

物理层认证 PHY-PCRAS 应用于 OFDM 传输的性能分析

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, 江苏 南京 210003)

摘 要:物理层认证是在无线物理层对通信用户身份的识别,与网络上层安全协议相结合进一步加强无线网络的安全性。文中基于物理层相位激励-响应认证方案(PHY-PCRAS),研究无线正交频分复用(OFDM)传输系统中,子信道频域相关性对认证性能的影响。针对 3GPP 标准中的典型 Urban 信道模型,采用随机时延推导 OFDM 子信道频域的相关性,并进行了仿真验证。仿真结果表明,子信道频域的相关性随着子信道间距的增大呈指数趋势减小,且相关性越小,PHY-PCRAS 认证性能越好。文中还将 PHY-PCRAS 和另一种激励响应型物理层认证机制(PHY-CRAM)进行了对比,结果表明:即使子信道相关,PHY-PCRAS 仍然接近理想的效果,比 PHY-CRAM 算法具有更好的认证性能。

关键词:激励-响应认证;OFDM 技术;频域相关性;认证性能分析

中图分类号:TN918

文献标识码:A

文章编号:1673-629X(2016)01-0137-05

doi:10.3969/j.issn.1673-629X.2016.01.029

Performance Analysis of Physical Layer Challenge-response Authentication with OFDM Transmission

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 in the wireless physical layer, and it combines the network upper security protocols to further strengthen the security of wireless networks. Based on physical layer challenge-response authentication scheme (PHY-PCRAS), the influence of sub-channels frequency domain correlation with wireless OFDM transmission on the authentication performance was studied. For the 3GPP typical Urban channel model, the random delay was adopted to deduce the correlation of OFDM frequency domain sub-channels, and verified it through the simulation. The simulation results show that the frequency domain sub-channels correlation decreases exponentially with the increasing of sub-channel space, and the smaller the correlation is, the better the authentication performance of PHY-PCRAS is. Compared PHY-PCRAS with another physical layer challenge-response authentication mechanism (PHY-CRAM), the simulation results show that even if sub-channels are related, PHY-PCRAS is still close to the ideal performance, better than the PHY-CRAM algorithm.

Key words: challenge-response authentication; OFDM technology; frequency domain correlation; authentication performance analysis

0 引言

随着无线通信的飞速发展和基于移动终端业务的增长,保证无线通信的安全变得越来越重要。由于无线通信链路的开放性为非法用户攻击提供了一些新的入侵途径,使通信系统存在很大的安全隐患,这使得对通信用户身份的认证变得尤为重要。

近年来,国内外一些学者对无线物理层安全认证颇为关注,许多物理层认证算法都是利用无线物理层资源的特性实现的^[1-12]。文献[1]首次利用信道短时互易性的特点实现信息安全传输;文献[9]中的认证算法是通过两个接收信号的频谱分析,采用假设检验的方法对其功率谱密度是否一致进行认证;文献

收稿日期:2015-04-18

修回日期:2015-07-22

网络出版时间:2016-01-04

基金项目:国家自然科学基金资助项目(61372123)

作者简介:张 丹(1989-),女,硕士生,研究方向为无线物理层安全认证;吴晓富,博士,教授,研究方向为无线物理层安全技术、编码与信息论;颜 俊,博士,讲师,研究方向为通信信号定位;朱卫平,博士,教授,研究方向为语音信号处理、通信信号处理。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20160104.1510.054.html>

[10]提出的 PHY-CRAM 适合通信用户的单、双向认证,它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幅度上(AM 调制),通过在通信用户间相互传送激励-响应信号实现身份认证,该算法具有高的成功认证率和低的错误接收率。文献[12]提出的 PHY-PCRAS 与 PHY-CRAM 算法的不同之处在于:

(1)利用多载波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(BPSK 调制);

(2)采用假设检验实现通信用户身份认证。

和信道的幅度响应相比,信道的相位响应对发送端和接收端之间的距离更敏感,因此 PHY-PCRAS 比 PHY-CRAM 的认证性能好,仿真结果也表明 PHY-PCRAS 的接收操作特性(ROC)曲线性能更好,所以文中采用 PHY-PCRAS 进行研究。PHY-PCRAS 在文献[12]中的子载波信道是并行且相互独立的,由于无线通信中的实际信道是时变的多径时延信道,在 OFDM 系统中子信道频响具有相关性,文中旨在研究实际应用中子信道频域相关性对 PHY-PCRAS 认证性能的影响。

