DOI：10.7652/xjtuxb201804015

无线网络物理层安全认证方法

宋华伟，金梁，王旭
（国家数字交换系统工程技术研究中心，450002，郑州）

摘要：针对无线通信中认证方法存在计算复杂度高的问题，提出一种无线网络物理层安全认证（PLSA）方法。首先，利用通信双方信道互易性和唯一性的特点，通过估计信道并量化信道响应提取出高度相关但并不完全一致的信道特征序列，然后基于信息论安全和信道编码理论提出安全认证编码，借助双方信道特征序列中蕴含的私密共享信息量优势，使合法通信方正确编解码，而第三方只能靠猜测消息码字实施认证攻击，从而建立不需要密码算法的物理层安全认证框架。利用典型集理论和窃听信道模型对PLSA方法进行安全性分析，发现在码本长度趋于无穷大时，攻击性能上下界趋于一致，从而证明了物理层安全认证具备可行性。仿真结果表明，与传统认证方法相比，当安全互信息量超过64 bit后，物理层认证方法的攻击成功率优于传统认证方法。

关键词：无线通信；物理层安全；认证；典型集；信道互易性
中图分类号：TN918.91 **文献标志码**：A **文章编号**：0253-987X(2018)04-0105-06

A Security Authentication Method for Wireless Network Physical Layers

SONG Huawei, JIN Liang, WANG Xu
(National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China)

Abstract: A method of physical layer security authentication (PLSA) is proposed to solve the high complexity of existing authentication method in wireless communication. Firstly the characteristics of reciprocity and uniqueness of the wireless channels of two sides are utilized, and the highly correlated but not completely consistent channel characteristic sequences are extracted by estimating the channel responses. Then the security authentication coding is proposed based on the principles of security and channel coding of information theory. At last, the physical layer security authentication framework that does not need cryptographic algorithm is established. The security analysis of the physical layer authentication method is carried out by using the theory of typical set and the wiretap channel model. It is found that when the length of the codebook tends to infinity, the upper bound and the lower bound of the attack tend to be consistent. It proves that the physical layer security authentication is feasible. Simulation results show that the performance of the proposed method is better than that of the traditional authentication method when the amount of security mutual information exceeds 64 bits.

Keywords: wireless communication; physical layer security; authentication; typical set; channel reciprocity

收稿日期：2017-10-09。 作者简介：宋华伟(1978—)，男，副研究员；金梁(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金资助项目(61501516,61601514)。
网络出版时间：2018-02-26 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20180226.1945.002.html

在无线通信系统中，认证的目的是确保所接收到的消息确实来自于所期望的发射机，换言之，在一个好的认证系统中，接收者应能够以较高的概率把真正的来自源的数据包和假的数据包、被篡改的数据包区别开[1]。传统的认证模型是 Simmons 提出的基于无噪信道模型[2]，发送者 Alice 与接收者 Bob 共享密钥，Eve 作为第三方可能主动发动攻击，在最好的防御策略下攻击成功率下界比猜测密钥要高。但是，这种认证模型必须事先共享密钥或者通过一个私密信道实现密钥分发，这并不适应一些通信场景，如 M2M、D2D 等网络，且由于认证对密钥的依赖性，万一密钥泄露或者攻击者拥有很强的计算能力破解密钥，则认证系统完全失效。

近年来兴起的物理层安全技术研究基于 Wyner 提出的窃听信道模型[3]，如果窃听信道的信道质量劣于主信道，不依赖于分享密钥即可实现所谓的“绝对安全通信”。LAI 等人研究了在噪声信道下的认证模型[4]，指出在窃听信道模型的有噪条件下可以利用安全编码方式来保护密钥，证明了一个有意思的结论：当主信道的信道容量大于窃听信道的信道容量时，提出的认证方法可以利用同一密钥多次认证消息而不会明显增加敌手攻击成功的概率，而上述结论在无噪声信道下是不可能的。最近，在物理层进行安全认证引起了一些研究者的兴趣[5]，作为一种新型的认证方法，可以作为高层认证技术的有益补充。Xiao 等人提出了跨层认证的思路[6]，初次认证在高层实现，对后续数据包可采用基于无线信道特征指纹的物理层认证的方法，即通过比较前后两次数据包的信道特征是否一致判断通信链路是否受到攻击。Shan 等人提出一种物理层挑战-响应认证机制[7]，并将该物理层认证机制嵌入高层认证机制中。最近，还出现了利用信道特征信息进行物理层认证的方法[8-11]和引入了机器学习的物理层安全认证方法[12-14]。

