基于哈希方法的物理层认证机制

季新生 杨 静* 黄开枝 易 鸣
(国家数字交换系统工程技术研究中心 郑州 450001)

摘 要：现有物理层挑战-响应认证机制使用无线信道信息掩藏密钥生成认证响应，一旦攻击方获得合法信道信息，则可直接破解密钥。针对上述问题，该文借鉴曲线匹配原理，提出一种基于哈希方法的物理层认证机制。首先，认证双方提取无线信道特征，并和认证密钥组合得到初始认证向量，该向量被等效为一条曲线；随后，采用具有容错性的单向哈希函数将该曲线映射为低维的哈希矢量，用作认证响应；最后，认证方根据需求设置认证门限，并根据响应的匹配结果进行判决。性能分析表明，所采用的哈希方法实质为欠定方程组，攻击方无法根据低维哈希矢量还原曲线信息，从而无法破解密钥；仿真结果表明，在攻击方窃取了合法信道信息的条件下，在 4 dB 时，现有挑战-响应机制攻击率约为 0.5，该文所提机制可实现攻击率小于10^{-5} 。

关键词：物理层；认证；曲线匹配；哈希方法
中图分类号：TN92 **文献标识码**：A **文章编号**：1009-5896(2016)11-2900-08
DOI: 10.11999/JEIT160007

Physical Layer Authentication Scheme Based on Hash Method

JI Xinsheng YANG Jing HUANG Kaizhi YI Ming
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450001, *China*)

Abstract: To solve the problem of key leakages in existing physical layer challenge-response authentication schemes, a physical layer authentication scheme based on hash method is proposed. The channel characteristics are extracted and linked with the key which can be regarded as a curve. Then a fault-tolerant hash function is employed to map the curve into a response with lower dimension. The authenticator lastly sets the threshold according to the authentication requirement and further to verify the identity of the requester. The hash function is an underdetermined system and attackers can not recover the curve according to the response. Simulation results prove the effectiveness of the scheme whose attack rate is less than 10^{-5} while attack rates for existing schemes are almost 0.5 under the SNR of 4 dB.

Key words: Physical-layer; Authentication; Curve matching; Hash method

1 引言

认证是确认通信实体身份合法性的过程，是实现安全通信的第一道保障。现有认证机制在高层采用密码机制实现，具有较大的时延和计算开销，给能量受限的终端带来诸多弊端；其次，高层认证没有充分考虑到无线信道的脆弱性，使得认证容易遭受来自物理层的攻击[1]。近年来出现了在物理层实现认证的研究，由于其低开销、轻量级以及能抵抗来自无线信道的攻击等优点得到了广泛的关注。

无线信道在空间上具有多样形、私有性[2]，即任意两个通信实体间建立的无线链路是唯一的、不可复制的；在时间上具有时变性、短时互易性，即无线信道时刻变化，但在信道相干时间内可认为是不变的，通信双方可提取出相同的信道特征[3]。无线信道的这些特性被用于实现认证[3,4]，文献[5–7]使用无线信道表征用户身份，将认证转化为信道特征的相似性检验问题，通过比较前后两次数据包的信道信息——如接收信号强度[5]、信道频率响应[6]或信道冲激响应[7]等参数是否一致，来判断通信链路是否改变从而检测无线信道是否遭受攻击，实现简单、开销低，可实现轻量级的认证。但该类方法只能用于检测通信过程是否遭受攻击，而无法实现用户初次接入网络时的身份认证。

文献[8–12]借鉴高层挑战-响应原理实现物理层

收稿日期：2016-01-04；改回日期：2016-05-23；网络出版：2016-07-19
*通信作者：杨静 yangjingFi@163.com
基金项目：国家 863 计划项目(2015AA01A708)，国家自然科学基金(61379006)，国家青年科学基金(61501516)
Foundation Items: The National 863 Program of China (2015AA01A708), The National Natural Science Foundation of China (61379006), The National Science Fund for Excellent Young Scholars (61501516)

身份认证，将密钥“藏”进经过无线信道作用后的认证挑战中生成认证响应，仅具有相同信道的合法接收方可解出认证数据，在身份认证的同时防止无线信道受到攻击。但上述方法隐藏密钥的方式比较直接，存在密钥泄露的安全隐患：攻击方只要窃取了合法信道信息，即可根据认证响应直接破解密钥。

基于上述问题，本文提出一种基于哈希方法的物理层认证机制。认证双方提取无线信道特征作为认证挑战，并将该挑战和密钥组合得到初始认证向量，该向量可等效为一条人工曲线，由此将认证问题转化为曲线匹配问题；随后，双方利用容错性的单向哈希方法将该曲线映射为低维哈希矢量，并用作认证响应；最后，认证方根据认证需求设置认证门限，采用距离参数评价双方产生的认证响应的匹配程度，并根据匹配结果进行判决。产生认证响应的哈希方法实质为欠定方程组，其解空间为无穷，攻击方无法根据低维的认证响应还原高维的曲线信息，从而无法破解密钥。仿真结果表明，在 4 dB 信噪比条件下，当攻击方窃取了合法信道信息时，现有物理层挑战-响应机制攻击率约为 0.5，本文所提机制可实现攻击率小于10^{-5}。

2　问题描述

认证模型如图 1 所示，Alice 为请求方，Bob 为认证方，双方存储有共享密钥 $\boldsymbol{K}$，并期望通过 $\boldsymbol{K}$ 建立信任关系；Eve 为攻击方，致力于窃取 Alice-Bob 间的共享密钥 $\boldsymbol{K}$ 或者伪造认证数据以期通过 Bob 的认证。由于信道具有互易性，Alice 和 Bob 观察到的信道是一致的，即 $h_{\mathrm{AB}}=h_{\mathrm{BA}}$；同时，信道具有快速去相关性，只要 Alice, Bob, Eve 三者间距离大于 $\lambda/2$ (λ 为波长)，则两两间的信道各不相关[13]，即 $h_{\mathrm{AB}}\neq h_{\mathrm{EA}}\neq h_{\mathrm{EB}}$。