1 PHY-PCRAS 算法介绍

1.1 PHY-PCRAS 的模型

PHY-PCRAS 算法是基于多载波传输,利用信道相位响应的随机性和互易性实现认证。该算法适合若干个通信用户的单、双向认证,单、双向认证的原理是一样的,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。文中通信模型中定义 Alice 和 Bob 是两个合法用户,Eve 为窃听用户。当 Alice 和 Bob 进行通信时,保障信息安全需要实现两者间的互认证,认证过程用到共享密钥 $\{K_A, K_B\}$ 。信息安全依赖密钥的可靠性,如果窃听者 Eve 知道 K_A 、 K_B ,那么他会伪装成 Alice 或者 Bob 对系统安全造成威胁。图 1 为互

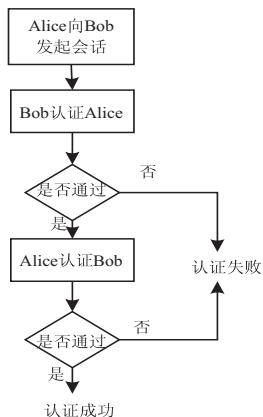


图 1 PHY-PCRAS 互认证的流程图

认证的流程图。

1.2 PHY-PCRAS 的具体步骤

PHY-PCRAS 利用相位响应特性把发送信号调制到 M 个并行独立的子信道相位上,由于单向认证和互认证的原理一样,文中就以 Alice 对 Bob 认证为例,描述 PHY-PCRAS 的单向认证过程。原理如图 2 所示。

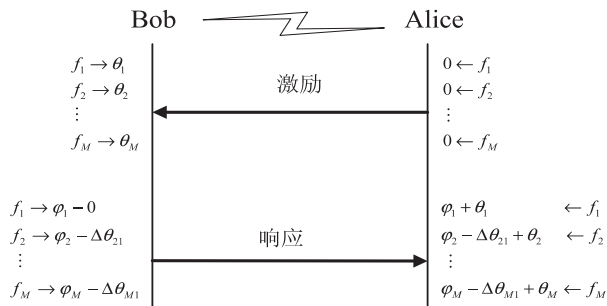


图 2 PHY-PCRAS 单向认证的原理图

PHY-PCRAS 的实现步骤如下:

(1) Alice 向 Bob 发送激励信号。Alice 在子载波频率 f_1, f_2, \dots, f_M 处向 Bob 发送等相位调制的正弦波作为激励信号,在 M 个并行独立的子信道上传输, Bob 接收到的信号包含每个子信道的相位信息 θ_i , Bob 估测出子载波 f_i 和 f_1 间的相位差 $\Delta\theta_{i1}$ ($i = 1, 2, \dots, M$)。

(2) Bob 向 Alice 反馈响应信号。Bob 根据接收到的激励信号和子载波间的相位差 $\Delta\theta_{i1}$, 反馈给 Alice 一个封装有共享密钥 $K_B = [k_1, k_2, \dots, k_M]^T$ 的响应信号。

(3) 认证。Alice 接收到响应信号后,采用假设检验认证对方的身份,假设检验条件如下所示:

$$H_1: K_i = K_B$$

$$H_0: K_i = K_E$$

令 $\eta = K_B^T y$, $\zeta = |\eta|$, y 为 Alice 的接收信号, K_B 为 Alice 和 Bob 的共享密钥,通过比较 ζ 和阈值 τ 的大小判决对方是否为合法用户。

(4) 阈值 τ 的选择和认证准则。在步骤(3)的假设检验条件下,先根据 $\eta|H_0$ 的分布和错误接收概率 α 确定阈值 τ ,再根据包络 ζ 的概率密度函数进行认证判决,若 $\zeta \geq \tau$ 则为合法用户,否则为非法用户。

