基于标签信号的物理层安全认证

宋华伟 金 梁* 张胜军
(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要：该文提出一种基于叠加标签信号进行认证的新方法。利用合法通信双方预先共享密钥和信道具有短时互易性的优势，在发送方利用扩谱码和量化的信道值生成标签信号，并与通信信号叠加发送，在接收方能够检测并鉴别标签信号，而且不影响通信信号的正常解调。这种方法不需要复杂的密码算法，减小了通信过程中的计算量，而且能够有效地防范被动窃听和主动攻击。仿真结果表明，该方法有较高的实用价值。

关键词：物理层安全；标签信号；认证
中图分类号： TN918.91 **文献标识码**： A **文章编号**：1009-5896(2018)05-1066-06
DOI: 10.11999/JEIT170672

Physical Layer Authentication Based on Tag Signal

SONG Huawei JIN Liang ZHANG Shengjun
(*National Digital Switching System Engineering & Technological R&D Center*, *Zhengzhou* 450002, *China*)

Abstract: This paper proposes a new method of authentication based on piling up tag signal. Using the advantage of legality sides sharing a private key and having coherent channel state information in short time, the sender produces a tag signal from spread frequency code and measures channel state information, then overlaps the tag signal on the communicational signal, the receiver can detect the correct tag signal and demodulate the communicational signal. This method avoids using complex cryptographic algorithm, reduces the amount of calculation, and prevents passive eavesdropping and active attack effectively. Simulation results show that this method has high use value.

Key words: Physical layer security; Tag signal; Authentication

1 引言

认证技术是信息安全的重要组成部分，而且在某些情况下，信息认证显得比信息保密更为重要[1]。一般来说，认证包括用户身份认证和消息认证两个方面。前者用于鉴别用户身份，后者用于保证通信的不可抵赖性和传递信息的完整性。在现有的移动通信系统标准中，规定了身份认证和消息认证可使用的密码算法，而对实时性很高的业务数据，基于计算量和能耗的考虑还没有规定认证方法。也就是说，现有系统中的认证实现是在高层完成的，利用密码算法计算出难以被仿冒的数值结果。例如在 USIM 卡中存储了用户的身份信息、根密钥和认证密码算法，这样就实现密钥预先分配。这种方法是根据有线通信认证方法衍生而来，窃听者能够获得传输的消息内容，其安全性完全依赖于密码算法的破译难度。Simmons[2]总结了这种认证的安全模型，利用信息论的方法进行了分析，指出认证攻击的成功率与密钥的长度也就是空间大小有关，攻击者的成功率下界为$1/\sqrt{|K|}$，这里$|K|$是指密钥 K 所在集合空间中元素的个数，这比猜测密钥的成功率要高很多。Maurer[3]进一步证明了攻击成功率还与认证次数有关，而且还会随着次数的增加而增大。另外，这种认证方法不能防范中间人转发和重放攻击，往往需要求助于加密技术和上层消息计数或者随机数的方法。

近年来兴起的物理层安全技术[4]利用无线信道的唯一性、互易性、多样性等特点，为信息安全特别是认证提供了新的方法[5,6]，已经成为认证技术新的研究热点[7–13]。Xiao Liang 等人[14,15]利用信道特征与位置强相关且短时间内不会突变的特点，提出了利用“信道指纹”进行认证的方法，文献[16]利用信道特征相似性进行假设检验的方法，但是这类方法需要高层使用密码算法完成首次身份认证。最近出现的物理层“激励-响应”认证方法[17,18]在无线信道的幅度和相位信息中隐藏密钥和认证信息，可用于实现用户初次接入网络时的身份认证增强，但该

收稿日期：2017-07-07；改回日期：2017-12-21；网络出版：2018-01-23
*通信作者：金梁 liangjin@263.net
基金项目：国家 863 计划项目(2015AA01A708)
Foundation Item: National 863 Program of China (2015AA01A708)

