物理层认证的中间人导频攻击分析

王少禹 黄开枝* 许晓明 马克明 陈亚军
(战略支援部队信息工程大学 郑州 450001)

摘 要：现有物理层认证机制依赖合法信道状态信息(CSI)的私有性，一旦攻击者能够操控或窃取合法信道，物理层认证机制就会面临被攻破的威胁。针对上述缺陷，该文提出一种中间人导频攻击方法(MITM)，通过控制合法双方的信道测量过程对物理层认证机制进行攻击。首先对中间人导频攻击系统进行建模，并给出一种中间人导频攻击的渐进无感接入策略，该策略允许攻击者能够顺利接入合法通信双方；在攻击者顺利接入后，可对两种基本的物理层认证机制发起攻击：针对基于CSI的比较认证机制，可以实施拒绝服务攻击和仿冒接入攻击；针对基于CSI的加密认证机制，可以实现对信道信息的窃取，从而进一步破解认证向量。该攻击方法适用于一般的公开导频无线通信系统，要求攻击者能够对合法双方的导频发送过程进行同步。仿真分析验证了渐进无感接入策略、拒绝服务攻击、仿冒接入攻击、窃取信道信息并破解认证向量等多种攻击方式的有效性。

关键词：物理层认证；中间人导频攻击；认证攻击
中图分类号：TN911.4; TN915.08 **文献标识码**：A **文章编号**：1009-5896(2021)11-3141-08
DOI: 10.11999/JEIT200831

Man-in-the-middle Pilot Attack for Physical Layer Authentication

WANG Shaoyu HUANG Kaizhi XU Xiaoming MA Keming CHEN Yajun
(*Information Engineering University*, *Zhengzhou* 450001, *China*)

Abstract: The existing physical layer authentication mechanism relies on the privacy of the legitimate channel. Once the attacker can manipulate or obtain legitimate channel information, the physical layer authentication mechanism will face the threat of being compromised. To overcome the above-mentioned shortcomings, a Man-In-The-Middle (MITM) pilot attack method is proposed, which attacks the physical layer authentication mechanism by controlling the channel measurement process of the legitimate parties. Firstly, the man-in-the-middle pilot attack system is modeled, and a progressive and non-sense access strategy for MITM pilot attack is given. This strategy allows the attacker to access smoothly legitimate communication. After the attacker accesses successfully, he can launch attacks on two basic physical layer authentication mechanisms: For CSI-based comparative authentication mechanisms, denial of service attacks and counterfeit access attacks can be implemented; For the CSI-based encryption authentication mechanism, the channel information can be stolen, thereby further cracking the authentication vector. This attack method is suitable for general public pilot wireless communication systems, and requires the attacker to be able to synchronize the pilot sending process of the legitimate two parties. Simulation analysis verifies the effectiveness of multiple attack methods such as the progressive and non-sense access strategy, denial of service attack, counterfeit access attack, or cracking authentication vector.

Key words: Physical layer authentication; Man-In-The-Middle (MITM) pilot attack; Authentication attack

1 引言

随着5G和移动互联时代的到来以及泄密事件的层出不穷，无线通信的安全问题得到越来越多的重视。而认证是无线节点之间安全通信的第1道屏障，用于确认节点身份或消息来源的合法性，是无线通信安全体系的“门卫”。除基于高层密码体制的认证方法外，近年来逐渐兴起基于物理层的认证方法研究。物理层认证利用无线信道的时变性、空间不相关性和唯一性实现无线节点的身份或消息认证[1]，具有开销低、轻量级、安全内生等特点，因而得到越来越多的研究。物理层认证包含基于射频指纹的认证和基于信道状态信息(Channel State

收稿日期：2020-09-25；改回日期：2021-10-15；网络出版：2021-10-20
*通信作者： 黄开枝 2694183974@qq.com
基金项目：国家自然科学基金(61701538, 61871404, 61521003)
Foundation Items: The National Natural Science Foundation of China (61701538, 61871404, 61521003)

Information, CSI)的认证，本文所涉及的物理层认证仅指代基于CSI的认证。物理层认证可大致分为两种基本机制，一种是基于信道状态信息的比较认证机制(CSI-based Comparative Authentication mechanisms)，基本原理是将CSI作为认证可信根，通过比较当前消息的CSI和上一消息的CSI，确认当前消息来源的合法性。另一种是基于CSI的加密认证机制(CSI-based Encryption Authentication mechanisms)，基本原理是发送端通过CSI对信号进行加密，对端通过具有互易性的CSI对信号进行解密，从而完成认证过程。文献[2–4]首先从移动环境、时变环境、MIMO系统等多个场景对比较认证机制进行了丰富的研究，并进行了实验验证。文献[5]中提出的挑战-响应机制和文献[6–8]中提出的物理层-高层融合认证机制是加密认证机制中的代表，在比较认证的思路之外，创新了物理层认证的应用方式。

然而，物理层认证依赖于CSI的私有性，即攻击者无法得知当前合法通信双方的CSI。一旦攻击者通过某种手段控制合法通信双方的信道测量，物理层认证就面临被攻破的风险。人们熟知的导频污染攻击就可以看作一种信道测量控制手段，文献[9]在合法通信双方的信道估计过程中发送相同的导频信号，使得合法方估计的信道部分来源于攻击信道，从而使攻击者获取合法链路CSI的部分信息。文献[10]研究了中间人主动攻击下的物理层密钥生成，并定量分析了对物理层密钥生成带来的负面影响。目前，还没有人研究过针对物理层认证的主动攻击，事实上，假如攻击者获得了合法信道的部分或全部信息，就可以对物理层认证发起攻击，这是由物理层安全的内在属性决定的，即依赖于无线信道的私有性。

针对物理层认证中的安全缺陷，本文提出了一种中间人导频攻击方法(MITM)，并基于该攻击方法进行了攻击分析和仿真验证。本文首先总结了物理层认证的两种基本机制，阐述了物理层认证的基本原理；然后对中间人导频攻击进行建模，揭示了中间人导频攻击的内在机理；进一步地，提出一种渐进无感的接入策略，使得攻击者能够顺利接入合法通信过程；最后，在攻击者顺利接入合法通信过程后，针对两种基本物理层认证机制进行攻击分析和仿真验证。

2 物理层认证的两种基本机制

2.1 基于CSI的比较认证机制

基于CSI的比较认证机制基本原理可总结为图1流程，Bob对来自Alice的信号进行认证。在通信初始时刻，Bob通过高层认证确保$\boldsymbol{H}_{\mathrm{AB},0}$来自于合法Alice，建立认证起点并存储$\boldsymbol{H}_{\mathrm{AB},0}$。在后续时刻，Bob比较当前帧的CSI和上一时刻存储的CSI，检验是否满足$\mathrm{diff}(\boldsymbol{H}_{\mathrm{AB,t}}-\boldsymbol{H}_{\mathrm{AB,t-1}})<\Gamma$。若满足，则Bob认为当前帧来自于合法Alice并更新当前存储的CSI；否则，拒绝当前消息。由于无线信道的空间去相关性和时变性，Eve很难复制当前合法CSI。