本文提出利用通信双方的信道的互易性和唯一性进行认证的思路。在时分复用（TDD）系统中，Alice 和 Bob 之间的信道具有短时互易性，通过估计信道量化出序列 $\boldsymbol{S}_{\text{Alice}}$ 和 $\boldsymbol{S}_{\text{Bob}}$，这两个序列具有高度相关性但并不完全一致，而这两个序列对 Eve 则天然具有私密性。利用信息论中典型集的方法把信道编码与认证编码相结合，提出基于相关序列和消息序列相结合编解码的认证框架。对于 Eve 可能采用的攻击行为进行了分类，并分析其攻击能力的上下界。通过理论分析发现，在编码的码字长度趋向于无穷大时，认证攻击成功率的上下界趋于一致。

1 系统模型

系统模型如图 1 所示。Alice 与 Bob 通过信道估计并量化，用同样的方法分别提取出序列 $\boldsymbol{S}_{\text{Alice}}$ 和 $\boldsymbol{S}_{\text{Bob}}$，Eve 在此过程中得到不相关的序列 $\boldsymbol{S}_{\text{Eve}}$。Alice 要将消息序列 $\boldsymbol{M}$ 传送给 Bob，经过编码后 Alice 发送序列 $\boldsymbol{S}_X$，经过有噪信道后 Bob 接收到序列 $\boldsymbol{S}_Y$，Eve 接收到序列 $\boldsymbol{S}_Z$。Eve 试图使 Bob 接收所发送的消息 $\boldsymbol{M}'$，可以伪造生成新消息，也可以根据接收到的信息篡改部分内容后进行仿冒。

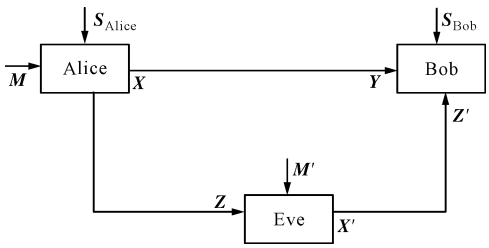

图 1 基于信道互易性的认证模型

为了表述方便，本文定义随机变量 X、Y、Z，其样本为 x、y、z，样本空间为 R_X、R_Y、R_Z，集合 R_x 的元素的个数称为集合的势，简记为 $|R_x|$。$\boldsymbol{S}_X$ 表示根据独立同分布的随机变量 X 生成长度为 K 的序列 $x_1, x_2, \cdots, x_K$。

2 信道特征相关优势条件下的安全认证

Alice 和 Bob 从具有互易性的信道特征中可以提取出高相关性的序列，但由于 Eve 和 Alice、Bob 所处位置不同则信道不同，因此，所得到的序列相关性大大降低。从信息论的观点来看，Alice 和 Bob 之间互易的信道特征可以看成是一个天然的随机源且不为 Eve 所知，其中蕴含了一定的共享私密信息量。利用这个优势，可以实现基于信道的认证。本文描述的认证方法是在初始身份认证完成的基础上的，可以作为消息认证的一种安全加强或者替代。由于 Alice 和 Bob 之间具有对称性，仅讨论 Bob 认证 Alice 的情形，互换 Alice 和 Bob 角色可以实现双向认证。