类方法不适用于消息认证。在信号的频谱上添加“水印”信息也是一个很好的方法，已经被用于密钥生成[19]和无线设备频谱身份识别和确定干扰方面[20]。除此之外，文献[21]提出联合物理层和高层的跨层认证方案。

本文提出一种利用标签信号在物理层进行认证的方法。在不影响通信信号的前提下，生成标签信号与通信信号叠加，形成信号“水印”。标签信号能够实现与共享密钥和信道的双重“绑定”，能够抵抗多种攻击。这种方法不需要复杂的密码算法，安全性分析和仿真结果表明能够达到较高的认证成功率和较低的误判率。从信号传输的角度来看，这种方法利用了信号层面的标签，从而节省了高层的消息认证标签，提高了传输效率，该方法实现身份认证和消息认证的安全性提升，并且能够解决业务数据难以认证的问题。

2　系统模型

系统模型示于图 1。Alice 和 Bob 分别是合法通信的发送方和接收方并预先分配了密钥 K, Eve 作为恶意的第三方，知道通信使用的时隙、频段、调制方式等信道参数。Alice 与 Bob 之间的信道为 h_{AB}，Alice 与 Eve 之间的信道为 h_{AE}，Eve 与 Bob 之间的信道为 h_{EB}。假设 Alice 发出信号 x, Bob 收到信号 y 而 Eve 收到信号 z，则有

$$y = x * h_{\mathrm{AB}} + n_{\mathrm{AB}} \tag{1}$$

$$z = x * h_{\mathrm{AE}} + n_{\mathrm{AE}} \tag{2}$$

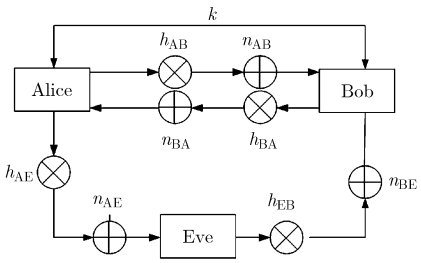

图 1 系统模型

其中，n_{AB}, n_{AE} 分别是 Alice 与 Bob 之间、Alice 与 Eve 之间的噪声，两者相互独立，$*$ 表示卷积运算。在 TDD(时分双工)的系统中，在一段短的时间内通信双方的信道参数基本不变，可以认为具有短时互易性，即有 $h_{\mathrm{AB}} \approx h_{\mathrm{BA}}$。Eve 可能会接收 Alice 发出的信号，也会冒充 Alice 向 Bob 发出信号，并试图使 Bob 接受。

3　基于标签信号认证的方法

在传统的通信系统中，为了实现消息认证，一般在高层使用密码算法计算一个认证码(Message Authentication Code, MAC)。由于合法双方共享密钥，同样的算法生成的认证码必然相同，在接收方通过比对认证码即可判断消息是否来自合法发送方，这种方法相当于在消息层面为传输的信息打上了一个供认证的标签。本文提出在物理层使用标签信号实现认证：Alice 产生标签信号，并与通信信号在时域进行叠加，在接收端既能正常接收并解调通信信号，又可同时检验标签信号。由于标签信号由共享密钥和具有互易性的信道量化值经过扩谱序列共同产生，Alice 和 Bob 能够生成相同的标签信号，标签信号和通信信号在信道上实现了复用。由于扩谱增益的存在使得在通信信号的干扰之下仍然能够获得相关峰，从而实现对信息源的认证，而 Eve 不知道具体使用的扩谱码，只能靠猜测的方法来仿冒 Alice 身份伪造信号，在有限次的攻击次数内很难成功，从而保证了安全性。