2.2 基于CSI的加密认证机制

基于CSI的加密认证机制基本原理可总结为图2流程，简单来说，通信一方利用$\boldsymbol{H}_{\mathrm{AB}}$对认证向量进行某种形式的加密运算，通信另一方利用与$\boldsymbol{H}_{\mathrm{AB}}$互易的$\boldsymbol{H}_{\mathrm{BA}}$对信号进行相应的解密，从而完成认证过程。基于CSI的加密认证有多种应用方式，文献[5–8]中物理层-高层融合认证机制本质上都是CSI加密认证机制基本原理的应用。

3 中间人导频攻击系统模型

无论是基于CSI的比较认证机制还是基于CSI的加密认证机制，其安全性都依赖于通信双方无线

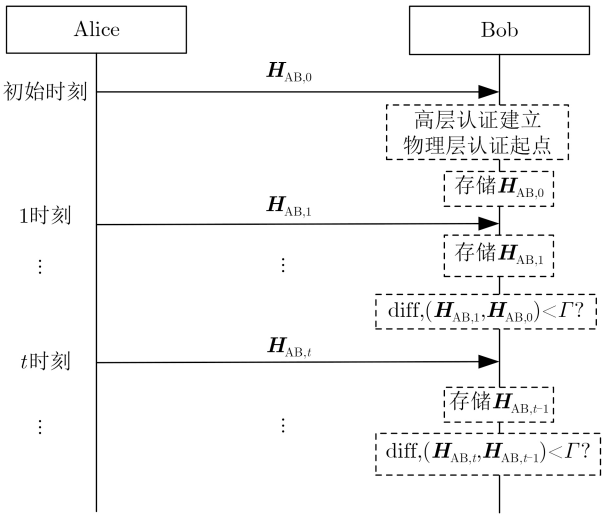

图 1 基于CSI的比较认证机制基本流程

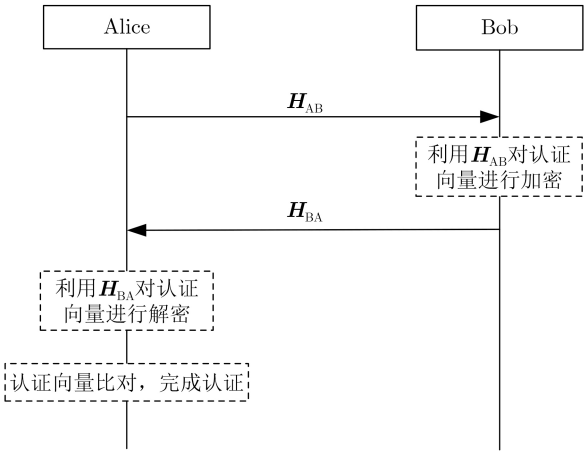

图 2 基于CSI的加密认证机制基本流程

信道的私有性和唯一性。本节将介绍一种中间人导频攻击模型，通过操控Alice和Bob之间的信道估计过程，窃取Alice和Bob之间的信道状态信息。

中间人导频攻击模型如图3所示，考虑时分双工系统(TDD)。假设有一个中间人导频攻击者(Man-in-the Middle (MITM) attacker)Eve，能够跟踪Alice和Bob的传输过程并进行同步。Eve为了隐蔽自己的身份和活动，采用透明转发模式，不对接收到的信息进行篡改和伪造，Eve接收来自Alice(Bob)的公开导频并透明放大转发至Bob(Alice)。假设信道为准静态块衰落信道，Alice, Bob, Eve处分别配备N_{A}，N_{B}，N_{E}根天线，各节点采用最小二乘(Least Squares, LS)信道估计算法。

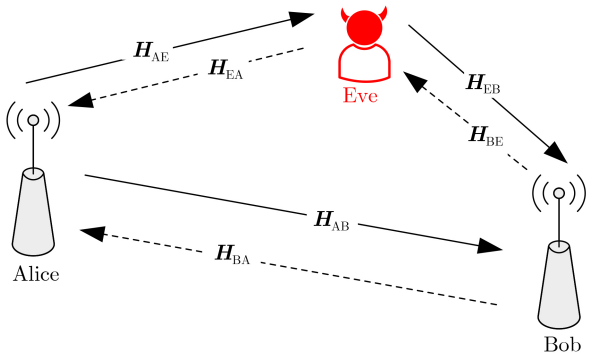

图 3 中间人导频攻击模型

Alice和Bob互发导频进行上下行信道估计，以Alice发送导频，Bob进行信道估计过程为例，Alice发送正交的公开导频矩阵$\boldsymbol{X}_{\mathrm{A}}$，$\boldsymbol{X}_{\mathrm{A}}=\left[\boldsymbol{x}_{\mathrm{A}}^{1},\boldsymbol{x}_{\mathrm{A}}^{2},\cdots,\boldsymbol{x}_{\mathrm{A}}^{\mathrm{L}}\right]\in\mathbb{C}^{\mathrm{N_A}\times\mathrm{L}}$，其中$L$是导频序列长度，$L>N_{\mathrm{A}}$，$\boldsymbol{x}_{\mathrm{A}}^{i}\in\mathbb{C}^{N_{\mathrm{A}}\times 1}$。当不考虑中间人导频攻击者时，Bob处的接收信号为

$$\boldsymbol{Y}_{\mathrm{B}}=\boldsymbol{H}_{\mathrm{AB}}\boldsymbol{X}_{\mathrm{A}}+\boldsymbol{V}_{\mathrm{B}} \tag{1}$$