在文献[8–10]中，Bob 产生随机数组 $\boldsymbol{D}$ 作为认证挑战，假设 Alice-Bob 信道响应为 $\boldsymbol{H}$，经过无线信道作用后 Alice 得到信号 $\boldsymbol{D}$、$\boldsymbol{H}$，并利用 $\boldsymbol{D}$、$\boldsymbol{H}$ 生成长为 M 的认证响应 $\mathbf{RES}=[\mathrm{RES}_1\ \mathrm{RES}_2\ \cdots\ \mathrm{RES}_M]$。将高层密钥 $\boldsymbol{K}$ 映射为物理层符号向量 $\boldsymbol{X}$，则每个载波上的认证响应生成方式如式(1)所示。

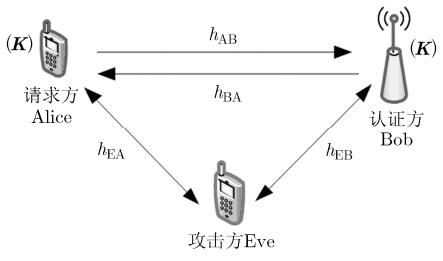

图 1 认证模型

$$\mathrm{RES}_n=\frac{X_n}{D_nH_n} \tag{1}$$

其中，X_n 为第 n 个密钥映射符号。随后，Alice 将 **RES** 发送给 Bob。由于信道具有互易性，**RES** 经过相同的信道 $\boldsymbol{H}$ 作用后，到达 Bob 端时信道作用被抵消，使 Bob 得到每个载波上得信号 X_n/D_n，则 Bob 可根据随机数组 $\boldsymbol{D}$ 得到密钥 $\boldsymbol{K}$，并进一步判断 Alice 是否合法。该方法利用 Alice-Bob 信道的私密性和唯一性掩藏密钥，其安全性基于攻击方无法获得合法信道信息的假设基础上；而一旦 Eve 掌握了 Alice-Bob 信道信息[14]，则可根据认证响应直接破解密钥。文献[11,12]也面临着类似的密钥泄露隐患。

因此，本文利用容错性的单向哈希方法生成认证响应，使得攻击方无法根据认证响应破解密钥。借鉴曲线匹配原理[15]，将无线信道特征及高层密钥进行组合，并等效为一条人工曲线上的采样点，随后采用容错性的哈希函数将曲线映射为低维的哈希矢量，仅经历相同信道且具有相同密钥的双方才能产生相同的认证响应。该哈希过程具有如下效果(证明见 4.1 节)：

(1)若双方的初始认证曲线差别足够小，则得到的认证响应差别也将足够小；

(2)具有单向性，攻击方无法根据认证响应破解密钥。

3　基于哈希方法的物理层认证

整个认证过程分为物理层挑战生成、哈希响应生成、曲线匹配、二进制假设检验 4 个步骤，如图 2 所示。本文描述的是单向认证过程，若需双向认证，只需进行两次单向认证或配备两个共享密钥即可。

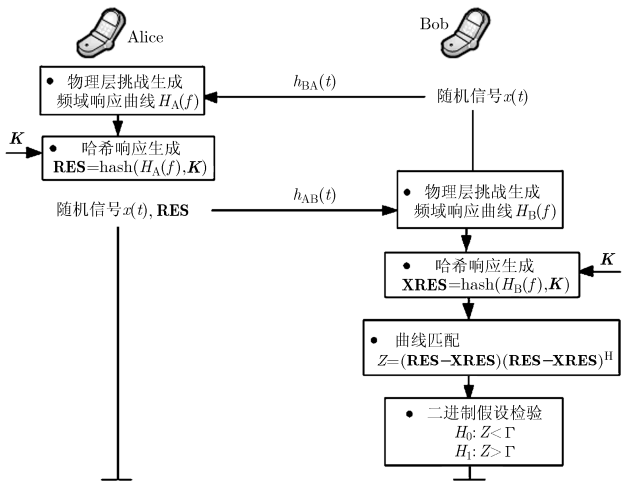

图 2 认证流程

3.1 物理层挑战生成

Bob 发送多载波随机信号 $x(t)$ 经过信道作用后到达 Alice 端。Alice-Bob 信道为多径衰落信道，可表示为 $h_{\mathrm{BA}}(t)=\sum_{n=1}^{T}c_n\mathrm{e}^{\mathrm{j}(2\pi f_n t+\vartheta_n)}$，其中 ϑ_n 为第 n 条路径的相位，c_n 为其衰减，T 为路径数。Alice 提取信道频率响应曲线得到 $H_{\mathrm{A}}(f)$，$H_{\mathrm{A}}(f)$ 可表示为

$$H_{\mathrm{A}}(f)=H(f)+N_{\mathrm{A}}(f) \tag{2}$$

其中，$H(f)$ 为 Alice-Bob 信道的真实频率响应，当路径数 T 趋于无穷时，$H(f)$ 可等效为服从 $(0,\sigma_H^2)$ 的复高斯随机过程[16]；$N_{\mathrm{A}}(f)$ 为噪声，服从 $(0,\sigma_N^2)$ 的复高斯分布。假设发射信号功率为 1，则信噪比 SNR 可表示为 $\mathrm{SNR}=\sigma_H^2/\sigma_N^2$。