3.1 标签信号认证流程

利用标签信号认证的流程如图 2 所示，共有 5 个步骤。

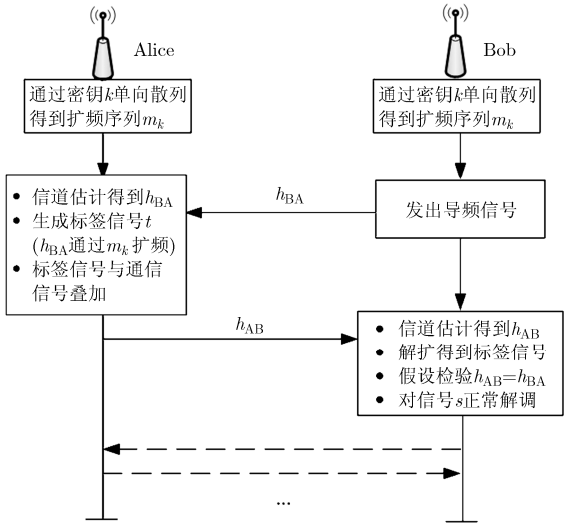

图 2 标签信号认证流程图

步骤 1　准备阶段：　在通信开始之前，Alice 和 Bob 预先分配了共享密钥 K 及公共的扩谱序列集合 $\{m_i\}, i = 0,1,\cdots, N$，设密钥 K 的集合空间数为 $|K|$，满足 $N>|K|$。这里选择扩谱序列需要具有良好的自相关性和互相关性，线性和非线性序列均可，使用 m 序列举例是因为实现方便且在通信系统中较为常用。Alice 和 Bob 采用相同的哈希函数将 K 映射到同一个扩谱序列 m_k，单向散列函数应该具有如下性质：

(1)散列值的随机性没有明显的统计特征；

(2)运算量小，可以快速实现；

(3)单向性，根据散列结果逆向获得输入很困

难，防止密钥作为私密信息泄露；

(4)抗碰撞性，要确保找到具有相同散列值的另外一个输入是非常困难的，也就是为了防止 Eve 字典攻击。

常用的单向散列函数有 MD5, SHA, HMAC, CRC 等，这里选用 SHA-1 算法完成共享密钥到 m 序列的映射，具有良好的安全性和较低的计算复杂度，符合上述要求，且在使用时引入初始化向量(Initialization Vector, IV)并保持更新，保证在密钥不变的情况下可以改变所使用的 m 序列。

步骤 2 Bob 发送导频： 由 Bob 向 Alice 发送导频信号，Alice 测量信道 h_{BA} 并量化得到估计值 $\hat{h}_{\mathrm{BA}}$。由于噪声的影响，$\hat{h}_{\mathrm{BA}}$ 是真实信道 h_{BA} 的有噪版本，即：$\hat{h}_{\mathrm{BA}} = h_{\mathrm{BA}} + n_{\mathrm{BA}}$，且 $h_{\mathrm{BA}} \sim \mathrm{CN}\left(0, \sigma_h^2\right)$，$n_{\mathrm{BA}}$ 服从均值为 0，方差为 σ_n^2 的复高斯分布，即 $n_{\mathrm{BA}} \sim \mathrm{CN}\left(0, \sigma_n^2\right)$，则信噪比 $\mathrm{SNR} = \sigma_h^2 / \sigma_n^2$。

步骤 3 Alice 生成标签信号，并与通信信号叠加发送： Alice 使用序列 m_k 对 $\hat{h}_{\mathrm{BA}}$ 进行扩谱，得到标签信号 s_t，并把标签信号和要发送的通信信号进行叠加发送给 Bob，也就是

$$s_t = m_k \hat{h}_{\mathrm{BA}} \tag{3}$$

$$x = s_s + s_t \tag{4}$$

Bob 收到的信号为

$$y = \left(s_s + s_t\right) * h_{\mathrm{AB}} + n_{\mathrm{AB}} \tag{5}$$

同时发送的还有导频信号。

步骤 4 Bob 接收信号并检验标签： Bob 利用导频符号进行信道估计，同样的等概率量化得到估计值 $\hat{h}_{\mathrm{AB}}$，并计算出标签信号 $s_t^{'} = m_k \hat{h}_{\mathrm{AB}}$。Bob 接收信号 y，根据 m_k 对信号 y 进行解扩处理，根据扩频通信原理，通信信号的叠加在较高扩谱增益下仍然可以正常解扩，解扩后得到 $\hat{h}_{\mathrm{AB}}$。把接收信号减去标签信号 $s_t^{'}$ 后继续进行解调。这里有两种备择假设：

