

基于物理层密钥的消息加密和认证机制

李兴志, 金梁, 钟州, 楼洋明

(国家数字交换系统工程技术研究中心, 河南 郑州 450002)

摘要: 针对传统高层消息认证存在密钥泄露隐患、物理层消息认证无法防止被动窃听的问题, 提出一种基于无线物理层特征的消息加密和认证机制。通过提取无线信道特征生成物理层密钥, 并与身份密钥结合生成种子密钥; 随后根据提取的种子通过密钥流生成器产生密钥流对消息进行加解密, 对传输数据的私密性进行保护; 最后接收方通过 CRC 校验结果对接收消息的真实性、完整性进行认证。仿真结果表明, 该方法在防止被动窃听和主动攻击上具有更好的性能, 密钥流随机性显著提高, 认证漏检率降低约 $\frac{1}{2}$ 。

关键词: 物理层密钥; CRC 校验; 流密码; 消息认证

中图分类号: TN918

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018055

Message encryption and authentication mechanism based on wireless physical layer key

LI Xingzhi, JIN Liang, ZHONG Zhou, LOU Yangming

National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China

Abstract: In order to solve the problem of hidden key leakage in traditional high-level message authentication and passive eavesdropping in physical layer message authentication, a message encryption and authentication mechanism based on the characteristics of wireless physical layer was proposed. By extracting the characteristics of the wireless channel, the physical layer key was generated and the seed key was generated by combining the identity key. The key stream generator then generated the key stream to decrypt the message according to the extracted seed, protects the privacy of the transmitted data, and the final receiver authenticated the authenticity and integrity of the received message through the CRC verification result. Simulation results show that the proposed method has better performance in preventing passive eavesdropping and active attack, and the randomness of key stream is greatly improved and the rate of authentication leak detection is reduced by half.

Key words: physical layer key, CRC check, stream cipher, message authentication

1 引言

随着移动通信应用场景的快速扩展, 通信的安全性受到了越来越多的关注。对接收到消息进

行认证, 以保证消息的真实性、完整性以及来源的合法性在通信安全中至关重要, 接收方要能够验证接收消息是否被替换或篡改, 并且来自声明的合法通信方。现有的消息认证一般在高层通过

收稿日期: 2018-06-14; 修回日期: 2018-07-02

通信作者: 李兴志, xingzhi_li@yeah.net

基金项目: 国家自然科学基金资助项目 (No.61601514)

Foundation Item: The National Natural Science Foundation of China (No.61601514)

信息加密^[1]、消息摘要^[2]或消息认证码^[3]的方式实现, 尽管可以保证消息的真实性和完整性, 但会产生较大的计算开销, 难以适应很多终端资源受限的情况^[4]; 同时高层认证机制通过预分配的身份密钥对消息进行验证, 安全性来自认证算法的计算复杂度, 随着计算能力的快速提高, 传统的消息认证方法可能面临新的威胁^[5]。

在传统高层认证机制中, Alice 向 Bob 发送消息 s 前, 首先根据加密算法 E 和身份密钥 K 计算出认证标签 $Tag = E_K(s)$, 并将其附在发送的消息 s 后产生待发送消息 $m = (s, Tag)$ 。Bob 接收到 $m' = (s', Tag')$, 利用接收消息 s' 和密钥 K 计算标签 $E'_K(s')$, 并与接收到的标签 Tag' 进行如下假设检验。

$$\begin{aligned} H_0 : Tag' &= E'_K(s') \\ H_1 : Tag' &\neq E'_K(s') \end{aligned} \quad (1)$$

如果计算的标签与接收的标签匹配, 接受假设 H_0 , 此时认为接收的消息 m' 为真实的, 并认为该消息来自实际的发送者^[6]; 如果计算的标签与接收的标签不匹配, 接受假设 H_1 , 此时认为接收消息 m' 受到了攻击, m' 的一个或多个位与发送消息 m 不同 (除非发生小概率的碰撞), 消息将被拒绝。攻击者 Eve 对通信系统完全了解, 包括加密方法 E , Eve 唯一不知道的是 Alice 和 Bob 用于加密算法 E_K 的身份密钥 K , 并且 Eve 有能力向信道发送伪造的消息 s_e , 企图使 Bob 将 s_e 当作真实消息接收。由于采用了加解密算法, 该方法有计算开销比较大、不适应终端资源受限情况, 安全性基于计算复杂度、容易受到攻击等缺点。

无线信道具有时变性、唯一性和互易性等特点^[7], 信道特征随时间和通信方的位置快速变化, 并且变化趋势无法预测, 这使无线信道成为一个天然的随机源^[8]; 同时在相干时间内, 可以认为信道条件不发生改变^[9-10], 即合法通信双方可以观察到一致的信道特征, 并且与攻击者观察到的信道特征不同, 无线信道的这些特征可以用来改进现有的认证机制。文献[11]提出了一种物理层消息认证方法, 利用物理层信道特征表征终端, 通过比较 2 次连续接收消息的信道特征的相关性, 对消息来源进行验证。通信时合法用户首先通过信道 h_{AB} 建立信任关系, 通过当前的数据分

组提取信道特征 H_t , 然后通过下一时刻的数据分组提取信道特征 H_{t+1} , 为了对 $t+1$ 时刻的数据分组来源进行认证, 根据 2 次提取的信道特征建立如下二进制假设检验:

$$\begin{aligned} H_0 : H_{t+1} &= H_t \\ H_1 : H_{t+1} &\neq H_t \end{aligned} \quad (2)$$