2.1 相关序列及其性质

Alice 和 Bob 先互发导频信号，并据此进行信道估计，从而获取 L bit 的信道信息序列，Eve 在此过程中实施被动窃听。假设 Alice 和 Bob 之间的信道为 h_{AB} 和 h_{BA}，而 Alice、Bob 和 Eve 之间信道为 h_{AE}、h_{BE}，通过信道估计得到的是他们的近似值。如

图 2 所示，Alice 在 t 时刻广播发送导频序列，Bob 和 Eve 通过信道估计分别得到 $\hat{h}_{AB}(t)$ 和 $\hat{h}_{AE}(t)$；随后 Bob 在 $t+\tau$ 时刻广播发送导频序列，Alice 和 Eve 通过信道估计分别得到 $\hat{h}_{BA}(t+\tau)$ 和 $\hat{h}_{BE}(t+\tau)$。现有的研究结果表明，通信双方的信道具有短时互易性[15]，所以 $\hat{h}_{AB}(t)$ 和 $\hat{h}_{AE}(t+\tau)$ 是具有高度相关性的。当 Eve 与 Alice 及 Bob 的间距超过信号波长的一半时，就可以认为窃听信道与合法通信信道间不相关，而这种情况通常在无线通信中也是普遍存在的[16]，所以 Eve 估计的信道信息与 Alice、Bob 均不相关。

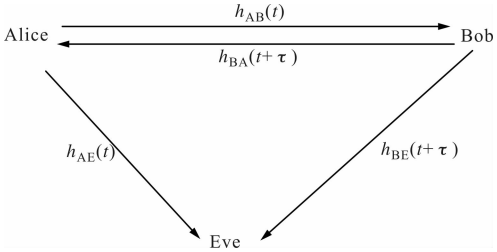

图 2　信道估计示意图

假设信道慢变的情形，则通过信道估计的可以根据导频信号中多个符号得到同一信道特征的不同估计值。鉴于 $\boldsymbol{S}_{Alice}$ 和 $\boldsymbol{S}_{Bob}$ 具有很高的相关性，可以看作是根据一组独立同分布随机变量产生的序列，不一致位看作是引起的扰动，设随机变量为 V，序列集合为 R_V。根据典型集理论，有以下引理[17]。

引理 1　随着序列长度 L 的增大，提取序列为典型序列的概率趋近于 1。

证明　序列的型是字符集中每个字符出现次数的比例，典型集理论相当于集合中的大数定理，当序列中的随机变量服从相同的分布，随着序列长度增大，序列中出现次数比例与随机变量分布越来越接近，所提取序列越接近典型序列。

2.2　安全认证理论基础

安全认证是指攻击方 Eve 在进行有限次尝试情况下，仍然不能伪造或者篡改出能通过认证的消息。传统的认证安全基于密码算法的破译难度，近年来兴起的物理层安全技术则是基于信息论的安全。下面首先介绍保密容量理论，随后介绍安全认证理论和认证框架。

2.2.1　完美安全的存在性

首先回顾与搭线窃听信道[3]相关的结论。在搭线窃听信道模型中定义了两个离散无记忆信道 $X\rightarrow(Y,Z)$，其中 X 为发送者的输入字符，Y 是合法接收者的输出字符，Z 是窃听者的输出字符。搭线窃听信道中的窃听者采用被动方式侦听，消息传输的目标是将消息发送给目的节点，同时使泄露给窃听者的信息最小。更具体地，为了发送消息 $\boldsymbol{M}$，发送者发送 $\boldsymbol{S}_X=f(\boldsymbol{M})$，其中 f 为一个随机编码器。目的节点接收到 $\boldsymbol{S}_Y$ 后，获得消息的估计值 $\boldsymbol{M}'=g(\boldsymbol{S}_Y)$。攻击者完全知道系统的设计，因此知道源节点所用的码本。如果存在 f 和 g 使得对于任意 $\varepsilon>0$ 均存在一个正整数 n_0（$\forall N>n_0$）时有