H_0：标签信号 s_t 是 Alice 所发；

H_1：标签信号 s_t 不是 Alice 所发。

相应地，由于 $\hat{h}_{\mathrm{AB}}$ 和 $\hat{h}_{\mathrm{BA}}$ 均为复数，由于信道噪声的影响，双方量化得到的信道特征可能不完全一致，令 $\hat{h}_{\mathrm{AB}}$ 和 $\hat{h}_{\mathrm{BA}}$ 量化后得到的比特串为 $\mathrm{Str}\left(\hat{h}_{\mathrm{AB}}\right)$ 和 $\mathrm{Str}\left(\hat{h}_{\mathrm{BA}}\right)$，这里定义量化的差异率为 ρ，即为逐一比特对比两个串相同的比特个数与整个串比特个数的百分比。选取检验门限为 Γ，在一般情况下可选择常数，比如令 $\Gamma = 99\%$，则检验准则为：原假设 H_0:$\rho \geq \Gamma$；备择假设 $H_1 : \rho < \Gamma$。

步骤 5 Alice, Bob 连续通信： 认证成功后，Alice 和 Bob 可以连续地进行数据通信，保持导频信号的正常发送与信道估计。如果通信过程中出现了较长间隔，测量到的信道不具备互易性条件，可以返回步骤 2 进行新一轮认证。比如 TDD 系统中一般相邻的的帧之间信道满足互易性，如果间隔时间超过了几个数据帧的长度，就可以认为信道产生了改变。

3.2 标签信号认证的性能

选取 BPSK 调制为例进行分析，在采用同步检测法时误码率为

$$P_{\mathrm{e}} = \frac{1}{2}\mathrm{erfc}(\sqrt{r}) \tag{6}$$

式中，$r = a^2 / 2\delta^2$, a 为接收信号的均值，δ^2 为方差。

由于 erfc 是一个信噪比的单调降函数，而标签信号与通信信号在时域是叠加的，并且标签信号通过直接序列进行扩谱。在 s_s 所在的频段，标签信号具有高斯白噪声的性质，其叠加的信噪比由 s_s / n_{AB} 变为 $s_s /(n_{\mathrm{AB}}+s_t)$，相当于系统中噪声有所增加，从而信噪比降低。$P_{\mathrm{e}}$ 随着噪声的增加而升高，主要受标签信号功率所占比例影响。

对于标签信号的检验，有成功率和失败率两类指标。影响标签信号检验成功率的主要因素是扩谱增益的大小和信道估计的量化误差及信道的时变性。而对于失败的标签检验主要有两类错误，一是 Alice 叠加了标签信号而未被检验出来，Bob 拒绝了 Alice 发出的信号，称为虚警率；二是 Eve 冒充 Alice 发出信号而被 Bob 所接受，称为漏警率。其中第 1 类错误的原因与成功检验的影响因素类似，而对第 2 类错误则可详见下文的安全性分析。

标签信号的检验成功率和虚警率主要受标签扩谱通信的误码率决定，根据相关研究成果[22]，直接序列扩谱下，传输一定带宽的信息，信噪比可以和带宽 W 互换，也就是说把扩谱带宽与信息带宽之比定义为扩谱增益的话，信噪比随扩谱增益线性增加。由于 BPSK 调制的误码率如式(6)所示，r 与信噪比之间只是差了一个常系数，则扩谱通信的误码率为

$$P_{\mathrm{e}}^{'} = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{E}{2N}\frac{B_W}{B_I}}\right) \tag{7}$$