2 信道模型建立及 OFDM 系统中子信道频域相关性研究

2.1 信道模型

文中采用 3GPP 标准^[13]中的典型 Urban 信道作为无线信道模型,它是一个时变多径时延信道,信道的脉冲响应记为:

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

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^[14]产生,第 l 条径的数学模型为:

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

其中, $M = \frac{N}{4}$, N 是入射波数目; $\alpha_{n,l} =$

$\frac{2\pi n - \pi + \theta_l}{4M}$ ($n = 1, 2, \dots, M$) 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。

无线信道脉冲响应是公式(2)产生的 l 条单径的叠加。

2.2 OFDM 系统中子信道频域相关性研究

OFDM 系统是把整个信道划分成若干个相互正交的子信道,相邻子载波在频谱上相互重叠,大大提高了信道频谱利用率,并且每个子信道的带宽远远小于信道的相干带宽,能有效对抗多径效应,消除符号间干扰(ISI),适合应用于存在多径信道和多普勒频移的无线信道中。

$$\begin{aligned} \rho_{\Delta k} &= \left| \frac{E[H(n,k)H^*(n,k+\Delta k)] - E[H(n,k)] \cdot E[H(n,k+\Delta k)]}{\sqrt{D[H(n,k)]} \cdot \sqrt{D[H(n,k+\Delta k)]}} \right| = \\ &= \left| \frac{E\left[\sum_{l=1}^L \|h_l(nT_s)\|^2 e^{j2\pi\Delta f \cdot \Delta k \cdot \tau_l}\right]}{E\left[\sum_{l=1}^L \|h_l(nT_s)\|^2\right]} \right| = \left| \frac{E\sum_{l=1}^L \sigma_l^2 e^{j2\pi\Delta f \cdot \Delta k \cdot \tau_l}}{E\sum_{l=1}^L \sigma_l^2} \right| = \\ &= \frac{4}{e^4 - 1} \left| \frac{e^4 - e^{j2\pi \cdot \Delta f \cdot \Delta k \cdot \tau_{\max}}}{4 - j2\pi \cdot \Delta f \cdot \Delta k \cdot \tau_{\max}} \right| = \frac{2}{e^4 - 1} \sqrt{\frac{1 + e^8 - 2e^4 \cos(2\pi \cdot \Delta f \cdot \Delta k \cdot \tau_{\max})}{4 + (\pi \cdot \Delta f \cdot \Delta k \cdot \tau_{\max})^2}} \quad (6) \end{aligned}$$

由于多径信道中每条径是相互独立且每径的信道增益均服从标准正态分布,即 $E[h_l(nT_s)] = 0$, $D[h_l(nT_s)] = 1$ 。

所以当 $l \neq i$ 时有:

$$E[h_l(nT_s)h_i^*(nT_s)] = E[h_l(nT_s)] \cdot E[h_i^*(nT_s)] = 0 \quad (7)$$

$$\begin{aligned} E[H(n,k)] \cdot E[H(n,k+\Delta k)] &= \\ E\left[\sum_{l=1}^L h_l(nT_s)e^{-j2\pi k \Delta f \tau_l}\right] \cdot \\ E\left[\sum_{i=1}^L h_i(nT_s)e^{-j2\pi(k+\Delta k) \Delta f \tau_i}\right] &= 0 \quad (8) \end{aligned}$$

式中, L 为路径数; σ_l^2 为第 l 条径的功率; Δf 为相邻两个子信道间的频率间隔; τ_l 为第 l 条径的时延; τ_{\max} 为多径信道的最大时延; Δk 为子信道的间隔数目 (Δk 为整数),由式(6)知在给定信道模型参数和不考虑时间维的情况下,子信道频域相关性的大小只与 Δk 有关。

由 2.1 节知无线信道的脉冲响应为式(1),对其进行傅里叶变换得到信道的频域时变冲激响应为:

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

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

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

其中, T_s 表示时域上一个 OFDM 符号的长度; Δf 表示频域上子信道间的间隔。

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 系统的等效频域信号模型如下:

$$Y_k = X_k H_k + N_k, k = 1, 2, \dots, N \quad (5)$$

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

文中研究子信道频响 $H(n,k)$ 和 $H(n,k+\Delta k)$ ($\Delta k = 0, 1, \dots, N-1$) 的相关性大小(不考虑时间维),定义相关系数 $\rho_{\Delta k}$ 为:

3 仿真结果与分析

文中采用具有 20 径的典型 Urban 信道进行仿真验证,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 $N = 1200$ 。首先给出子信道频域的相关性大小与 Δk 的关系图,然后给出 PHY-PCRAS 算法在具有相关性的 OFDM 系统中 $\zeta|H_1$ 和 $\zeta|H_0$ 的概率密度函数曲线图,最后给出在相关性存在的情况下,PHY-PCRAS 算法和 PHY-CRAM 算法的 ROC 曲线并作对比分析。

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 $e^{-\frac{\tau}{\tau_{\text{rms}}}}$ 分布,其中 τ_{\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 $\tau_{\text{rms}} \approx \frac{1}{4} \tau_{\max}$ 。子信道频域相关系数的理论值和统计值如图 3 所示。

Urban 信道的最大时延 $\tau_{\max} = 2\ 140\ \text{ns}$, 信道的相干带宽 $B_c = \frac{1}{\tau_{\max}} = 467\ \text{kHz}$, 由于相邻子信道间隔 $\Delta f = 15\ \text{kHz}$, $\frac{B_c}{\Delta f} = \frac{467\ \text{k}}{15\ \text{k}} \approx 31$, 所以当 Δk 在 $[0, 31]$ 范围内, 子信道频域响应具有强相关性。图 3 表明 OFDM 系统中子信道频域的相关性随着子信道间隔的增大呈指数趋势减小, 且当 $\Delta k \in [0, 31]$ 时, 相关系数 $\rho \in [0.62, 1]$, 子信道频域响应是强相关的, 仿真结果与理论一致。接着文中分析子信道的相关性对 PHY-PCRAS 算法认证性能的影响, 通过 Monte-Carlo 仿真给出了在假设检验 H_0 和 H_1 下包络的概率密度函数 (见图 4 和图 5)。

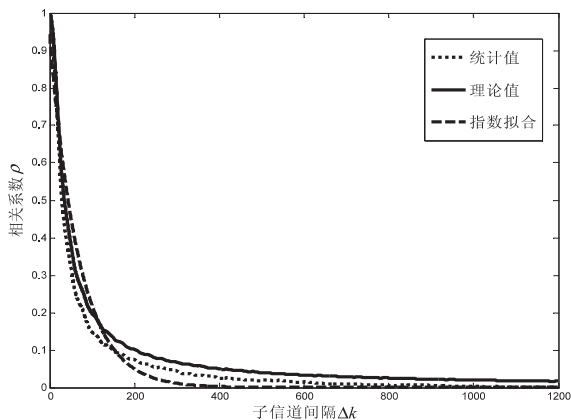


图 3 相关系数 ρ 与 Δk 的关系图

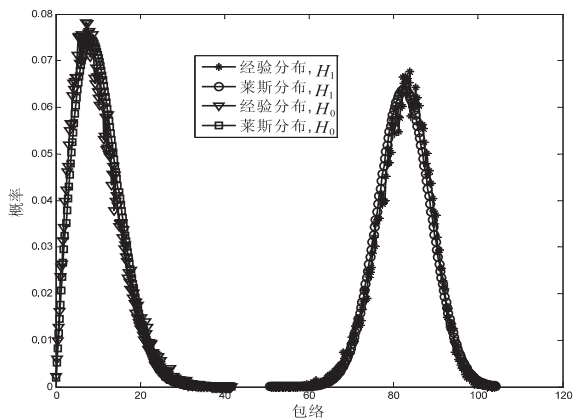


图 4 PHY-PCRAS 算法在相关子信道中的包络概率密度函数 (在 1 200 个子信道中连续取 100 个子信道)

图 4 和图 5 表明: 即使子信道相关, 在信噪比 $\text{SNR} = 5\ \text{dB}$ 时, 经验分布与理论莱斯分布也相吻合, 并且 $\zeta | H_0$ 和 $\zeta | H_1$ 的概率密度函数是分开的, 由算法原理知在给定错误接收概率的情况下, 很容易确定用于认证判决的阈值 τ 。比较图 4 和图 5 得出: 等间隔选取子信道时的认证性能比连续选取子信道时好, 说明子信道频域的相关性越低, PHY-PCRAS 的认证性能越好。事实上, PHY-PCRAS 用在 OFDM 传输系统中时, PHY