$$|\boldsymbol{M}|\geqslant 2^{nR_S} \tag{1}$$

$$P\{\boldsymbol{M}'\neq\boldsymbol{M}\}\leqslant\varepsilon_P \tag{2}$$

$$\frac{1}{n}I(\boldsymbol{M};\boldsymbol{S}_Z)\leqslant\varepsilon \tag{3}$$

式中：R_S 为完善保密速率；n 为消息长度；ε_P 为在 P 概率下的无穷小量；I 为互信息。

满足式(1)～(3)，则称完美保密速率 R_S 是可达的。完美保密容量 C_S 定义为 R_S 的上确界，其数值满足上式条件。文献中已证明完美保密容量为

$$C_S=\max_{U\rightarrow X\rightarrow YZ}[I(U;Y)-I(U;Z)]^+ \tag{4}$$

式中：函数 $[x]^+=\max(x,0)$；U 为一个辅助变量，满足马尔可夫链 $U\rightarrow X\rightarrow YZ$。

如果对于所有满足上述马尔可夫链的 U，有 $I(U;Z)>I(U;Y)$，那么就称搭线窃听信道噪声低于主信道噪声，或者说具有优势信道。搭线窃听信道模型使得源节点和目的节点之间无需预先分配密钥，只需利用码率高于安全信息速率 R_S 的码字进行编码（即将消息映射到多个不同的码字中），就能实现通信的完美安全。通常，将码字速率设定为可被源-目的信道所支持的速率，使得合法接收者在该速率下能正确恢复出码字，而该速率对于攻击者过高，使其无法译码。

2.2.2　安全编码与认证

搭线窃听模型中的安全编码方法利用优势信道能够实现信息论的完美安全，如果搭线窃听信道噪声大于主信道噪声，则存在一个输入分布满足 $I(X;Y)-I(X;Z)>0$。因此，对于给定的 N（这里 N 与安全容量有关），存在一个正整数 n_1，使得在 $\forall n>n_1$ 的条件下，满足

$$2^{n(I(X;Y)-I(X;Z))}>N \tag{5}$$

同样，对于给定的消息长度 $|\boldsymbol{M}|$ 及 N，存在一个正整数 n_2，使得在 $\forall n>n_2$ 的条件下，满足

$$2^{nI(X;Y)}>|\boldsymbol{M}|N \tag{6}$$

由香农编码定理可知，只要码长 N 足够长，Alice 和 Bob 之间存在一个信道编码的码本 C，C 有 $2^{nI(X;Y)}$ 个码字，使译码的最大错误概率任意小。

满足式(5)和式(6)的编码方案为安全传输编

码。类似地，如果能够在认证应用中设计的编码利用 Alice 和 Bob 之间的某种优势，使得 Eve 不知道消息 M 所对应的码字，而且通过 Eve 的窃听过程仍然不能提高攻击成功率，那么这种编码就成为安全认证编码。

这里需要为安全认证编码生成一个码本，本文参考离散无记忆(DMC)信道编码方案[18]。具体而言，源节点为任意一个 ε 强典型序列赋予一个独特的编号，并给非典型序列统一编号为 0，记信道估计值 $h_{AB}(t)$、$h_{AB}(t+\tau)$、$h_{AE}(t)$、$h_{BE}(t+\tau)$分别为 S_1、S_2、V_1、V_2，$I(S_1;S_2)$表示 Alice 与 Bob 之间互易信道特征的互信息，由于 Eve 得到了 V_1、V_2，所以这部分信息量是不安全的，则 $I(S_1;S_2|V_1,V_2)$代表 Alice 与 Bob 之间安全的互信息。取 $N=2^{I(S_1;S_2|V_1,V_2)}$，将码本分割为 N 个子集，每一个子集与一个典型集相关联。因为消息和典型集长度满足方程(6)，所以每个子集中的码字数量都大于$|\boldsymbol{M}|$。然后，源节点将每个子集进一步分为$|\boldsymbol{M}|$个二进制码字，每个二进制码代表一条消息。图 3 给出安全认证编码方案中的码本结构。