式中，E/N 为信噪比，B_W/B_I 为扩谱增益。

另一方面，由于噪声及信道不完美特性等影响，Alice 和 Bob 提取到的信道特征可能不完全一致，假设比特不一致程度为 ψ，则若 ψ 大于认证门限 Γ，也会导致认证失败。若信道特征长度为 M 比特，Alice 和 Bob 采用二进制相位均匀量化，则 Alice 和 Bob 由于信道特征提取不一致造成的认证失败概率

为

$$P_{\mathrm{mis}} = P(\psi \geq \Gamma) = 1 - \sum_{i=1}^{M} C_M^i P_{\mathrm{dif}}^i \left(1 - P_{\mathrm{dif}}\right)^{(M-i)} \quad (8)$$

其中，C_M^i 为从 M 个中选取 i 的组合数，P_{dif} 为单个比特不一致的概率，可根据文献[23]得到。

所以虚警率可表示为扩谱传输的错误率及 Alice 与 Bob 提取信道不匹配的概率之和，即

$$\alpha = P_{\mathrm{e}}^{'} + P_{\mathrm{mis}} \quad (9)$$

4　安全性分析

4.1 标签信号认证的理论安全性

如前文所述，在基于密钥和密码算法的传统认证模型下，攻击者的成功率下界为 $1/\sqrt{|K|}$ [2]，这比猜测密钥的成功率要高很多。而在本文的认证方法下，攻击者想要伪造标签信号，就要伪造一个能够通过检验的扩谱信号，即 m 序列。根据前文假设，m 序列的空间数为 $|\mathrm{m}|$，且空间数足够大，满足 $|\mathrm{m}| > |K|$ 成立，而且由于从密钥 K 到 m 序列所用散列函数的单向性，攻击者单纯靠猜测获得的成功率下界为 $1/|K|$。

由于 m 序列之间互相关性特性，不同的 m 序列之间互不相关，在认证过程中 Eve 即使获得了一些标签信号的样本，在 $|\mathrm{m}|$ 个 m 序列集合中选择一个与 Alice 所用的 m 序列进行相关操作的话，不能得到有用的相关峰，这样 Eve 的成功率仍然限制在 $1/|K|$，这与猜测密码的效果是相同的。下一节中针对 Eve 不同的攻击行为做具体分析。

4.2 抗攻击行为的安全性

4.2.1 被动式窃听　这种方法实现了标签信号的隐蔽传输，很难被窃取。一般情况下，由于 Bob 和 Eve 所处的位置不会完全相同，当 Eve 与 Alice 及 Bob 间的距离大于信号半个波长时，就可以认为合法信道 h_{AB} 和窃听信道 h_{AE} 是不相关的，Eve 无从获取合法信道 h_{AB} 的信息。而这种对 Eve 位置的假设在实际通信中是非常合理的，也是极易满足的[18]。另一方面，Alice 和 Bob 的密钥 K 是通过安全方式预先分配的，Eve 无法获得。由于标签信号由信道信息和密钥共同产生，这相当于为标签信号上了“两道锁”，Eve 无法获得关于标签信号的生成信息。

在信号传输环节，Eve 在不知道扩谱序列时由于其良好的互相关性很难检测到标签信号，即使 Eve 通过统计信号处理的方法获取了部分信道信息，由于信道具有时变性，标签信号具有天然的时效性，使得 Eve 被动式窃听获取到的信息难以构成安全威胁。

4.2.2 替代攻击　Eve 可通过窃听并修改 Alice 发送的信号实现攻击目的，Eve 在要发射的信号附上伪造的标签信号。若该信号被 Bob 接收并认证成功，则认为 Eve 攻击成功，攻击成功的概率用漏检率 β 表征，表示 Bob 错误地接收 Eve 发送的信号的概率。