其中，$\boldsymbol{H}_{\mathrm{AB}}\in\mathbb{C}^{N_{\mathrm{B}}\times N_{\mathrm{A}}}$是从Alice到Bob的信道矩阵，不考虑天线之间的相关性，假设信道矩阵各元素服从独立同分布的零均值循环对称复高斯(Circular Symmetric Complex Gaussian, CSCG)随机变量，即$h\in\mathcal{CN}\left(0,\sigma_{\mathrm{h}}^{2}\right)$，方差$\sigma_{\mathrm{h}}^{2}$与传输距离有关，代表路径损耗的大小。后文所涉及的各信道矩阵均服从这一分布。$\mathrm{tr}\left(\boldsymbol{x}_{\mathrm{A}}\boldsymbol{x}_{\mathrm{A}}^{H}\right)\le\mathrm{P_A}$满足导频功率约束，$P_{\mathrm{A}}$是一个导频序列的功率。$\boldsymbol{V}_{\mathrm{B}}\in\mathbb{C}^{N_{\mathrm{B}}\times L}$是Bob处的接收噪声，矩阵元素$\boldsymbol{v}\in\mathcal{CN}\left(0,\sigma_{v}^{2}\right)$，服从独立同分布的CSCG随机变量，假设后文所涉及的噪声矩阵均符合这一分布且方差均为σ_{v}^{2}。同理，Bob发送公开导频$\boldsymbol{X}_{\mathrm{B}}=\left[\boldsymbol{x}_{\mathrm{B}}^{1},\boldsymbol{x}_{\mathrm{B}}^{2},\cdots,\boldsymbol{x}_{\mathrm{B}}^{\mathrm{L}}\right]\in\mathbb{C}^{N_{\mathrm{B}}\times L}$时，Alice处的接收信号为

$$\boldsymbol{Y}_{\mathrm{A}}=\boldsymbol{H}_{\mathrm{BA}}\boldsymbol{X}_{\mathrm{B}}+\boldsymbol{V}_{\mathrm{A}} \tag{2}$$

其中，$\boldsymbol{H}_{\mathrm{BA}}\in\mathbb{C}^{N_{\mathrm{A}}\times N_{\mathrm{B}}}$表示从Bob到Alice的信道矩阵，$\mathrm{tr}\left(\boldsymbol{x}_{\mathrm{B}}\boldsymbol{x}_{\mathrm{B}}^{\mathrm{H}}\right)\le P_{\mathrm{B}}$，$\boldsymbol{V}_{\mathrm{A}}\in\mathbb{C}^{N_{\mathrm{A}}\times L}$表示Alice处的噪声矩阵。Alice和Bob采用LS信道估计算法分别估计信道为

$$\tilde{\boldsymbol{H}}_{\mathrm{BA}}=\boldsymbol{H}_{\mathrm{BA}}+\boldsymbol{V}_{\mathrm{A}}\boldsymbol{X}_{\mathrm{B}}^{*} \tag{3}$$

$$\tilde{\boldsymbol{H}}_{\mathrm{AB}}=\boldsymbol{H}_{\mathrm{AB}}+\boldsymbol{V}_{\mathrm{B}}\boldsymbol{X}_{\mathrm{A}}^{*} \tag{4}$$

其中，$\boldsymbol{X}_{\mathrm{B}}^{*}=\boldsymbol{X}_{\mathrm{B}}^{\mathrm{H}}\left(\boldsymbol{X}_{\mathrm{B}}\boldsymbol{X}_{\mathrm{B}}^{\mathrm{H}}\right)^{-1}$，$\boldsymbol{X}_{\mathrm{A}}^{*}=\boldsymbol{X}_{\mathrm{A}}^{\mathrm{H}}\left(\boldsymbol{X}_{\mathrm{A}}\boldsymbol{X}_{\mathrm{A}}^{\mathrm{H}}\right)^{-1}$分别是$\boldsymbol{X}_{\mathrm{B}}$, $\boldsymbol{X}_{\mathrm{A}}$的伪逆矩阵。

当考虑中间人导频攻击者时，Eve对Alice和Bob发来的公开导频分别进行转发。当Alice或Bob发送公开导频时，Eve处的接收信号为

$$\boldsymbol{Y}_{\mathrm{AE}}=\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{X}_{\mathrm{A}}+\boldsymbol{V}_{\mathrm{AE}} \tag{5}$$

$$\boldsymbol{Y}_{\mathrm{BE}}=\boldsymbol{H}_{\mathrm{BE}}\boldsymbol{X}_{\mathrm{B}}+\boldsymbol{V}_{\mathrm{BE}} \tag{6}$$

采用和Alice, Bob相同的信道估计过程，Eve能够估计其与Alice和Bob之间的信道

$$\tilde{\boldsymbol{H}}_{\mathrm{AE}}=\boldsymbol{H}_{\mathrm{AE}}+\boldsymbol{V}_{\mathrm{AE}}\boldsymbol{X}_{\mathrm{A}}^{*} \tag{7}$$

$$\tilde{\boldsymbol{H}}_{\mathrm{BE}}=\boldsymbol{H}_{\mathrm{BE}}+\boldsymbol{V}_{\mathrm{BE}}\boldsymbol{X}_{\mathrm{A}}^{*} \tag{8}$$

其中，$\boldsymbol{H}_{\mathrm{AE}}$, $\boldsymbol{H}_{\mathrm{BE}}$分别是Alice到Eve, Bob到Eve的信道矩阵，$\boldsymbol{V}_{\mathrm{AE}}$和$\boldsymbol{V}_{\mathrm{BE}}$是噪声矩阵。

由于中间人导频攻击者Eve对导频信号进行转发，因此Bob或Alice不仅接收来自合法端的导频，还接收到Eve放大转发而来的导频，此时Bob或Alice的接收到的混合信号为

$$\boldsymbol{Y}_{\mathrm{B}}^{+}=\boldsymbol{H}_{\mathrm{AB}}\boldsymbol{X}_{\mathrm{A}}+\mu_{1}\boldsymbol{H}_{\mathrm{EB}}\left(\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{X}_{\mathrm{A}}+\boldsymbol{V}_{\mathrm{AE}}\right)+\boldsymbol{V}_{B} \tag{9}$$

$$\boldsymbol{Y}_{\mathrm{A}}^{+}=\boldsymbol{H}_{\mathrm{BA}}\boldsymbol{X}_{\mathrm{B}}+\mu_{2}\boldsymbol{H}_{\mathrm{EA}}\left(\boldsymbol{H}_{\mathrm{BE}}\boldsymbol{X}_{\mathrm{B}}+\boldsymbol{V}_{\mathrm{BE}}\right)+\boldsymbol{V}_{\mathrm{A}} \tag{10}$$

其中，$\mu_{1}>0$, $\mu_{2}>0$是中间人导频攻击者Eve的放大转发系数，可表示为

$$\left.\begin{aligned}\mu_{1}&=\left(P_{\mathrm{E}}/\left\|\boldsymbol{H}_{\mathrm{AE}}\boldsymbol{X}_{\mathrm{A}}+\boldsymbol{V}_{\mathrm{AE}}\right\|^{2}\right)^{\frac{1}{2}}\\ \mu_{2}&=\left(P_{\mathrm{E}}/\left\|\boldsymbol{H}_{\mathrm{BE}}\boldsymbol{X}_{\mathrm{B}}+\boldsymbol{V}_{\mathrm{BE}}\right\|^{2}\right)^{\frac{1}{2}}\end{aligned}\right\} \tag{11}$$