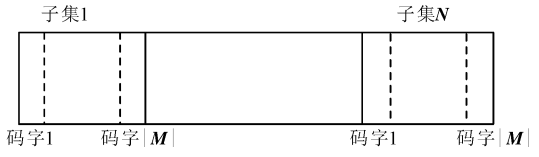

图 3 安全认证编码方案中采用的码本结构

2.3 安全认证框架

Alice 和 Bob 先互发导频信号，并据此进行信道估计，从而获取高度相关的信道信息序列 $\boldsymbol{S}_{\text{Alice}}$ 和 $\boldsymbol{S}_{\text{Bob}}$，Eve 在此过程中实施被动窃听，得到 $\boldsymbol{S}_{\text{Eve}}$。

Alice 要将消息 $\boldsymbol{M}$ 传送给 Bob，经过编码后 Alice 得到序列 $\boldsymbol{S}_X$，编码函数 $f:\boldsymbol{M},\boldsymbol{S}_{\text{Alice}}\rightarrow\boldsymbol{S}_X$。

经过有噪信道后 Bob 接收到 $\boldsymbol{S}_Y$，经过译码后还原出消息 $\boldsymbol{M}$ 或者拒绝消息，解码函数 $g:\boldsymbol{S}_Y,\boldsymbol{S}_{\text{Bob}}\rightarrow\boldsymbol{M}\cup\{\perp\}$构成，$\perp$表示解码失败，则认为该消息不是 Alice 所发。

编解码的码本由 $N|\boldsymbol{M}|$个码字组成，信道信息序列对应 N 个典型集，每个消息对应$|\boldsymbol{M}|$个子集中的一个。

Eve 试图使 Bob 接收所发送的消息 $\boldsymbol{M}'$，为简便起见，假设编解码函数和所用的码本是公开的，Eve 知道除了相关序列以外的所有细节。

3 安全性分析

下面讨论认证的安全性。所谓的安全认证就是要在 Eve 有限次的攻击下，攻击成功的概率是可忽略的，希望在敌手 Eve 通过信道窃听并且动态的修改接收到消息的前提下，Eve 还是不能伪造一个可通过认证的消息。

Eve 可以窃听信道的输出，并可发起主动攻击，主要采用以下两种攻击方式：伪造攻击和替代攻击。

(1)伪造攻击。Eve 可以在 Alice-Bob 认证过程中切断正常通信，伪装成 Alice 发送消息给 Bob，期望通过 Bob 的认证。

(2)替代攻击。Eve 窃听信道的输出，然后将消息 $\boldsymbol{M}$ 替换为 $\boldsymbol{M}'$发送给 Bob。

记 Eve 攻击的成功率为 P_{D}，伪造攻击成功率为 P_{I}，替代攻击成功率为 P_{S}。因为替代攻击是 Eve 先接收 Alice 发出的消息，然后进行修改或者伪造，由于通过接收消息获取一定的信息量，所以比直接伪造攻击的成功率要高，则有 $P_{\text{I}}<P_{\text{S}}$ 成立，所以有

$$P_{\text{I}}\leqslant P_{\text{D}}\leqslant P_{\text{S}} \tag{7}$$

下面分析 Eve 认证攻击成功率的性能，也就是 P_{D} 的上下界。

3.1 认证攻击成功率下界

首先讨论认证性能的下界，也就是 P_{D} 的最小值。根据前面的假设，Eve 知道信道编码的码本，也知道码本分成 N 个组，只是不知道使用码本的哪个子集。由于典型集出现的概率几乎相等，因此考虑 Eve 伪造攻击进行猜测的情况，Eve 随机选取一个分组，成功的概率为 $1/N$，不加证明的给出下面的定理 1。

定理 1 伪造攻击的成功率下界为 $1/N$。

3.2 认证攻击成功率上界

Eve 在初始时替代攻击和伪造攻击的成功率相同，只能猜测密钥，当窃听方接收到通信内容后，其中就蕴含了与密钥相关的信息量，所以替代攻击的成功率会逐渐提高。如果一种编码能够使窃听方接收信息后对密钥的信息量获取没有任何帮助，那么就把攻击者的攻击能力限定在猜测密钥水平，替代攻击也就与伪造攻击效能相同。