3.2 哈希响应生成

Alice 将信道响应曲线 $H_{\mathrm{A}}(f)$ 及共享密钥 $\boldsymbol{K}$ 作为认证参数，通过物理层哈希过程生成认证响应，即

$$\mathbf{RES}=\mathrm{hash}\left(H_{\mathrm{A}}(f),\boldsymbol{K}\right) \tag{3}$$

包括以下步骤：

(1)对 $H_{\mathrm{A}}(f)$ 进行 N 点采样，得到采样值 $\boldsymbol{H}_{\mathrm{A}}$，假设采样间隔足够大，使每个采样值独立地服从 $(0,\sigma_H^2)$ 的复高斯分布。当 N 足够大时，$\boldsymbol{H}_{\mathrm{A}}$ 可用于表征 $H_{\mathrm{A}}(f)$。将高层共享密钥序列映射为服从 $(0,\sigma_H^2)$、长为 L 的复高斯序列 $\boldsymbol{X}$[17]，此时 $\boldsymbol{X}$ 类似于文献[18,19]中的人工指纹，不同密钥对应不同的指纹。将 $\boldsymbol{H}_{\mathrm{A}}$，$\boldsymbol{X}$ 进行组合，得到长度为 $(N+L)$ 的初始认证信息 **AUC**。

$$\mathbf{AUC}=[\boldsymbol{H}_{\mathrm{A}},\boldsymbol{X}] \tag{4}$$

则 **AUC** 可看做一条人工曲线。

(2)将初始认证信息 **AUC** 映射为长度为 M 的哈希矢量，即 $\mathbf{RES}=[P_1,P_2,\cdots,P_M]$，$N+L>M$，矢量中每一个元素 P_m 的计算方式如式(5)所示。

$$P_m=a\sum_{i=1}^{N+L}\mathrm{AUC}_i\cdot\cos\left(2\pi m(i-1)/(N+L)\right) \tag{5}$$

其中，$m=1,2,\cdots,M$。由于 $\boldsymbol{H}_{\mathrm{A}}$，$\boldsymbol{X}$ 的元素均服从 $(0,\sigma_H^2)$ 的复高斯分布，因此，$P_m\sim CN(0,a^2\eta\sigma_H^2)$，即每个元素服从均值为 0、方差为 $a^2\eta\sigma_H^2$ 的复高斯分布，其中 $\eta=\sum_{i=1}^{N+L}\left(\cos\frac{2\pi m(i-1)}{N+L}\right)^2=\frac{N+L}{2}$。**RES** 被用作认证响应，Alice 将其发送给 Bob，同时发送相同的随机信号给 Bob。

3.3 曲线匹配

Bob 采用和 Alice 相同的方法产生认证响应 **XRES**。假设 Bob 采样得到的信道特征为 $\boldsymbol{H}_{\mathrm{B}}$，由于信道的互易性，$\boldsymbol{H}_{\mathrm{B}}=\boldsymbol{H}_{\mathrm{A}}+\Delta\boldsymbol{H}$，其中 $\Delta H_i\sim CN(0,2\sigma_N^2)$，Bob 利用 $\boldsymbol{H}_{\mathrm{B}}$ 恢复 Alice 产生的认证响应 **RES**。

Bob 无法根据 $\boldsymbol{H}_{\mathrm{B}}$ 及 **RES** 得到密钥信息，而只能采用和 Alice 相同的方法生成认证响应 **XRES**，并和 **RES** 比较判断用户是否合法。Bob 利用共享密钥 $\boldsymbol{K}$ 及 $\boldsymbol{H}_{\mathrm{B}}$ 生成认证响应 $\mathbf{XRES}=(Q_1,Q_2,\cdots,Q_M)$，并利用测试统计参数 Z 判断 **RES** 和 **XRES** 两者的匹配程度，在这里我们采用距离作为判决参数，如式(6)：

$$Z=\boldsymbol{z}\boldsymbol{z}^{\mathrm{H}}=(\mathbf{RES}-\mathbf{XRES})(\mathbf{RES}-\mathbf{XRES})^{\mathrm{H}} \tag{6}$$

Z 用以衡量 Alice，Bob 产生的认证响应的匹配程度：若 **RES** 和 **XRES** 匹配度高，则 Z 较小；反之较大。

3.4 二进制假设检验

Bob 根据认证需求设置认证门限 Γ，并采用二进制假设检验根据统计参数 Z 判断用户是否合法：

$$\left.\begin{aligned}H_0: Z<\Gamma\\ H_1: Z>\Gamma\end{aligned}\right\} \tag{7}$$

假设 H_0 表示统计参数 Z 小于门限值 Γ，认证成功，此时用户合法并且无线信道未受到攻击；反之，当 Z 大于门限值 Γ 时，接收假设 H_1，此时用户为非法用户或者无线信道受到了攻击，认证失败。

对 Alice 认证成功后，Bob 可用另一共享密钥 $\boldsymbol{K}_2$ 及 $\boldsymbol{H}_{\mathrm{B}}$，采用上述的方法生成新的响应 $\mathbf{XRES}_2=\mathrm{hash}(H_{\mathrm{B}}(f),\boldsymbol{K}_2)$，并发送给 Alice, Alice 采用相同的方法对 Bob 进行鉴别。或者 Bob 可发起一次新的单向认证，从而实现双向鉴别。