$\|\cdot\|$表示Frobenius范数。Alice和Bob采用LS算法时的信道估计为

$$\tilde{\boldsymbol{H}}_{\mathrm{AB}}^{+}=\boldsymbol{H}_{\mathrm{AB}}+\mu_{1}\boldsymbol{H}_{\mathrm{AB}}^{\prime}+\left(\mu_{1}\boldsymbol{H}_{\mathrm{AB}}^{\prime}\boldsymbol{V}_{\mathrm{AE}}+\boldsymbol{V}_{\mathrm{B}}\right)\boldsymbol{X}_{\mathrm{A}}^{*} \tag{12}$$

$$\tilde{\boldsymbol{H}}_{\mathrm{BA}}^{+}=\boldsymbol{H}_{\mathrm{BA}}+\mu_{2}\boldsymbol{H}_{\mathrm{BA}}^{\prime}+\left(\mu_{2}\boldsymbol{H}_{\mathrm{BA}}^{\prime}\boldsymbol{V}_{\mathrm{BE}}+\boldsymbol{V}_{\mathrm{A}}\right)\boldsymbol{X}_{\mathrm{B}}^{*} \tag{13}$$

其中，$\boldsymbol{H}_{\mathrm{AB}}^{\prime}=\boldsymbol{H}_{\mathrm{EB}}\boldsymbol{H}_{\mathrm{AE}}$, $\boldsymbol{H}_{\mathrm{BA}}^{\prime}=\boldsymbol{H}_{\mathrm{EA}}\boldsymbol{H}_{\mathrm{BE}}$是两段攻击信道的级联信道。由式(12)和式(13)可知，当存在中间人导频攻击者Eve时，Alice和Bob所估计的信道均“混入”了攻击信道状态信息，因此Eve可以窃取合法信道的部分信息，这会对依赖信道状态信息私有性的物理层认证机制产生重大威胁。

4 中间人导频攻击的渐进无感接入策略

由式(12)和式(13)可知，当存在Eve时，Alice或Bob所估计的信道中“混入”了Alice-Eve-Bob攻击链路的CSI，若Eve直接接入Alice和Bob之间，会导致Alice或Bob所估计的CSI发生较大变化，从而导致认证失败和通信过程中断。因此，在考虑利用中间人导频攻击者实施攻击时，应首先考虑攻击者Eve的接入问题。

另外，为了对抗信道估计误差和信道的时变性，物理层认证机制一般为CSI的变化留有一定的容忍度，即具有一定的鲁棒性。这种“鲁棒性”一方面增强了物理层机制的健壮性，另一方面为中间人导频攻击的接入留下了空间和漏洞。中间人导频攻击者Eve能够逐步增大转发时的导频功率，利用物理层认证机制为CSI变化留下的“裕度”，使得中间人接入过程中的信道波动在物理层认证机制的“容忍”范围内，从而渐进接入Alice和Bob之间。本文将这种方式称为渐进无感的接入策略。下面主要基于CSI的比较认证机制，给出Eve的渐进无感接入策略。其他物理层认证机制的接入过程需要针对性分析，本节重在阐述渐进无感接入策略的基本思想。

考虑最基本的基于CSI的比较认证机制，Alice是合法发送者，Bob是接收者，潜在攻击者Eve试图在无线链路中注入欺骗信号冒充Alice。Bob通过假设检验的方式确定相邻两帧CSI的相似度，从而确定系统是否遭到攻击。假设上一帧的信道矩阵为$\boldsymbol{H}_{t-1}$，由于信道的短时不变性，当前帧的信道矩阵$\boldsymbol{H}_t$与上一帧信道矩阵$\boldsymbol{H}_{t-1}$具有极强的相似性；又由于无线环境的变化和节点的移动性，连续帧间的信道状态会发生一定变化。本文采用1阶自回归模型[2,4]表示连续帧之间的相似性和变化性，即

$$\boldsymbol{H}_t = \rho\boldsymbol{H}_{t-1} + \sqrt{(1-\rho^2)\,\sigma_h^2}\boldsymbol{\varepsilon}_t \tag{14}$$

其中，系数ρ代表连续帧之间的相似性，ρ越大，表示连续两帧的信道越相似。由于相邻两帧信道探测在相干时间内，ρ一般取接近1的数值；噪声矩阵$\boldsymbol{\varepsilon}_t$与$\boldsymbol{H}_t$具有相同的维度且相互独立，每个元素均服从$\mathcal{CN}(0,1)$；$\sigma_h^2$是$\boldsymbol{H}_t$每个元素的方差。

采用LS算法时，Bob处存储的上一帧的CSI和当前帧的CSI分别为

$$\tilde{\boldsymbol{H}}_{t-1} = \boldsymbol{H}_{t-1} + \boldsymbol{V}_{\mathrm{B},t-1}\boldsymbol{X}_{\mathrm{A}}^{*} \tag{15}$$

$$\tilde{\boldsymbol{H}}_{t} = \boldsymbol{H}_{t} + \boldsymbol{V}_{\mathrm{B},t}\boldsymbol{X}_{\mathrm{A}}^{*} \tag{16}$$

Bob利用二元假设检验判断发送者是否合法，零假设$\mathcal{H}_0$代表前后两帧的信道状态信息很相近，当前帧的发送者仍然是Alice；备择假设$\mathcal{H}_1$代表前后两帧的信道状态发生了较大变化，当前帧的发送者不是Alice。

$$\begin{aligned}&\mathcal{H}_0 : \tilde{\boldsymbol{H}}_t = \tilde{\boldsymbol{H}}_{t-1}\\ &\mathcal{H}_1 : \tilde{\boldsymbol{H}}_t \neq \tilde{\boldsymbol{H}}_{t-1}\end{aligned} \tag{17}$$

采用基于广义似然比检测(Generalized Likelihood Ratio Test, GLRT)的假设检验统计量[4]。

$$L = \frac{\left\|\tilde{\boldsymbol{H}}_t - \tilde{\boldsymbol{H}}_{t-1}\right\|^2}{\sigma_h^2 + \sigma_N^2} \tag{18}$$

其中，σ_N^2是噪声项$\boldsymbol{V}_{\mathrm{B}}\boldsymbol{X}_{\mathrm{A}}^{*}$的方差，$\|\cdot\|$表示Frobenius范数，统计量$L$可以看作前后两次信道探测之间差异的归一化。

在基于CSI的比较认证机制中，虚警率(I类错误，将Alice误判为攻击者Eve)和漏检率(II类错误，将攻击者Eve误判为Alice)定义为

$$\begin{aligned}&\alpha = \Pr_{\mathcal{H}_0}, L > \Gamma\\ &\beta = \Pr_{\mathcal{H}_1}, L \le \Gamma\end{aligned} \tag{19}$$