在模型的假设中，$\boldsymbol{S}_{\text{Alice}}$ 和 $\boldsymbol{S}_{\text{Bob}}$ 之间的相关度高于 $\boldsymbol{S}_{\text{Eve}}$，这 3 个序列之间具有互信息的优势，也就是要满足

$$I(\boldsymbol{S}_{\text{Alice}};\boldsymbol{S}_{\text{Bob}})>I(\boldsymbol{S}_{\text{Alice}};\boldsymbol{S}_{\text{Eve}}) \tag{8}$$

$$I(\boldsymbol{S}_{\text{Alice}};\boldsymbol{S}_{\text{Bob}})>I(\boldsymbol{S}_{\text{Bob}};\boldsymbol{S}_{\text{Eve}}) \tag{9}$$

Csiszar 基于窃听信道模型提出关于强安全的窃听信道编码[19]。定义 C 表示一个窃听信道的码本，$P(X,Z)$为 C 上 X 与 Z 的联合分布。当输入均

匀分布于 C 时，$Q(Z)$ 为 Z 的边缘分布。$P(X|Z)=\frac{P(X,Z)}{Q(Z)}$ 为给定 Z 时的条件分布。

令 $\{C_1,\cdots,C_N\}$ 为 C 的一个分割，将此分割表示为一个映射，$f:C\to\{C_1,C_2,\cdots,C_k,\cdots,C_N\}$，$1\leqslant k\leqslant N$。$Q_k(Z)$ 表示 Z 在码本子集 C_k 下的概率分布函数，也就是

$$Q_k(Z)=\sum_{x\in C_k}(P(X,Z)/P(C_k)) \tag{10}$$

定义

$$d_{\mathrm{av}}(f)=\sum_{k=1}^{N}P(C_k)d(Q_k,Q) \tag{11}$$

式中

$$d(Q_k,Q)=\sum_{k=1}|\,Q_k(Z)-Q(Z)\,| \tag{12}$$

这里 $d(Q_k,Q)$ 为分布 Q_k 与 Q 间的距离。当 $d(Q_k,Q)$ 为 0 时，窃听者通过信道的输出 Z 进行观察，无法区分 C 上的任何子集 C_k。直观上看，如果适当地选择 C 和 f 可使 $d_{\mathrm{av}}(f)$ 任意小，在给定输出的情况下，所发送的码字来自于子集 C_k，接收者不能获得关于子集 C_k 的任何信息。下面引入一个重要的引理。

引理 2[19]　考虑一个窃听信道 $X\to(Y,Z)$，假设 T_{p} 为信道输入的典型集，满足 $P(x)>0$，选择 $\delta>0$，满足 $I(X;Y)>I(X;Z)+2\delta$，存在一个取自于 T_{p} 的集合作为码本 C，$|C|=2^{n[I(X;Y)-\delta]}$，属于 C 的大小相等且不相交子集 $C_1,C_2,\cdots,C_N$，$N\leqslant 2^{n[I(X;Y)-I(X;Z)-2\delta]}$，满足 $C=\bigcup C_k$ 为主信道 $X\to Y$ 的码字集合，平均错误概率指数级无穷小。C 的分割函数 $f:C\to\{C_1,C_2,\cdots,C_N\}$，且有 $f^{-1}(k)=C_k$，$k=1,\cdots,N$，在概率分布 $P(X,Z)=\frac{1}{|C|}P(Z|X)$ 下具有指数级无穷小的 $d_{\mathrm{av}}(f)$，而且 $I(N;Z)$ 对于 N 为指数级无穷小。