-PCRAS 的性能依赖于子信道的相关性, 所以子信道的选取很重要。比如可以根据时间-频率二维信息, 选取合适的子信道使其相关性最小, 以便达到更好的认证性能。

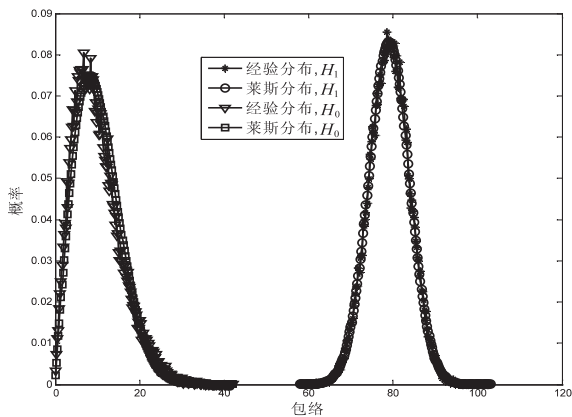


图 5 PHY-PCRAS 算法在相关子信道中的包络概率密度函数 (在 1 200 个子信道中等间隔取 100 个子信道)

PHY-CRAM 是激励响应型物理层认证的另一种算法, 该算法简单, 复杂度低。图 6 是子信道相关情况下 PHY-PCRAS 和 PHY-CRAM 的 ROC 曲线, 并将两者的认证性能进行对比分析。

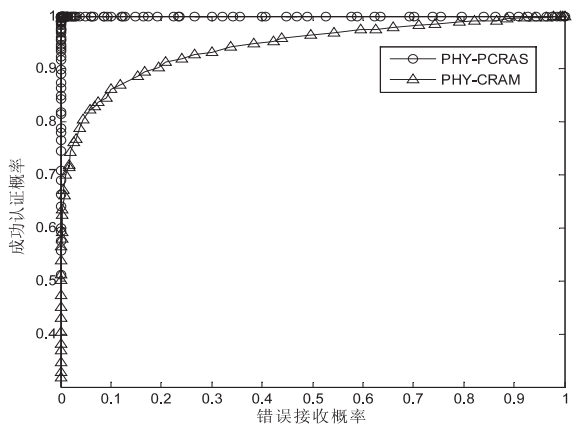


图 6 PHY-PCRAS 和 PHY-CRAM 的 ROC 曲线

图 6 表明: 通过设置合适的阈值 τ , PHY-PCRAS 算法的 ROC 曲线接近于理想情况。由于 PHY-PCRAS 算法是基于信道相位响应的, 而 PHY-CRAM 是基于信道幅度响应的, 相位响应对通信用户间的距离更敏感, 因此 PHY-PCRAS 的认证性能比 PHY-CRAM 好, 更适用于无线物理层认证。

4 结束语

文中针对 3GPP 中的典型 Urban 信道模型, 研究了无线通信 OFDM 系统中子信道频域的相关性, 得出随着子信道间距的增大, 子信道频域的相关性呈指数趋势递减。并对 PHY-PCRAS 在相关子信道下的认证性能进行了仿真, 通过仿真分析得出相关性越小其认证

性能越好。将 PHY-PCRAS 与 PHY-CRAM 的 ROC 曲线对比还可得出:即使在子信道相关的条件下,PHY-PCRAS 仍然具有很好的认证性能。

参考文献:

[1] Koorapaty H, Hassan A, Chennakeshu S. Secure information transmission for mobile radio[J]. IEEE Communication Letters, 2000, 4(2): 52-55.

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

[3] 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.

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

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

[6] 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): 1399-1406.

(上接第 136 页)

飞行小团队协作能力进行评价。通过对协作能力的测评, 组建一个高效的飞行团队, 对于提高工作效率和安全性具有非常重要的意义。

参考文献:

[1] Horowitz S K, Horowitz I B. The effects of team diversity on team outcomes: a meta-analytic review of team demography [J]. Journal of Management, 2007, 33(6): 987-1015.