门限值Γ在提供认证鲁棒性和稳健性的同时，也为比较认证机制中非法的CSI变化留下了“裕度”。

利用该“裕度”，渐进无感接入策略的方法是假设中间人导频攻击者Eve的放大转发系数从0开始以一个小斜率k逐渐增大，直至放大转发系数增大至式(11)所示的μ_1和μ_2，即认为顺利接入Alice和Bob之间。在Eve渐进无感的接入过程中，Bob处存储的上一帧的CSI和当前帧所估计的CSI分别为

$$\begin{aligned}\tilde{\boldsymbol{H}}_{\mathrm{AB},t-1}^{+} =&\boldsymbol{H}_{\mathrm{AB},t-1} + k\times(t-1)\,\boldsymbol{H}'_{\mathrm{AB},t-1} + \Big(k\times(t-1)\\ &\cdot\boldsymbol{H}'_{\mathrm{AB},t-1}\boldsymbol{V}_{\mathrm{AE},t-1} + \boldsymbol{V}_{\mathrm{B},t-1}\Big)\boldsymbol{X}_{\mathrm{A}}^{*}\end{aligned} \tag{20}$$

$$\begin{aligned}\tilde{\boldsymbol{H}}_{\mathrm{AB},t}^{+} =&\boldsymbol{H}_{\mathrm{AB},t} + (k\times t)\,\boldsymbol{H}'_{\mathrm{AB},t}\\ &+ \left((k\times t)\,\boldsymbol{H}'_{\mathrm{AB},t}\boldsymbol{V}_{\mathrm{AE},t} + \boldsymbol{V}_{\mathrm{B},t}\right)\boldsymbol{X}_{\mathrm{A}}^{*}\end{aligned} \tag{21}$$

若要不被Bob处的比较认证机制察觉，则$t-1$时刻和t时刻的信道差异应满足

$$L^{+} = \frac{1}{\sigma_h^2 + \sigma_N^2}\left\|\tilde{\boldsymbol{H}}_{\mathrm{AB},t}^{+} - \tilde{\boldsymbol{H}}_{\mathrm{AB},t-1}^{+}\right\| \le \Gamma \tag{22}$$

渐进无感攻击时的统计量L^{+}相对于式(18)中的统计量L，增加了攻击链路上的信道变化$(k\times t)\,\boldsymbol{H}'_{\mathrm{AB},t} - k\times(t-1)\,\boldsymbol{H}'_{\mathrm{AB},t-1}$和噪声项$(k\times t)\,\boldsymbol{H}'_{\mathrm{AB},t}\boldsymbol{V}_{\mathrm{AE},t}\boldsymbol{X}_{\mathrm{A}}^{*} - k\times(t-1)\,\boldsymbol{H}'_{\mathrm{AB},t-1}\boldsymbol{V}_{\mathrm{AE},t-1}\boldsymbol{X}_{\mathrm{A}}^{*}$，信道变化项制约了放大转发系数的增大斜率$k$不能过大，否则信道的快速变化会引起认证失败；噪声项制约了放大转发系数的绝对值kt也不能无限制增大，否则过高的噪声同样会引起认证失败，即Eve转发功率有上限制约(另一方面，Eve转发功率

的过大会面临暴露风险，文献[11–13]均给出了导频攻击的检测方法)。统计量L^+很难给出具体分布，下面仅通过仿真进行说明。本文的路径损耗系数用$\mathrm{d}^{-\alpha}$表示，α是路径损耗因子，仿真参数设置如表1所示，以下所求概率类指标均通过蒙特卡洛实验求得。

图4给出了Eve从0开始首次增大导频转发功率时，Alice和Bob之间认证成功率(1-虚警率)的变化。由图4可知，随着放大转发系数的增大，斜率k不断增加，认证成功率逐渐变小，特别是当$k>10$时，认证成功率急剧下降，说明当$k>10$时，由于Eve导频功率的增大而带来的信道变化已经超过了认证门限Γ的“容忍度”，极易引起Eve接入过程的失败。对比$\Gamma=9,10,11$ 3条曲线可以发现，门限值Γ越大，对Eve导频功率的变化容忍度越高，即允许Eve导频功率以一个较大的速率增长。

攻击者的放大转发系数在渐进增大过程中所设定的目标值，称为放大转发系数的目标值。由图5可知，放大转发系数的目标值越大，Eve成功接入的概率越小，其原因是对相同的增大斜率k来说，放大转发系数的目标值越大，Eve经历的导频功率增加过程越长，而每一次导频增大都带来一定的失败风险，因而造成最终接入概率越小。当$k=18$时，Eve成功接入概率变得很小，这和图4中当$k>10$时信道变化超过门限值Γ的“容忍度”的分析是吻合的。

由图6可知，当斜率$k<8$时，即使对于较大的放大转发系数目标值，Eve仍然能够以一个较高的概率成功接入；当以$k>8$的斜率接入时，信道的快速变化逐渐引起物理层比较认证机制的察觉，因而造成成功接入概率较低。因此，Eve若要实现“无感”接入，需要以较小的斜率“渐进”增大导频功率，这正是渐进无感接入策略的含义。

表 1　仿真参数列表

仿真参数	设定值
配置天线数	$N_{\mathrm{A}}=N_{\mathrm{B}}=N_{\mathrm{E}}=8$
导频功率	$P_{\mathrm{A}}=P_{\mathrm{B}}=30$ dBm
噪声功率	$\sigma_v=-80$ dBm
节点之间的距离	$d_{\mathrm{AB}}=100, d_{\mathrm{AE}}=60, d_{\mathrm{EB}}=60$
路径损耗因子	$\alpha=3$
系数ρ	0.95
导频长度	$L=16$

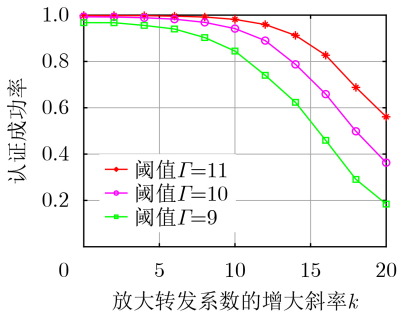

图 4 Eve首次增大转发功率时认证成功率随斜率k的变化

5　针对物理层认证的攻击分析

当中间人导频攻击者Eve按照第4节所述的渐进无感策略接入Alice和Bob之间后，可对两种物理层认证机制发起多种形式的攻击。本节主要对两种物理层认证机制进行攻击分析并仿真验证。

5.1　针对基于CSI的比较认证机制的攻击

5.1.1　拒绝服务攻击

当中间人导频攻击者Eve成功接入后，Eve可以通过突然大幅改变导频转发功率使得当前认证失败，但这种方式容易暴露窃听者的目的和位置[11–13]。本小节提出了一种绿色环保隐蔽的Eve随机相位加扰的方法操控Bob处的信道快变，从而使Alice无法通过认证，达到拒绝服务攻击的效果。