引理 2 的证明过程参见文献[19]。

由引理 2 中 $d_{\mathrm{av}}(f)$ 为指数小，假设

$$d_{\mathrm{av}}(f)=\varepsilon_1=\mathrm{e}^{-n\alpha} \tag{13}$$

考虑把 Eve 观察到的码字集合分成两部分，一个是使 $d(Z)$ 较小的集合 U，剩下部分为补集 $\overline{U}$，有以下定义

$$U\triangleq\{z:d(Z)>\varepsilon_1^{1/2}\} \tag{14}$$

基于引理 2，选择满足下面两个式子的正整数 n_1 和 n_2

$$2^{n_1(I(X;Y)-\delta)}>|\,M\,|\,N \tag{15}$$

$$2^{n_2(I(X;Y)-I(X;Z)-2\delta)}>N \tag{16}$$

然后，选择 N，使得 N 满足 $N>\max\{n_1,n_2\}$。分析替代攻击的成功率 P_{S}，可以得到以下定理。

定理 2　替代攻击的成功率上界为 $1/N+\varepsilon$，当码字长度 N 趋近无穷大时，ε 趋近于 0。

证明　首先重写一下引理 2 中的 $d_{\mathrm{av}}(f)$，如下式

$$d_{\mathrm{av}}(f)=\sum_{k=1}^{N}\sum_{Z\in U\bigcup\overline{U}}|\,P(C_k)Q_k(Z)-P(C_k)Q(Z)\,|=\sum_{Z\in U\bigcup\overline{U}}Q(Z)d(Z) \tag{17}$$

式中

$$d(Z)=\sum_{k=1}^{N}|\,P(C_k\mid Z)-P(C_k)\,|=\sum_{k=1}^{N}|\,P(C_k\mid Z)-\frac{1}{N}\,| \tag{18}$$

式(18)成立是由于信道输入均匀分布，从而有 $P(C_k)=1/N$。

由集合 U、$\overline{U}$ 的定义和式(17)可得

$$d_{\mathrm{av}}(f)=\sum_{Z\in U}Q(Z)d(Z)+\sum_{Z\in\overline{U}}Q(Z)d(Z) \tag{19}$$

把式(13)带入式(19)，重点考虑 $Z\in U$ 部分，有以下不等式成立

$$\varepsilon_1^{1/2}\sum_{Z\in U}Q(Z)\leqslant\sum_{Z\in U}Q(Z)d(Z)\leqslant d_{\mathrm{av}}(f)\leqslant\varepsilon_1 \tag{20}$$

整理可得

$$\sum_{Z\in U}Q(Z)\leqslant\varepsilon_1^{1/2} \tag{21}$$

而对于 $Z\in\overline{U}$ 组成的集合，有以下不等式成立

$$\max_K\{P(k\mid Z)-\frac{1}{N}\}\leqslant\sum_{k=1}^{N}|\,P(C_k\mid Z)-\frac{1}{N}\,|=d(Z)\leqslant\varepsilon_1^{1/2} \tag{22}$$

整理可得

$$\max_k P(k\mid Z)\leqslant\varepsilon_1^{1/N}+\frac{1}{N} \tag{23}$$

则有

$$P_{\mathrm{S}}\leqslant\sum_Z p(Z)\max_k P(k\mid Z)=\sum_{Z\in U}P(Z)\max_k P(k\mid Z)+\sum_{Z\in\overline{U}}P(Z)\max_k P(k\mid Z)\leqslant\sum_{Z\in U}Q(Z)+\varepsilon_1^{1/2}+\frac{1}{N}\leqslant\varepsilon_1^{1/2}+\varepsilon_1^{1/2}+\frac{1}{N}\leqslant\frac{1}{N}+2\mathrm{e}^{-N\alpha/2} \tag{24}$$

式中，等式右边第 1 个不等式成立是由于 $\max_k P(k|Z)\leqslant 1$，第 2 个不等式成立是由于带入了式(21)，第 3 个不等式成立是由于带入了式(23)。