由于标签信号是由信道和密钥通过单向散列函数产生的，Eve 可通过猜测信道和密钥生成标签信号，或者直接伪造标签信号。当 Eve 伪造合法信道特征及密钥生成标签信号发起攻击时，对于一个 Eve 伪造的特定的密钥 K，若伪造的信道特征可以使其与对应的 m 序列相乘后得到的标签信号与合法标签的比特不一致概率小于 Γ 时，攻击成功，因此，攻击率可以表示为

$$\beta = P(\rho < \Gamma) = \sum_{i=1}^{\Gamma M} C_M^i \left(\frac{1}{2}\right)^i \left(\frac{1}{2}\right)^{M-i} = \sum_{i=1}^{\Gamma M} C_M^i \left(\frac{1}{2}\right)^M \quad (10)$$

当 Eve 直接伪造标签信号时，若伪造的标签信号和合法标签信号的比特不一致率小于门限值 Γ，则攻击成功，其概率同式(8)。

在这个方法里，单向散列函数是可以公开的，即使 Eve 获取了部分信道信息，对于密钥仍然是安全的。由于扩谱序列良好的互相关性，在密钥被保护的前提下也不能够检测到所使用的序列。由上一节分析 Eve 通过被动式窃听获取标签信号的可能性较小，即使采用被动式与替代结合的方式，也难以构成成功攻击。

4.2.3 中间人转发攻击　中间人转发攻击分为两种：解码转发与放大转发。在本文模型中，解码转发相当于被动式窃听与替代攻击的结合，前面已有分析，下面讨论放大转发攻击。

Eve 采用放大转发，或称透明转发的攻击方式，此时 Eve 不对信号进行改变。根据系统模型，Bob 接收到的信号变为

$$y = \left(x * h_{\mathrm{AE}} + n_{\mathrm{AE}}\right) * h_{\mathrm{EB}} + n_{\mathrm{EB}} \quad (11)$$

整理后变为

$$y = x * \left(h_{\mathrm{AE}} * h_{\mathrm{EB}}\right) + \left(n_{\mathrm{AE}} * h_{\mathrm{EB}} + n_{\mathrm{EB}}\right) \quad (12)$$

可以看出，Bob 接收信号的信道和噪声均发生了变化。把式(9)中 $n_{\mathrm{AE}} * h_{\mathrm{EB}} + n_{\mathrm{EB}}$ 部分看成噪声，Alice 与 Bob 之间的信道 h_{AB} 变成了信道 h_{AE} 和 h_{EB} 的级联，反之亦然，此时仍然能够满足 Alice 与 Bob 信道互易性的条件。同时，由于 Eve 的参与，Bob 收到的信号被混入了 Eve 带来的噪声。噪声的增加可能恶化信噪比，对认证的性能产生影响，但是，Eve 无法实现 Alice 身份的替代，而在标签信号获取方面与被动式窃听没有差别。

5 仿真分析

仿真在瑞利衰落信道模型下进行，采用 BPSK 调制符号作为通信信号，长度为 255 bit 的 m 序列作为扩谱序列，选用 SHA-1 算法作为单向散列算法，使用最小二乘信道估计方法，并对每个径信道估计值 4 bit 均匀量化，采用 10000 次蒙特卡洛方法仿真。

首先来看标签信号与通信信号之间的影响，由于两者是时域叠加在一块的，比较关键的是功率的分配比例，即标签信号功率所占的比重。误比特率是通信系统的重要衡量指标，从图 3 的仿真结果可以看出，随着标签信号功率的增加，误比特率略有提高，在标签功率占比为 0.1%时，在 10 dB 的信噪比环境下仍然可以达到 0.06%。而漏警率随着标签信号功率增加而降低，同时信噪比越高性能越好，相应结果见图 4，可以发现在高底噪情况下漏警率和误比特率均较高，在超过 10 dB 以后可以达到较好指标。

与传统的密码认证方法相比较，这里选取信噪比为 10 dB，以 $|K|=2^{32}$ 为例，由图 5 的仿真结果可见，当标签功率超过 0.08%以后，漏警率即低于密码认证方法。