[2] de Church L A, Mesmer-Magnus J R. The cognitive underpinnings of effective teamwork: a meta-analysis [J]. Journal of Applied Psychology, 2010, 95(1): 32-53.

[3] Marks M A, Mathieu J E, Zaccaro S J. A temporally based framework and taxonomy of team processes [J]. Academy of Management Review, 2001, 26(3): 356-376.

[4] Kozlowski S W J, Bell B S. Work groups and teams in organizations [J]. Handbook of Psychology: Industrial and Organizational Psychology, 2003, 12: 333-375.

[5] Levine J M, Moreland R L. Progress in small group research [J]. Annual Review of Psychology, 1990, 41: 585-634.

[7] Liu Yao, Ning Peng. Enhanced wireless channel authentication using time - synched link signature [C]//Proceedings of IEEE. Orlando, FL: IEEE, 2012: 2636-2640.

[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.

[9] Tugnait J K. Wireless user authentication via comparison of power spectral densities [J]. IEEE Journal of Selected Areas in Communication, 2013, 31(9): 1791-1802.

[10] Shan D, Zeng K, Xiang W, et al. PHY-CRAM: physical layer challenge-response authentication mechanism for wireless networks [J]. IEEE Journal of Selected Areas in Communication, 2013, 31(9): 1817-1827.

[11] 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.

[12] Wu Xiaofu, Yang Zhen. Physical-layer authentication for multi-carrier transmission [J]. IEEE Communication Letters, 2014, 19(1): 74-77.

[13] 3GPP. Tr 25. 943: technical specification group radio access networks-deployment aspects [S]. 2009.

[14] Yahong R. Improved models for the generation of multiple uncorrelated rayleigh fading waveforms [J]. IEEE Communication Letters, 2002, 6(6): 256-258.

[6] Bell S T. Deep-level composition variables as predictors of team performance: a meta-analysis [J]. Journal of Applied Psychology, 2007, 92: 595-615.

[7] 惠铎铎, 胡文东, 李晓京, 等. 心理运动能力测试软件的开发与应用[J]. 计算机技术与发展, 2014, 24(4): 155-157.

[8] 惠铎铎, 李晓京, 文治洪, 等. 心理运动能力测评系统的开发应用[J]. 计算机技术与发展, 2014, 24(12): 180-182.

[9] 任 婧, 王二平. 团队作业结构的分类及其特征研究[J]. 管理学报, 2011, 8(8): 1169-1173.

[10] 常 涛, 廖建桥. 国外团队有效性研究新进展述评[J]. 科学学与科学技术管理, 2007, 28(9): 163-169.

[11] 刘 宁, 张 爽. 团队效能经典模型评述[J]. 南京邮电大学学报: 社会科学版, 2010, 12(4): 1-6.

[12] 武 欣, 吴志明. 国外团队有效性影响因素研究现状及发展趋势[J]. 外国经济与管理, 2005, 27(1): 47-50.


[13] 郑日昌, 蔡永红, 周益群. 心理测量学 [M]. 北京: 人民教育出版社, 2007.

[14] 高翠翠, 朱丽娟, 李春燕. 中国民航飞行员心理选拔存在问题及改进措施[J]. 考试周刊, 2009(11): 238-239.

物理层认证 PHY-PCRAS 应用于 OFDM传输的性能分析

作者：[张丹](#)，[吴晓富](#)，[颜俊](#)，[朱卫平](#)，[ZHANG Dan](#)，[WU Xiao-fu](#)，[YAN Jun](#)，[ZHU Wei-ping](#)

作者单位：[南京邮电大学 通信与信息工程学院](#)，[江苏 南京](#)，[210003](#)

刊名：[计算机技术与发展](#)

英文刊名：

年，卷(期)：2015(1)

引用本文格式：[张丹](#)，[吴晓富](#)，[颜俊](#)，[朱卫平](#)，[ZHANG Dan](#)，[WU Xiao-fu](#)，[YAN Jun](#)，[ZHU Wei-ping](#) [物理层认证 PHY-PCRAS 应用于 OFDM传输的性能分析](#)[期刊论文]-[计算机技术与发展](#) 2015(1)