令 $\varepsilon=2\mathrm{e}^{-n\alpha/2}$，当 N 趋近于无穷大时，ε 趋近于 0。证毕。

从定理 2 可以看出，替代攻击的上界与模拟攻

击的下界在码字长度 N 趋近无穷大时都趋近 $\frac{1}{N}$，也就是说，Eve 攻击的成功率上下界重合。这里 N 与 $\boldsymbol{S}_{\text{Alice}}$ 和 $\boldsymbol{S}_{\text{Bob}}$ 之间的私密信息量有关，也就是相对于 Eve 的优势。

4 仿真分析

认证安全性的主要指标是 Eve 仿冒攻击的成功率。由于密码算法进行认证的成功率下界是 $2^{-H(K)/2}$，而物理层安全认证的主要因素是 Alice 与 Bob 的安全互信息。图 4 为物理层认证方法与传统认证方法的性能比较。由图 4 所示的数值结果可以看出，随着安全互信息量的增加，攻击成功率逐渐下降。与传统认证方法相比较，假设传统方法密钥长度为 128 bit，当安全互信息量超过 64 bit 后，物理层认证方法即可优于传统方法。

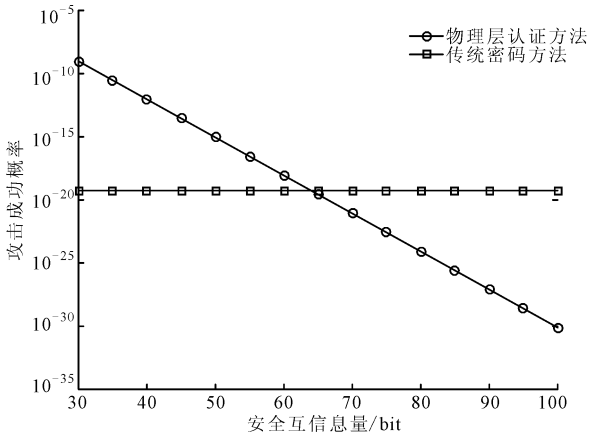

图 4 物理层认证与传统认证方法的性能比较

在实际环境中，由于 Alice 和 Bob 的互易性偏差或者存在干扰等因素，安全互信息量难以满足条件，此时该方法性能有所下降，但是仍然有效，也可以把物理层安全认证方法与传统认证方法结合以保证安全性。

5 结 论

认证安全要求的条件是信道相关性优势，这比安全传输的要求低。从信息论的观点来看，Alice 和 Bob 共享的私密信道特征形成了优势，而且由于信道特征的测量可以在通信过程中持续进行，天然保障了提取序列的新鲜性。本文描述的认证框架不需要设计和实现复杂的密码算法，因而这种认证方法有更强的适应性。本文从理论上证明了通过互易的信道特征提取序列进行认证的可行性，存在一种把认证码和信道编码结合的编码方法能够实现认证的安全性，但是，这种编码要求码长趋近于无穷大，如何设计出计算可行的编码还需要继续研究。

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，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 [M]// Lecture Notes in Computer Science，Vol 196. Berlin，Germany：Springer Verlag，1985：411-431.

[3] WYNER A D. The wire-tap channel [J]. Bell Labs Technical Journal，1975，54(8)：1355-1387.

[4] LAI L F，GAMAL H E，POOR H V. Authentication over noisy channels [J]. IEEE Transactions on Information Theory，2009，55(2)：906-916.

[5] WANG X B，HAO P，HANZO L. Physical-layer authentication for wireless security enhancement：current challenges and future developments [J]. IEEE Communications Magazine，2016，54(6)：152-158.

[6] XIAO L，GREENSTEIN L，MANDAYAM N，et al. Fingerprints in the ether：using the physical layer for wireless authentication [C]// IEEE International Conference on Communications. Piscataway，NJ，USA：IEEE，2007：4646-4651.

[7] SHAN D，ZENG K，XIANG W D，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.

[8] LIU J Z，WANG X B. Physical layer authentication enhancement using two-dimensional channel quantization [J]. IEEE Transactions on Wireless Communications，2016，15(6)：4171-4182.

[9] 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(99)：7808-7815.

[10] 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.
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.

（下转第 138 页）