6 总结

物理层标签的方法在信号层面实现信道和发送方的双重认证，主要应用在高安全等级和计算资源有限的场景中。由于不需要复杂的密码算法，在保证认证安全性的前提下，单向散列函数比密码算法计算量降低了几个数量级，且本文方法中使用的单向散列函数、扩谱和解扩等模块均为成熟的方法并取得应用，方便使用硬件实现。本方法能够对现有认证的过程实现安全性增强，还能用于弥补业务数据传输难以认证的缺陷，可以适用于未来移动通信的低时延、高可靠特点，实现“轻量级”认证。

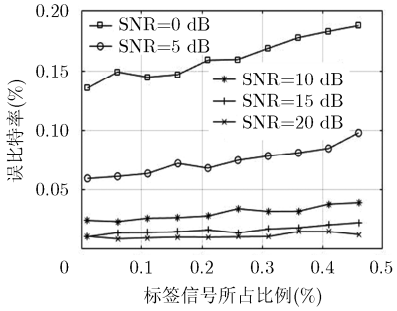

图 3 不同标签信号功率比例下误比特率仿真图

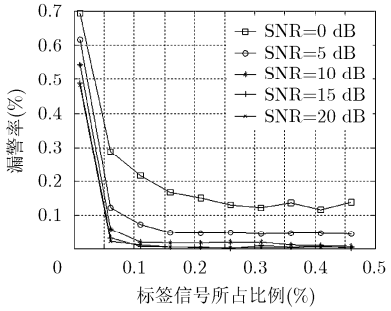

图 4 不同标签信号功率比例下漏警率仿真图

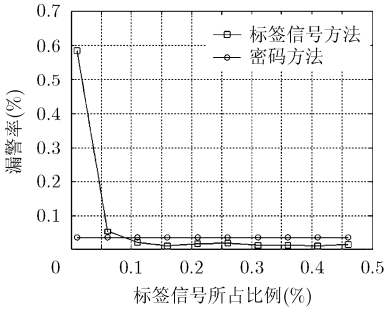

图 5 与密码认证方法比较仿真图

参 考 文 献

[1] 李中献, 詹榜华, 杨义先. 认证理论与技术的发展[J]. 电子学报, 1999, 27(1): 98–102.
LI Zhongxian, ZHAN Banghua, and YANG Yixian. A survey of identification and authentication[J]. *Acta Electronica Sinica*, 1999, 27(1): 98–102.

[2] SIMMONS G J. Authentication theory/coding theory[C]. Proceedings of CRYPTO 84 on Advances in Cryptology, New York, USA, 1985: 411–431.

[3] MAURER U. Authentication theory and hypothesis testing [J]. *IEEE Transactions on Information Theory*, 2000, 46(4): 1350–1356. doi: 10.1109/18.850674.

[4] WANG Xianbin, HAO Peng, and HANZO Lajos. Physical-layer authentication for wireless security enhancement: current challenges and future developments[J]. *IEEE Communications Magazine*, 2016, 54(6): 152–158. doi: 10.1109/MCOM.2016.7498103.

[5] PAUL L Y, BARAS J S, and SADLER B M. Physical-layer authentication[J]. *IEEE Transactions on Information Forensics and Security*, 2008, 3(1): 38–51. doi: 10.1109/TIFS.2007.916273.

[6] PAUL L Y, BARAS J S, and SADLER B M. Multicarrier authentication at the physical layer[C]. Proceedings of the 2008 International Symposium on a World of Wireless Mobile and Multimedia Networks, Newport Beach, CA, USA, 2008: 1–6. doi: 10.1109/WOWMOM.2008.4594926.

[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] WANG Ning, JIANG Ting, LÜ Shichao, *et al*. Physical- layer authentication based on extreme learning machine [J]. *IEEE Communications Letters*, 2017, 21(7): 1557–1560. doi: 10.1109/LCOMM.2017.2690437.

[9] DAI Chuping, YANG Jianxi, QIN Yongning, *et al*. Physical layer authentication algorithm based on SVM[C].