4 性能分析

4.1 哈希证明

本节将证明文中所采用的哈希方法的两个性能：

(1)容错性： Alice, Bob 的初始认证信息为 $\{\mathrm{AUC}_{\mathrm{A}i}\}$, $\{\mathrm{AUC}_{\mathrm{B}i}\}$, $i\in[1,N+L]$，后 L 个元素为密钥，完全一致。令：$\mathrm{dist}_{\mathrm{AB}}=(\mathbf{AUC}_{\mathrm{A}}-\mathbf{AUC}_{\mathrm{B}})(\mathbf{AUC}_{\mathrm{A}}-\mathbf{AUC}_{\mathrm{B}})^{\mathrm{H}}$，则 $\mathrm{dist}_{\mathrm{AB}}=\sum_{i=1}^{N}\|\Delta H_i\|^2$，使用 $\mathrm{dist}_{\mathrm{AB}}$ 表征初始信息间的差别，则

$$\begin{aligned}z_m&=\mathrm{RES}_m-\mathrm{XRES}_m\\&=a\cdot\sum_{i=1}^{N+L}\left(\mathrm{AUC}_{\mathrm{A}i}\cdot\cos\frac{2\pi m(i-1)}{N+L}-\mathrm{AUC}_{\mathrm{B}i}\cdot\cos\frac{2\pi m(i-1)}{N+L}\right)\\&=a\cdot\sum_{i=1}^{N+L}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot\left(\mathrm{AUC}_{\mathrm{A}i}-\mathrm{AUC}_{\mathrm{B}i}\right)\right)\\&=a\sum_{i=1}^{N}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot\left(\Delta H_i\right)\right)\end{aligned} \tag{8}$$

则：$z_m z_m^{\mathrm{H}}\le a^2\sum_{i=1}^{N}\|\Delta H_i\|^2=a^2\mathrm{dist}_{\mathrm{AB}}$，因此，$Z\le$

$a^2M\cdot \mathrm{dist}_{\mathrm{AB}}$。只要初始认证信息差别 $\mathrm{dist}_{\mathrm{AB}}$ 足够小，则产生的认证响应的差距 Z 也将足够小。因此，该哈希方法并不需要 Alice, Bob 双方的认证信息完全一致，只要其差距在允许范围内均可认证成功，具有容错性，符合物理层无线信道有噪性的特点。如图 3 为该方法的容错性能，门限值 Γ 越大，信噪比越高，方法的容错性越好。

(2)单向性：

$$\left.\begin{aligned} P_1=&r_{11}H_1+\cdots+r_{1N}H_N+r_{1(N+1)}X_1\cdots\\ &+r_{1(N+L)}\cdot X_L\\ \vdots\quad&\vdots\qquad\qquad\qquad\qquad,\ (N+L)>M\\ P_{\mathrm{M}}=&r_{M1}H_1+\cdots+r_{MN}H_N+r_{M(N+1)}X_1\cdots\\ &+r_{M(N+L)}\cdot X_L \end{aligned}\right\} \tag{9}$$

产生认证响应的哈希方法经过简化后可表示为如式(9)所示，式(9)方程组具有 M 个等式，$N+L$ 个未知数，且 $(N+L)>M$，为欠定方程组，方程组的解空间为无穷，根据信道信息 $\boldsymbol{H}$ 和 $\boldsymbol{K}$ 可以唯一的确定认证响应 **RES**，而无法根据 **RES** 得到 $\boldsymbol{H}$ 和 $\boldsymbol{K}$。因此，该哈希方法具有单向性。

4.2 安全性分析

本文主要讨论 Eve 两种攻击方式：主动攻击和被动攻击。在被动攻击中，Eve 主要对 Alice-Bob 间的认证数据进行窃听，期望通过窃听数据破解用户密钥；在主动攻击中，Eve 采用重放、中间人及伪造等攻击方式发起攻击。

4.2.1 被动攻击　文献[8–12]的安全性基于攻击方无法获得 Alice-Bob 间的信道特征的假设基础上，一旦 Eve 获取了合法信道信息[14]，Eve 可根据认证响应直接窃取密钥。

本文利用哈希方法生成认证响应，将无线信道特征和密钥信息等效为一条曲线，并经过哈希过程后生成认证响应，仅经历了相同的信道且具有相同密钥的双方才可得到相同的认证响应。由于该哈希函数的实质为欠定方程组，Eve 无法根据低维的认证响应信息 **RES** 得到曲线信息；即使 Eve 获取了 Alice-Bob 信道信息 $\boldsymbol{H}$，只要保证 $L>M$, Eve 依旧无法破解密钥。

4.2.2 主动攻击　安全性由虚警率 α，攻击率 β 描述。虚警率 α 为 Alice 认证失败的概率，即 Bob 误判 Alice 非法的概率，这是由噪声等因素导致双方提取的信道特征不一致造成的；攻击率 β (也可称作漏检率)代表 Eve 攻击成功的概率，此时 Bob 没有检测出 Eve，如式(10)：

$$\left.\begin{aligned} \alpha&=P_{H_0},\ Z>\Gamma\\ \beta&=P_{H_1},\ Z_{\mathrm{E}}<\Gamma \end{aligned}\right\} \tag{10}$$

其中，Z_{E} 为 Eve 发起攻击时 Bob 端得到的统计参数，当 $Z_{\mathrm{E}}<\Gamma$ 时，Eve 攻击成功。Eve 采用不同的攻击方式时，Bob 方会得到不同的 Z_{E} 统计值，在后面将分别讨论。当请求方为 Alice 时，式(8)已经给出：$z_m=a\sum_{i=1}^{N}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot(\Delta H_i)\right)$，则 $z_m\sim CN(0,a^2\eta_1\cdot 2\sigma_N^2)$，其中，$\eta_1=\sum_{i=1}^{N}\left(\cos\frac{2\pi k(i-1)}{N+L}\right)^2$。令 $\lambda_1=a^2\eta_1\sigma_N^2$，则 Z/λ_1 服从自由度为 $2M$ 的 χ^2 分布，即 $\frac{Z}{\lambda_1}\sim\chi^2(2M)$。对于特定的门限值 Γ，虚警率 α 为

$$\alpha=\mathrm{P}\{Z>\Gamma\mid H_0\}=\mathrm{P}\left\{\frac{Z}{\lambda_1}>\frac{\Gamma}{\lambda_1}\middle|H_0\right\}=1-\mathrm{F}_{\chi^2_{2M}}\left(\frac{\Gamma}{\lambda_1}\right) \tag{11}$$