当中间人导频攻击者Eve在进行放大转发时，在N_{E}根天线上添加随机相位因子$\boldsymbol{\theta}=[\theta_1,\theta_2,\cdots,\theta_{N_{\mathrm{E}}}]$，此时Bob处的接收信号为

$$\boldsymbol{Y}_{\mathrm{B}}^{+}=\boldsymbol{H}_{\mathrm{AB},t}\boldsymbol{X}_{\mathrm{A}}+\mu_1\boldsymbol{H}_{\mathrm{EB},t}\boldsymbol{\Theta}\left(\boldsymbol{H}_{\mathrm{AE},t}\boldsymbol{X}_{\mathrm{A}}+\boldsymbol{V}_{\mathrm{AE},t}\right)+\boldsymbol{V}_{\mathrm{B},t} \tag{23}$$

其中，$\boldsymbol{\Theta}=\mathrm{diag}\left(\beta\mathrm{e}^{\mathrm{j}\theta_1},\beta\mathrm{e}^{\mathrm{j}\theta_2},\cdots,\beta\mathrm{e}^{\mathrm{j}\theta_{N_{\mathrm{E}}}}\right)$表示随机相位加扰矩阵，$\beta\in(0,1)$，在本方法中取$\beta=1$，即

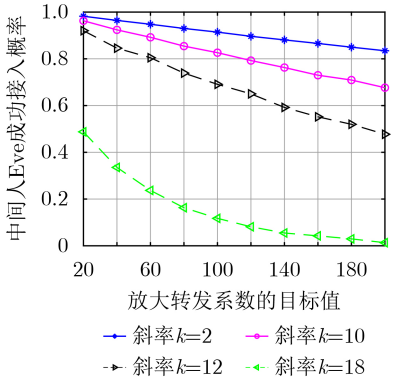

图 5 Eve成功接入概率随放大转发系数目标值的变化

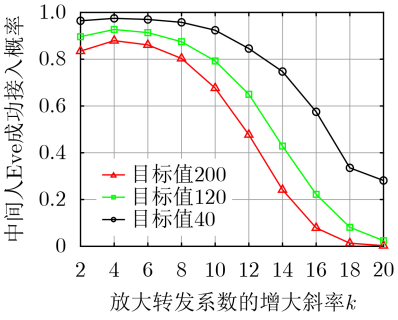

图 6 不同目标值下Eve成功接入概率与增大斜率k的关系

只考虑相位加扰，不考虑幅度变化，此时随机相位加扰矩阵$\boldsymbol{\Theta}$可由一系列廉价的移相器实现。此时Bob处的信道估计为

$$\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB},t}=\boldsymbol{H}_{\mathrm{AB},t}+\mu_1\boldsymbol{H}'_{\mathrm{AB},t}+\left(\mu_1\boldsymbol{H}'_{\mathrm{AB},t}\boldsymbol{V}_{\mathrm{AE},t}+\boldsymbol{V}_{\mathrm{B},t}\right)\boldsymbol{X}^{*}_{\mathrm{A}} \tag{24}$$

其中，$\boldsymbol{H}'_{\mathrm{AB},t}=\boldsymbol{H}_{\mathrm{EB},t}\boldsymbol{\Theta}\boldsymbol{H}_{\mathrm{AE},t}$表示攻击链路的等效信道矩阵，通过调整随机相位加扰矩阵$\boldsymbol{\Theta}$，使得$\boldsymbol{H}'_{\mathrm{AB}}$快变，进而使Bob处的估计信道$\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}}$快变。若要比较认证机制失败，则假设检验统计量$L^{+}$需满足

$$L^{+}=\frac{1}{\sigma_h^2+\sigma_N^2}\left\|\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB},t}-\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB},t-1}\right\|>\Gamma \tag{25}$$

其中，$\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB},t}$是叠加随机相位加扰矩阵后的当前帧的CSI, $\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB},t-1}$是上一帧保存的信道矩阵。下面通过仿真说明随机相位加扰方法的有效性，仿真参数在表1中列出。

图7给出了Eve采用随机相位加扰方法时，Bob拒绝服务的概率与放大转发系数大小的关系。放大转发系数越大意味着攻击信道在合法信道中的比重越大，因此采用随机相位加扰方法时的拒绝服务攻击效果越好。由图7可以看出，当放大转发系数大于20时，拒绝服务的概率达到0.9。这意味着拒绝服务攻击对Eve导频功率的大小要求很低，只需要很小的导频功率就可以成功实施拒绝服务攻击。拒绝服务攻击达到了阻断当前Alice和Bob之间通信的效果。

5.1.2 仿冒接入攻击

当Eve转发的导频功率相对Alice到Bob的导频功率足够大时，Bob在信道估计时甚至会把攻击信道当做合法信道，此时攻击者Eve极有可能取代Alice接入Bob，实施仿冒Alice身份进行接入。下面通过仿真说明仿冒接入攻击效果，仿真参数在表1中列出。

图8给出了仿冒接入成功率随放大转发系数的变化，由图可知，随着放大转发系数的增大，仿冒接入攻击成功率在很大的区间内保持为0；直到放大转发系数超过120，仿冒接入成功率才开始逐渐增大。其原因是仿冒接入攻击是用攻击信道替换原来的混合信道，在仿冒接入攻击时Bob处估计的信道中不再包含Alice到Bob间的信道，因而使得信道发生变化并超出了门限值Γ的“容忍度”。只有当攻击信道在混合信道中占据绝对优势时，仿冒接入攻击才有成功的可能性。这意味着仿冒接入攻击实施难度较高，一方面这种攻击对Eve导频的功率要求很高；另一方面过高的Eve导频功率不仅导致接入过程漫长，成功率低(由图5可以得出该结论)，而且容易被Alice或Bob检测发现Eve的导频攻击行为。但需要指出，Eve仍然有一定机会实施仿冒接入攻击，即使是较小的攻击成功率，对于Alice和Bob来说也是不可接受的。

5.2 针对基于CSI的加密认证机制的攻击

基于CSI的加密认证机制基本思想是利用物理信道所蕴含的丰富信息对信号进行加密，接收端利用信号互易性进行解密，从而完成认证过程。在中间人导频攻击下，由式(12)和式(13)可知，发送端和接收端加密认证所使用的物理信道信息面临污染和泄露。由于基于CSI的加密认证机制多种多样，本节仅从信息论角度给出中间人导频攻击效果的理论值，并仿真说明中间人导频攻击的效果。

