication using time-synched link signature, 2012 [C] // IEEE International Conference on Computer Communications (INFOCOM'12). Orlando, FL, 2012: 2636-2640

[11] Wu Xiao-fu, Yang Zhen. Physical-layer authentication for multicarrier transmission[J]. IEEE Commun. Lett., 2014, 19(1): 74-77

[12] Ma Ting, Ren Meng-yin, Wen Hong, et al. Bi-Directional Physical Layer-Assist Authentication in Smart-Meter System[J]. China Information Security, 2014(11): 85-87(in Chinese)
马婷, 任梦吟, 文红, 等. 智能电表系统中的双向物理层辅助认证技术[J]. 信息安全与通信保密, 2014(11): 85-87

[13] Shan Dan, Zeng Kai, Xiang Wei-dong, et al. PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks[J]. IEEE J. Sel. Areas Commun., 2013, 31(9): 1817-1827

[14] Tugnait J K. Wireless user authentication via comparison of power spectral densities[J]. IEEE J. Sel. Areas Commun., 2013, 31(9): 1791-1802

[15] 3GPP. Technical specification group radio access networks-deployment aspects: TR25. 943[R]. 2009

[16] Yahong R. Improved Models for the Generation of Multiple Uncorrelated Rayleigh Fading Waveforms[J]. IEEE Commun. Lett., 2002, 6(6): 256-258