同理，对于特定的虚警率 α，相应的门限值可表示为

$$\Gamma=\lambda_1\mathrm{F}^{-1}_{\chi^2_{2M}}(1-\alpha) \tag{12}$$

(1)重放攻击：重放攻击中，Eve 获取了 Alice 第 t 次认证响应 **RES**$[t]$，并发送给 Bob 期望通过其认证。但由于信道具有时变性，只要 Eve 在大于信道相关时间的时刻发起攻击，Bob 即会产生不同的认证响应。假设第 t 次、$t+1$ 次认证 Alice, Bob 提取的信道特征分别为 $H_{\mathrm{A}i}[t]$，$H_{\mathrm{B}i}[t+1]$，则 $t+1$ 次认证 Bob 得到的测试统计参数为

$$z_{\mathrm{E},m}=a\sum_{i=1}^{N}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot(H_{\mathrm{B}i}[t+1]-H_{\mathrm{A}i}[t])\right) \tag{13}$$

其中，$(H_{\mathrm{B}i}[t+1]-H_{\mathrm{A}i}[t])\sim CN(0,2\sigma_H^2)$，则 $z_{\mathrm{E},m}\sim CN(0,a^2\eta_1\cdot 2\sigma_H^2)$，令 $\lambda_2=a^2\eta_1\sigma_H^2$，则 $\frac{Z_{\mathrm{E}}}{\lambda_2}\sim\chi^2(2M)$。若 Eve 期望攻击成功，则需 $Z_{\mathrm{E}}<\Gamma$，即 $\frac{Z_{\mathrm{E}}}{\lambda_2}<\frac{\Gamma}{\lambda_2}$，漏检率或攻击率 β 可表示为

$$\beta=\mathrm{P}\{Z_{\mathrm{E}}<\Gamma\mid H_1\}=\mathrm{F}_{\chi^2_{2M}}\left(\frac{\lambda_1}{\lambda_2}\mathrm{F}^{-1}_{\chi^2_{2M}}(1-\alpha)\right) \tag{14}$$

图 4，图 5 仿真了攻击率随着信噪比及虚警率变化的关系曲线。图 4 为虚警率为 0.005，不同认证响应长度下攻击率随信噪比的变化曲线；图 5 为攻击率随虚警率的变化曲线。虚线为式(14)计算出的理论值，实线为蒙特卡洛法得到的仿真值，可以发现理论值和仿真值吻合度较高，攻击率随着信噪比的增大而减小；同时，认证响应长度越大，攻击率越小。当认证响应采用 40 位，SNR = 5 dB 时，可实现攻击率趋近 10^{-5}。

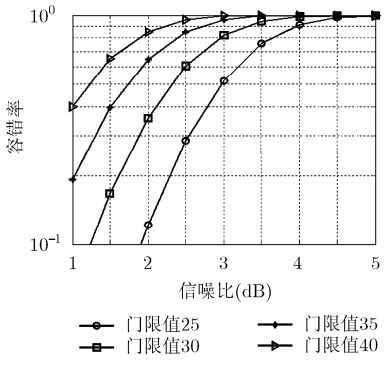

图 3 哈希方法的容错性能

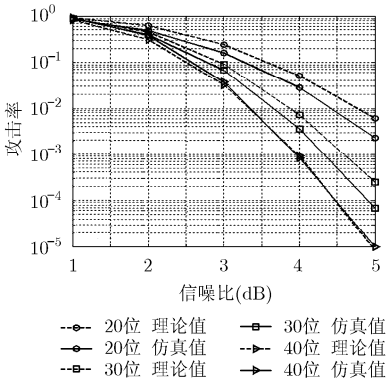

图 4 不同信噪比下的攻击性能(α=0.005)

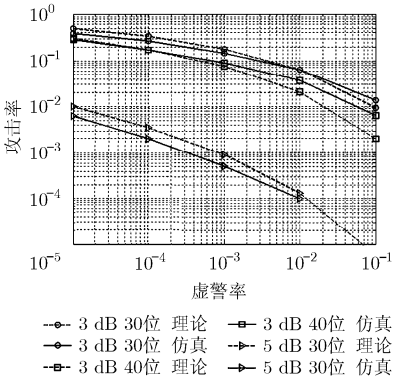

图 5 不同虚警率条件下的攻击率

(2)中间人攻击：中间人串接在 Alice, Bob 间，期望通过“透明”转发认证数据实现攻击。此时，Alice 和 Bob 提取的信道特征分别为 $\boldsymbol{H}_{\mathrm{EA}}$，$\boldsymbol{H}_{\mathrm{EB}}$，且互不相关。此时，Bob 得到的测试统计参数为

$$z_{\mathrm{E},m}=a\sum_{i=1}^{N}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot\left(H_{\mathrm{EB}i}-H_{\mathrm{EA}i}\right)\right) \tag{15}$$

其中，$(H_{\mathrm{EB}i}-H_{\mathrm{EA}i})\sim CN(0,\sigma_{\mathrm{EA}}^2+\sigma_{\mathrm{EB}}^2)$，假设 $\sigma_{\mathrm{EB}}^2=\sigma_{\mathrm{EA}}^2=\sigma_H^2$，则 $z_{\mathrm{E},m}\sim CN(0,a^2\eta_1\cdot 2\sigma_H^2)$。因此，中间人攻击成功的概率与重放攻击中式(14)相同，性能仿真同图 4，图 5。