加密认证机制本质上是将Alice和Bob之间的互易随机信道作为共享的“秘密信息”，对认证向量进行加解密从而实现认证过程。根据信息论理论，在不考虑攻击者Eve的情况下，Alice和Bob之间可用于加密认证的“秘密信息”的理论上限为$\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}}$和$\tilde{\boldsymbol{H}}^{+}_{\mathrm{BA}}$之间的互信息，可计算如下[14]

$$\begin{aligned}I_{\mathrm{AB}}=&I\left(\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}},\tilde{\boldsymbol{H}}^{+}_{\mathrm{BA}}\right)=h\left(\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}}\right)+h\left(\tilde{\boldsymbol{H}}^{+}_{\mathrm{BA}}\right)\\&-h\left(\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}},\tilde{\boldsymbol{H}}^{+}_{\mathrm{BA}}\right)=\log_2\frac{|\boldsymbol{R}_{\mathrm{AA}}|\,|\boldsymbol{R}_{\mathrm{BB}}|}{|\boldsymbol{C}_{\mathrm{AB}}|}\end{aligned} \tag{26}$$

其中，$h(\cdot)$表示矩阵的熵值，$|\cdot|$表示矩阵的行列式值，$\boldsymbol{R}_{\mathrm{AA}}$, $\boldsymbol{R}_{\mathrm{BB}}$和$\boldsymbol{C}_{\mathrm{AB}}$分别表示信道矩阵$\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}}$自相关矩阵、$\tilde{\boldsymbol{H}}^{+}_{\mathrm{BA}}$的自相关矩阵以及$\tilde{\boldsymbol{H}}^{+}_{\mathrm{AB}}$和$\tilde{\boldsymbol{H}}^{+}_{\mathrm{BA}}$的互相关矩阵，分别定义为

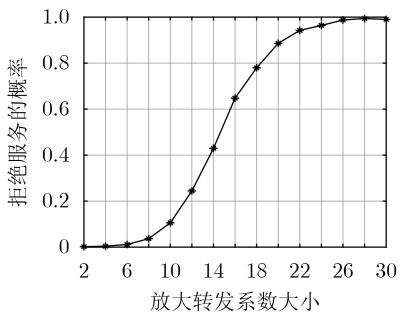

图 7 拒绝服务概率与放大转发系数的关系

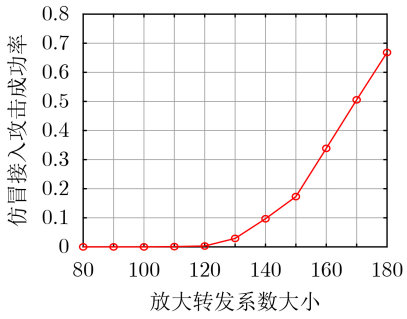

图 8 仿冒接入成功率随放大转发系数的变化

$$\left.\begin{aligned}\boldsymbol{R}_{\mathrm{AA}} &= \mathbb{E}\left(\tilde{\boldsymbol{H}}_{\mathrm{AB}}^{+}\tilde{\boldsymbol{H}}_{\mathrm{AB}}^{+\,\mathrm{H}}\right)\\ \boldsymbol{R}_{\mathrm{BB}} &= \mathbb{E}\left(\tilde{\boldsymbol{H}}_{\mathrm{BA}}^{+}\tilde{\boldsymbol{H}}_{\mathrm{BA}}^{+\,\mathrm{H}}\right)\\ \boldsymbol{C}_{\mathrm{AB}} &= \mathbb{E}\left(\tilde{\boldsymbol{H}}_{\mathrm{AB}}^{+}\tilde{\boldsymbol{H}}_{\mathrm{BA}}^{+\,\mathrm{H}}\right)\end{aligned}\right\} \tag{27}$$

当考虑攻击者Eve时，Alice和Bob可用于加密认证的私密信息量为$\tilde{\boldsymbol{H}}_{\mathrm{AB}}^{+}$和$\tilde{\boldsymbol{H}}_{\mathrm{BA}}^{+}$之间的条件互信息

$$I_{\mathrm{AB|Eve}}= I\left(\tilde{\boldsymbol{H}}_{\mathrm{AB}}^{+},\tilde{\boldsymbol{H}}_{\mathrm{BA}}^{+}|\boldsymbol{H}'_{\mathrm{AB}}\right) \tag{28}$$

其中，$\boldsymbol{H}'_{\mathrm{AB}}=\boldsymbol{H}_{\mathrm{EB}}\boldsymbol{H}_{\mathrm{AE}}$。私密信息泄露率(Private Information Leakage Rate)是Alice和Bob在信道估计过程中泄露给Eve的信息量，即

$$I_{\mathrm{LR}} = I_{\mathrm{AB}} - I_{\mathrm{AB|Eve}} \tag{29}$$

信道信息泄露量I_{LR}表征了攻击者Eve对加密认证机制的攻击能力大小，定义I_{LR}和I_{AB}之比为

$$A = \frac{I_{\mathrm{LR}}}{I_{\mathrm{AB}}} \tag{30}$$

该比值的大小更加直观地反映了Eve的攻击效果。本节利用Szabo[15]开发的ITE(Information Theoretical Estimators, ITE)MATLAB工具箱计算Shannon互信息，利用蒙特卡洛仿真求互信息平均值。

图9仿真了Alice和Bob间信道的互信息、条件互信息以及信息泄漏量随放大转发系数的变化。每个信道矩阵包含64个复数元素，本文中互信息计算的是64个复数矩阵元素的互信息量。由图9可知，随着放大转发系数的增大，条件互信息不断减少，信息泄漏量持续增加，中间人导频攻击所能获得的私密认证信息越来越多，攻击效果越来越好，这和本文的理论和逻辑分析是一致的。图10通过信息泄漏率随放大转发系数的变化曲线，更加直观地说明了中间人导频攻击的效果。随着放大转发系数的增大，信息泄漏率越来越高，在放大转发系数为40时，信息泄漏率就已经接近50%。随着Eve攻击次数的增加，Eve持续累积关于认证向量的密文和对应明文，就有可能实现对认证向量的完全破解。

5.3 关于中间人导频攻击的防护

对于基于CSI的比较认证机制来说，中间人导频攻击很难防护，一种可行的办法是加大对中间人导频攻击的检测力度，可参考一般导频攻击的检测方法，从源头上杜绝攻击者的存在。

对于基于CSI的加密认证机制来说，可以采取文献[16]中的私密导频方法，即通过Alice和Bob共享私密导频序列，从而杜绝Eve获得任何信道状态信息。该私密导频方法可简要叙述如下：