Proceedings of 2016 2nd IEEE International Conference on Computer and Communications (ICCC), 2016: 1597–1601.

[10] RAHMAN M M U, ABBASI Q H, CHOPRA N, *et al*. Physical layer authentication in nano networks at terahertz frequencies for biomedical applications[J]. *IEEE Access*, 2017, 5: 7808–7815. doi: 10.1109/ACCESS.2017.2700330.

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

[12] BARACCA P, LAURENTI N, and TOMASIN S. Physical layer authentication over MIMO fading wiretap channels[J]. *IEEE Transactions on Wireless Communications*, 2012, 11(7): 2564–2573. doi: 10.1109/TWC.2012.051512.111481.

[13] KUMAR V, PARK J M, CLANCY T C, *et al*. PHY-layer authentication by introducing controlled inter symbol interference[C]. Proceedings of IEEE Conference on Communications and Network Security (CNS), National Harbor, USA, 2013: 10–18. doi: 10.1109/CNS.2013. 6682687.

[14] XIAO Liang, GREENSTEIN L J, MANDAYAM N B, *et al*. A physical-layer technique to enhance authentication for mobile terminals[C]. Proceedings of IEEE International Conference on Communications, Beijing, 2008: 1520–1524. doi: 10.1109/ICC.2008.294.

[15] XIAO Liang, GREENSTEIN L, MANDAYAM N, *et al*. Fingerprints in the ether: Using the physical layer for wireless authentication[C]. Proceedings of IEEE International Conference on Communications, Glasgow, UK, 2007: 4646–4651. doi: 10.1109/ICC.2007.767.

[16] TUGNAIT J K and KIM H. A channel-based hypothesis testing approach to enhance user authentication in wireless networks[C]. Proceedings of Second International Conference on Communication Systems and Networks, Bangalore, India, 2010: 1–9. doi: 10.1109/COMSNETS. 2010.5432018.

[17] 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.

[18] DU Xianru, SHAN Dan, ZENG Kai, *et al*. Physical layer challenge-response authentication in wireless networks with relay[C]. IEEE INFOCOM, Toronto, Canada, 2014: 1276–1284. doi: 10.1109/INFOCOM.2014.6848060.

[19] MOLIÈRE R, DELAVEAU F, NGASSA C L K, *et al*. Tag signals for early authentication and secret key generation in wireless public networks[C]. European Conference on Networks and Communications, Paris, 2015: 108–112. doi: 10.1109/EuCNC.2015.7194050.

[20] 张余, 许金勇, 柳永祥, 等. 基于相关标识符的频谱水印嵌入与提取方法[J]. 电波科学学报, 2016, 31(1): 185–192. doi: 10.13443/j.cjors.2015031701.

ZHANG Yu, XU Jinyong, LIU Yongxiang, *et al*. Spectrum watermark embedding and extracting methodbased on correlation identifier[J]. *Chinese Journal of Radio Science*, 2016, 31(1): 185–192. doi: 10.13443/j.cjors.2015031701.

[21] ZHANG Jinling, WEN Hong, SONG Huanhuan, *et al*. Using basis expansion model for physical layer authentication in time-variant system[C]. IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 2016: 348–349. doi: 10.1109/CNS.2016.7860505.

[22] 曾璐, 谢晓尧. 基于 MATLAB 扩谱通信系统误码率的研究[J]. 通信技术, 2011, 44(11): 25–26.

ZENG Lu and XIE Xiaoyao. Study on bit error rate of spread spectrum communication system based on MATLAB [J]. *Communications Technology*, 2011, 44(11): 25–26.

[23] JAKES W C and COX D C. Microwave Mobile Communications[M]. Wiley-IEEE Press, 1994, Ch 1.

宋华伟：　男，1978 年生，副研究员，研究方向为移动通信安全.

金　梁：　男，1969 年生，教授，博士生导师，研究方向为移动通信网络与信息安全.

张胜军：　男，1988 年生，博士生，研究方向为无线通信安全.