当中间人足够强大时，中间人可建立一条等效信道，使得 Alice, Bob 双方提取的信道特征一致。即：$H_{\mathrm{AB}i}=H_{\mathrm{BA}i}=H_{\mathrm{EB}i}\cdot H_{\mathrm{EA}i}$。此时 Alice, Bob 认证成功，中间人可得到认证响应，但由于认证响应由哈希方法产生，中间人不能根据响应值破解密钥。

(3)伪造攻击：在伪造攻击中，Eve 伪造认证数据期望通过 Bob 的认证。

(a)Eve 不知道 Alice-Bob 信道时，Eve 可伪造合法信道特征及密钥，或直接伪造认证响应发起攻击。

当 Eve 伪造信道特征和密钥时，

$$z_{\mathrm{E},m}=a\sum_{i=1}^{N+L}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot\left(\mathrm{AUC}_{\mathrm{E}i}-\mathrm{AUC}_{\mathrm{B}i}\right)\right) \tag{16}$$

其中，$(\mathrm{AUC}_{\mathrm{E}i}-\mathrm{AUC}_{\mathrm{B}i})\sim CN(0,2\sigma_H^2)$，则 $z_{\mathrm{E},m}\sim CN(0,2a^2\eta\sigma_H^2)$，令 $\lambda_3=a^2\eta\sigma_H^2$，则 $\dfrac{Z_{\mathrm{E}}}{\lambda_3}\sim\chi^2(2M)$。

当 Eve 直接伪造认证响应时，$z_{\mathrm{E},m}=\mathrm{RES}_{\mathrm{E},m}-\mathrm{XRES}_m\sim CN(0,2a^2\eta\sigma_H^2)$，和 Eve 伪造信道特征和密钥具有相同的效果，此时攻击率 β 为

$$\beta=\mathrm{P}\left\{Z_{\mathrm{E}}<\Gamma\mid H_1\right\}=\mathrm{F}_{\chi_{2M}^2}\left(\frac{\lambda_1}{\lambda_3}\mathrm{F}_{\chi_{2M}^2}^{-1}(1-\alpha)\right) \tag{17}$$

图 6 为虚警率为 0.005 时的攻击率性能：攻击率随着信噪比和响应长度的增大而降低，在 SNR = 3 dB 时，采用 40 位响应值可实现攻击率小于 10^{-5}。

图 7 为攻击率随虚警率的变化曲线，可以发现，攻击率随着虚警率的增大而减小，SNR=1 dB 时，可实现 $\alpha,\beta\sim(10^{-3},10^{-2})$；SNR=3 dB 时，$\alpha,\beta\sim(10^{-5},10^{-4})$。

(b)当 Eve 窃取了 Alice-Bob 信道信息时，Eve 可选择伪造密钥或伪造认证响应发起攻击，伪造认证响应时，性能和式(17)一致。当 Eve 伪造密钥时，

$$z_{\mathrm{E},m}=a\sum_{i=N+1}^{N+L}\left(\cos\frac{2\pi m(i-1)}{N+L}\cdot\left(K_{\mathrm{E}(i-N)}-K_{\mathrm{B}(i-N)}\right)\right) \tag{18}$$

则 $z_{\mathrm{E},m}\sim CN(0,a^2(\eta-\eta_1)\cdot 2\sigma_H^2)$，令 $\lambda_4=a^2(\eta-\eta_1)\sigma_H^2$，则 $\dfrac{Z_{\mathrm{E}}}{\lambda_4}\sim\chi^2(2M)$，此时攻击率为

$$\beta=P\left\{Z_{\mathrm{E}}<\Gamma\mid H_1\right\}=F_{\chi_{2M}^2}\left(\frac{\lambda_1}{\lambda_4}F_{\chi_{2M}^2}^{-1}(1-\alpha)\right) \tag{19}$$

图 8 为 Eve 获取了合法信道信息时，不同认证响应长度条件下，本文所提机制和文献[8]PHY-CRAM 机制的攻击率对比图。对于 PHY-CRAM 机制，认证响应长度即为密钥长度。可以发现对于 PHY-CRAM 机制，密钥长度对认证性能的影响不是太大，这是因为一旦 Eve 获得 Alice-Bob 信道信息，则可直接获得密钥。本文采用哈希方法生成认证响应，攻击方无法根据认证响应破解密钥，而仅能通过猜测伪造密钥生成认证响应。当 SNR = 4 dB 时，本文机制可实现攻击率小于 10^{-5}，而对于 PHY-CRAM 机制，攻击率约为 0.5。

当 Eve 获取了某次认证的认证响应及信道信息时，Eve 可通过式(20)得到关于密钥的信息。

$$r_{i(N+1)}X_1\cdots+r_{i(N+L)}\cdot X_L=P_i-r_{i1}H_1+\cdots+r_{iN}H_N \tag{20}$$

这时，可采取改变采样数 N 或密钥映射长度 L 的方法，使得每次认证的加权系数 r_{im} 值均不同，由于 Eve 不知道完整的 $\boldsymbol{X}$，因此无法产生正确的认证响应。此时，Eve 依然只能伪造密钥信息，其性能同式(19)。

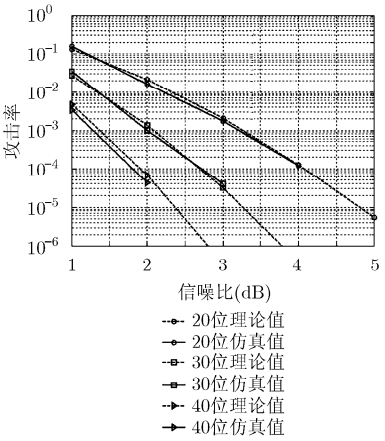

图 6 不同信噪比条件下的攻击率(α=0.005)