(1) Alice和Bob利用高层秘密信息对私密导频的种子信息进行初始化；

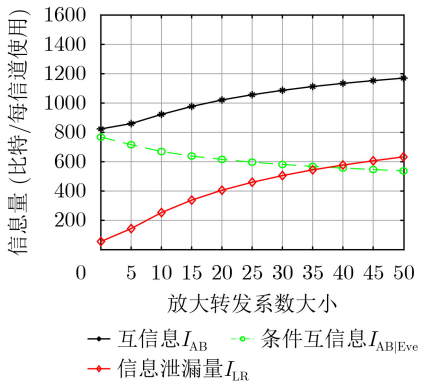

图 9 互信息、条件互信息、信息泄漏量随放大转发系数的变化

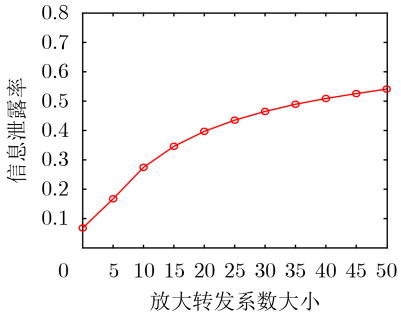

图 10 信息泄漏率随放大转发系数的变化

(2) Alice和Bob根据初始私密导频进行信道估计，根据信道估计值生成私密导频新的种子信息；

(3) 根据新的种子信息对私密导频进行更新。

中间人导频攻击检测和私密导频方法均对中间人导频攻击有良好的防护作用，但也付出了一定防护代价，增加了计算开销，对系统延迟也有一定影响。因此，系统安全性的提高往往伴随着复杂度等多方面开销的增加。无论是高层密码技术还是物理层安全技术，安全性的提高均要付出一定代价，安全与防护呈现交替螺旋式上升关系。

6 结束语

本文针对现有物理层认证机制依赖信道状态信息私有性的特点，对物理层认证的中间人导频攻击进行了分析。中间人导频攻击通过控制合法通信双方的信道测量，破坏合法信道的私有性，可采用渐进无感接入策略接入合法通信过程，进而发起拒绝服务攻击、仿冒接入攻击、破解认证向量等多种攻击方式。对中间人导频攻击的防护需要加大对中间人导频攻击者的检测力度或采用某种手段保护信道探测过程的私密性，可留作后续研究。

参 考 文 献

[1] WU Yongpeng, KHISTI A, XIAO Chengshan, *et al*. A survey of physical layer security techniques for 5G wireless networks and challenges ahead[J]. *IEEE Journal on Selected*

Areas in Communications, 2018, 36(4): 679–695. doi: 10.1109/JSAC.2018.2825560.

[2] XIAO Liang, GREENSTEIN L, MANDAYAM N, *et al*. A physical-layer technique to enhance authentication for mobile terminals[C]. IEEE International Conference on Communications, Beijing, China, 2008: 1520–1524.

[3] XIAO Liang, GREENSTEIN L, MANDAYAM N, *et al*. MIMO-assisted channel-based authentication in wireless networks[C]. 2008 42nd Annual Conference on Information Sciences and Systems, Princeton, USA, 2008: 642–646.

[4] XIAO Liang, GREENSTEIN L J, MANDAYAM N B, *et al*. Using the physical layer for wireless authentication in time-variant channels[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(7): 2571–2579. doi: 10.1109/TWC.2008.070194.

[5] SHAN Dan, ZENG Kai, XIANG Weidong, *et al*. PHY-CRAM: Physical layer challenge-response authentication mechanism for wireless networks[J]. *IEEE Journal on Selected Areas in Communications*, 2013, 31(9): 1817–1827. doi: 10.1109/JSAC.2013.130914.

[6] WEN H, HO P H, QI C, *et al*. Physical layer assisted authentication for distributed ad hoc wireless sensor networks[J]. *IET Information Security*, 2010, 4(4): 390–396. doi: 10.1049/iet-ifs.2009.0197.

[7] YANG Jing, JI Xinsheng, HUANG Kaizhi, *et al*. Unified and fast handover authentication based on link signatures in 5G SDN-based HetNet[J]. *IET Communications*, 2019, 13(2): 144–152. doi: 10.1049/iet-com.2018.5405.

[8] 季新生, 杨静, 黄开枝, 等. 基于哈希方法的物理层认证机制[J]. 电子与信息学报, 2016, 38(11): 2900–2907. doi: 10.11999/JEIT160007.

JI Xinsheng, YANG Jing, HUANG Kaizhi, *et al*. Physical layer authentication scheme based on hash method[J]. *Journal of Electronics & Information Technology*, 2016, 38(11): 2900–2907. doi: 10.11999/JEIT160007.

[9] ZHOU Xiangyun, MAHAM B, and HJORUNGNES A. Pilot contamination for active eavesdropping[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(3): 903–907. doi: 10.1109/TWC.2012.020712.111298.

[10] HUANG Yu, LIANG Jin, WEI Hongquan, *et al*. Pilot contamination with MITM attack[C]. 2017 IEEE 85th Vehicular Technology Conference (VTC Spring), Sydney, Australia, 2017: 1–7.

[11] XIONG Qi, LIANG Yingchang, LI K H, *et al*. An energy-ratio-based approach for detecting pilot spoofing attack in multiple-antenna systems[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(5): 932–940. doi: 10.1109/TIFS.2015.2392564.

[12] TUGNAIT J K. Detection and identification of spoofed pilots in TDD/SDMA systems[J]. *IEEE Wireless Communications Letters*, 2017, 6(4): 550–553. doi: 10.1109/LWC.2017.2715814.

[13] LIU Xiaoming, LI Bin, CHEN Hongbin, *et al*. Detecting pilot spoofing attack in MISO systems with trusted user[J]. *IEEE Communications Letters*, 2019, 23(2): 314–317. doi: 10.1109/LCOMM.2018.2889491.

[14] COVER T M and THOMAS J A. Elements of Information Theory[M]. New York: Wiley-Interscience, 1991: 1–6.

[15] SZABÓ Z. Information theoretical estimators toolbox[J]. *Journal of Machine Learning Research*, 2014, 15(9): 283–287.

[16] HUANG Yu, JIN Liang, WEI Hongquan, *et al*. Fast secret key generation based on dynamic private pilot from static wireless channels[J]. *China Communications*, 2018, 15(11): 171–183. doi: 10.1109/CC.2018.8543098.

王少禹：男，1993年生，博士生，研究方向为物理层安全及信息安全.

黄开枝：女，1973年生，教授、博士生导师，研究方向为移动通信网络及信息安全.

许晓明：男，1988年生，副研究员，研究方向为移动通信网络及信息安全.

马克明：男，1988年生，助理研究员，研究方向为移动通信网络及信息安全.

陈亚军：男，1988年生，助理研究员，研究方向为移动通信网络及信息安全.

责任编辑：陈 倩