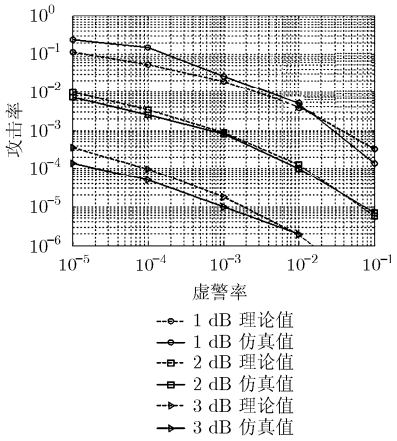

图 7 不同虚警率条件下的攻击率(M=30)

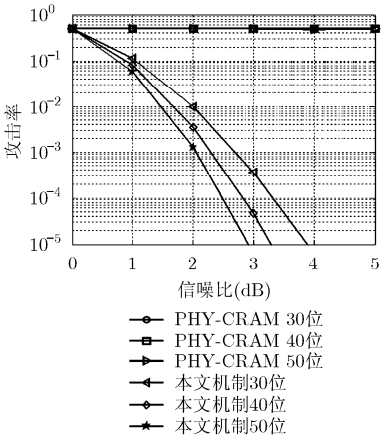

图 8 不同响应长度下的攻击性能

但是，当攻击方足够强大，获取了多次合法信道信息及相应的认证响应时，其可能会联合多次认证数据破解密钥，此时密钥的条件熵随着认证数据的观测数减小，即 $H(\boldsymbol{K}\,|\,(\mathbf{RES}_1,\boldsymbol{H}_1),(\mathbf{RES}_2,\boldsymbol{H}_2),\cdots,(\mathbf{RES}_n,\boldsymbol{H}_n))$ 随着 n 的增加而减小。当 n 足够大时，攻击方能以较高的概率破解密钥。因此，在实际应用时当密钥的条件熵降低于特定门限时，可以考虑更换密钥；或者，该方法可以和高层认证结合，物理层无线信道为高层认证提供信息熵，即使信道信息遭受泄露，由于高层认证每次的认证数据不一致，攻击方也无法破解密钥。

4.3 开销分析

本文采用哈希方法防止了文献[8]中 PHY-CRAM 机制的密钥泄露问题，但是开销有所增加。本文所提机制主要增加了乘法的开销，产生认证响应需 $M(N+L)$ 次，而 PHY-CRAM 仅需 N 次除法。但由于本文所需的乘法均是常数与复数的乘法，计算复杂度较低。另外，本文所提机制的有效性仅为 PHY-CRAM 的 M/L，因为长度为 L 的密钥信息，最终只生成了长为 M 的认证响应；但同时也使得本文机制的带宽消耗为 PHY-CRAM 的 M/L。因此，本文机制使用计算复杂度和有效性换取了带宽效率和安全。

4.4 实用性分析

上面的理论分析和仿真中，我们均假设多径数目趋于无穷大使得信道特性服从 $(0,\sigma_H^2)$ 的复高斯过程，但在实际通信场景中，路径数可能有限，因此下面验证所提方法在不同路径数 N_i 条件下的认证性能。如图 9 所示，采用文献[20]给出的散射仿真环境，认证方 Bob(一般为基站)位置较高，因此，Alice 经历的散射簇主要集中在其周围，散射簇数目随机，且位置随机；Eve 在离 Alice 附近足够近的地方但相距大于 $\lambda/2$，使其经历的散射簇和 Alice 一致，但经历的信道特性和 Alice 的不相关。Eve 也采用相同的方法提取信道特征，并伪造密钥生成认证响应，发送给 Bob 期望通过其认证。

如图 10 所示为认证响应长度为 30，$\alpha=5\times10^{-7}$ 时，不同路径数下的认证性能。可以发现，路径数越少，Eve 攻击成功率越低，4.2.2 节所得到的理论结果为最差情况下的认证性能。这是因为路径数越低，合法双方提取的信道特性对抗噪声的能力越大，而攻击方伪造密钥成功的概率不变，因此攻击成功率越低。另外，当路径数 $N_i\geq10$ 时，性能趋于路径数无穷时的认证性能，这是因为，当路径数 ≥10 时，信道已经足以接近瑞利分布，这和文献[16]的结论是契合的。

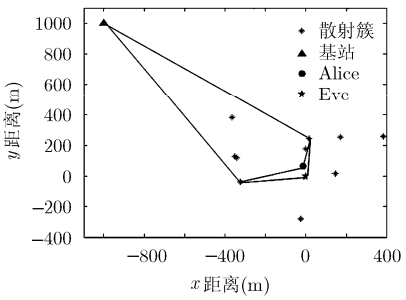

图 9 仿真环境示意图

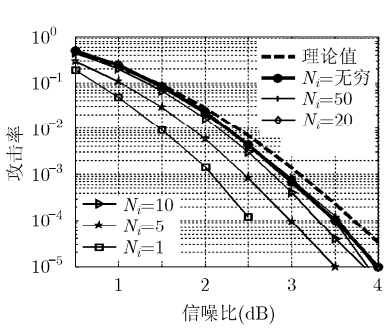

图 10　不同路径数下的认证性能

从实用角度看，未来 5G 系统将是一个具有各种低功率节点的异构融合网，其中，物联网、车载网等对时延和能耗要求比较高的网络需要轻量级的认证，高层认证开销太大，本文机制仅在物理层实现，且只涉及到简单的乘法运算，认证开销相对于高层认证减小，可以为这些网络的认证提供一种思路和参考。

5 结束语

针对现有物理层挑战-响应认证面临的密钥泄露隐患，本文提出了一种基于哈希方法的物理层认证机制。借鉴曲线匹配原理，将无线信道信息和密钥等效为一条人工曲线，并利用容错性的单向哈希函数将曲线映射为低维的认证响应，仅经历了相同的信道并具有相同密钥的双方才能产生相同的认证响应，且攻击方无法根据该响应恢复密钥信息，从而防止密钥信息泄露。由于认证仅在物理层实现，相比于传统的高层认证可减小认证时延及计算开销，且无线信道的私有性和时变性可防止认证遭受重放、中间人及伪造等攻击。但由于物理层认证的安全基于无线信道的私有性，因此，保证无线信道特征不被攻击方获取至关重要。本文所提机制为未来 5G 轻量级的认证及跨层认证的实现方法提供了一种新的思路。

参 考 文 献

[1] JIN Cao, MA Maode, LI Hui, *et al*. A survey on security aspects for LTE and LTE-A networks[J]. *IEEE Communications Surveys & Tutorials*, 2014, 16(1): 283–302. doi:10.1109/SURV.2013.041513.00174.

[2] PATWARI N and KASERA S K. Temporal link signature measurements for location distinction[J]. *IEEE Transactions on Mobile Computing*, 2011, 10(3): 449–462. doi: 10.1109/TMC.2010.189.

[3] JORSWIECK E, TOMASIN S, and SEZGIN A. Broadcasting into the uncertainty: authentication and confidentiality by physical-layer processing[J]. *Proceedings of the IEEE*, 2015, 103(10): 1702–1724. doi: 10.1109/JPROC.2015.2469602.

[4] ZENG K, GOVINDAN K, and MOHAPATRA P. Non-cryptographic authentication and identification in wireless networks[J]. *IEEE Wireless Communications*, 2010, 17(5): 56–62. doi: 10.1109/MWC.2010.5601959.

[5] DEMIRBAS M and SONG Y. An RSSI-based scheme for Sybil attack detection in wireless sensor networks[C]. Proceedings of the 2006 International Symposium on World of Wireless, Mobile and Multimedia Networks, New York, 2006: 564–570. doi: 10.1109/WOWMOM.2006.27.

[6] 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.

[7] LIU Jiazi and WANG Xianbin. Physical layer authentication enhancement using two-dimensional channel quantization[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(6): 4171–4182. doi: 10.1109/TWC.2016.2535442.

[8] 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.

[9] 张继明. 无线网络中物理层身份认证研究[D]. [硕士论文]. 华中科技大学, 2013.
ZHANG Jiming. Research on physical-layer identity authentication in wireless networks[D]. [Master dissertation], Huazhong University of Science and Technology, 2013.

[10] DU Xianru, SHAN Dan, ZENG Kai, *et al*. Physical layer challenge-response authentication in wireless networks with relay[C]. IEEE International Conference on Computer Communications, Orlando, 2014: 1276–1284. doi: 10.1109/INFOCOM. 2014.6848060.

[11] WU Xiaofu and ZHEN Yan. Physical-layer authentication for multi-carrier transmission[J]. *IEEE Communications Letters*, 2015, 19(1): 74–77. doi: 10.1109/LCOMM.2014.2375191.

[12] WU Xiaofu, ZHEN Yan, CONG Ling, *et al*. A physical-layer authentication assisted scheme for enhancing 3GPP authentication[OL]. http://arxiv.org/abs/1502.07565, 2015.

[13] JAKES W C and COX D C. Microwave Mobile Communications[M]. New Jersey, Wiley-IEEE Press, 1994: 13–39.

[14] TRAPPE W. The challenges facing physical layer security[J]. *IEEE Communications Magazine*, 2015, 53(6): 16–20. doi: 10.1109/MCOM.2015.7120011

[15] 吕科, 耿国华, 周明全. 基于哈希方法的空间曲线匹配[J]. 电子学报, 2003, 31(2): 294–296. doi: 10.3321/j.issn:0372-2112.2003.02.037.
LÜ Ke, GENG Guohua, and ZHOU Mingquan. Matching of 3D curve based on the hash method[J]. *Acta Electronica Sinica*, 2003, 31(2): 294–296. doi: 10.3321/j.issn:0372-2112.2003.02. 037.

[16] PATZOLD M. Mobile Radio Channels[M]. New York, John Wiley & Sons, 2012: 55–147.

[17] SWAMINATHAN A, MAO Yinian, and WU Min. Robust and secure image hashing[J]. *IEEE Transactions on Information Forensics and Security*, 2006, 1(2): 215–230. doi: 10.1109/TIFS.2006.873601.

[18] GOERGEN N, CLANCY T C, and NEWMAN T R. Physical layer authentication watermarks through synthetic channel emulation[C]. 2010 IEEE Symposium on New Frontiers in Dynamic Spectrum, Singapore, 2010: 1–7. doi: 10.1109/DYSPAN.2010.5457897.

[19] GOERGEN N, LIN W S, LIU K J, *et al*. Authenticating MIMO transmissions using channel-like fingerprinting[C]. Global Telecommunications Conference, Miami, 2010: 1–6. doi: 10.1109/GLOCOM.2010.5684218.

[20] FONTAN F P and ESPIEIRA P M. Modeling the Wireless Propagation Channel: A Simulation Approach with Matlab[M]. New Jersey, John Wiley & Sons, 2008: 105–111.

季新生： 男，1968 年生，教授，博士生导师，研究方向为移动通信、信息安全.

杨 静： 女，1991 年生，硕士生，研究方向为移动通信、物理层安全.

黄开枝： 女，1973 年生，教授，博士生导师，研究方向为移动通信、物理层安全.

易 鸣： 男，1986 年生，讲师，博士，研究方向为移动通信、信息安全.