当 2 次信道特征一致时, 接受假设 H_0 , 此时认为 H_{t+1} 提取于合法信道 h_{AB} , 即该消息仍然来自之前的合法用户, 认证成功; 当 2 次信道特征不一致时, 接受假设 H_1 , 此时认为 H_{t+1} 提取于自攻击者的信道 h_{EB} , 即该消息来自攻击者 Eve, 通信遭受了攻击, 认证失败。文献[11-13]分别利用信道频率响应^[11]、接收信号强度^[12]和信道冲击响应^[13]等参数验证了该方法的有效性。为了解决物理层认证无法实现初始认证的问题, 文献[14]提出了物理层认证与高层认证结合的认证方法, 即初次认证在高层实现, 并通过合理的参数设计和物理层认证结合起来, 高层认证成功后, 后续消息采用无线信道进行认证, 一旦物理层认证失败即重新转为高层认证。该方法开销低、实现简单, 但是仅对消息来源的真实性进行了认证, 无法对消息的完整性和私密性进行保护, 无法防止被动攻击; 同时对信道特征只进行了简单的二元假设检验, 没有充分利用无线信道特征的随机性。此外, 由于文献[11-13]中的方法通过比较连续消息的信道特征相似性进行认证, 不适用于快速移动场景。文献[14]中的方法可能需要频繁地在高层认证和物理层认证间切换, 增加了认证开销和身份密钥泄露的风险。方法实现简单、开销低, 但是仅仅对消息来源的真实性进行了认证, 缺少对消息私密性的保护, Eve 可以通过被动式窃听窃取双方的通信内容。

基于传统高层消息加密和认证机制开销大, 不适应终端资源受限情况、存在密钥泄露隐患, 物理层消息认证存在身份密钥泄露风险、无法防止被动窃听等问题, 本文提出一种基于物理层密钥和流密码的消息加密与认证机制。认证双方通过提取私有的无线信道特征生成物理层密钥, 并通过散列函数和身份密钥结合作为流密钥的生成种子; 随后, 收发双方根据该种子产生相同的密钥流, 分别用于消息的加解密过程, 对传输数据

的私密性进行保护；最后，接收方通过 CRC 校验判断接收消息中是否产生错误位，实现对接收消息真实性、完整性的认证。由于信道特征在时间和空间上都是快速去相关的，每次提取的物理层密钥是动态随机的，即密钥流的生成种子是不断变化的。本文所提的方案，利用现有的加密和校验技术，对物理层密钥进行合理有效的利用，从而有效地提高了现有加密和认证机制的安全性，可以提供高效率的消息认证，高安全性的数据保护，同时仅消耗较少的资源。仿真结果表明，该方法在防止被动窃听和主动攻击上均具有更好的性能，密钥流随机性显著提高，认证漏检率明显降低。

2 系统模型

认证系统模型如图 1 所示，包含 2 个合法通信方 Alice、Bob，一个潜在的攻击者 Eve。Alice 和 Bob 存储有预分配的身份密钥 K ，并通过 K 实现初始身份认证，建立信任关系。Eve 为攻击方，企图窃取或伪造 Alice-Bob 间的消息认证信息，伪装成 Alice 或 Bob 向对方发送虚假信息，并通过合法通信方的消息认证达到攻击目的。

本文首先通过散列函数，将利用信道特征 H_i 提取的物理层密钥 K_z 与身份密钥 K 结合，生成种子密钥 $Seed$ ，以实现身份密钥 K 的保护，随后利用流密码的方法产生密钥流对消息进行加密保护。只有同时具有身份密钥 K 和物理层密钥 K_z 的接收方才能产生相同的密钥流解密接收消息，并通过对接接收数据的 CRC 校验结果进行认证判决。

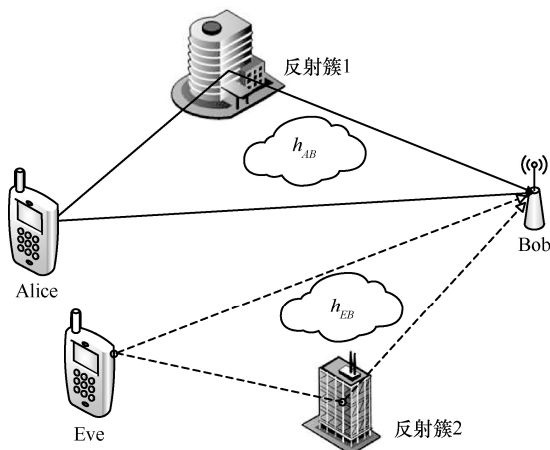


图1 认证系统模型

3 加密和认证方案的设计实现

3.1 消息加密和认证流程

本文所提的加密及认证机制的整体流程如图 2 所示。图 2 表示的是 Bob 对 Alice 发送的消息进行解密和认证的情况，Alice 对 Bob 的发送消息解密和认证的步骤与该过程一样。具体过程分为以下 4 个步骤。

1) 消息认证开始之前，Alice 和 Bob 首先提取物理层安全密钥 K_z ，并分别和共享的身份密钥通过散列函数生成物理层种子密钥 $Seed_A$ 和 $Seed_B$ 。

2) Alice(Bob) 根据生成的种子密钥 $Seed_A$ ($Seed_B$) 利用流密钥生成器产生密钥流 s_A (s_B)。

3) Alice 通过异或(XOR)操作，将密钥流 s_A 添加到消息流 $Message$ 上并发送给 Bob；Bob 对接收消息，添加 s_B 后进行 CRC 校验。如果通过 CRC 校验则说明 $s_A = s_B$ ，此时 Bob 认为该消息来自 Alice，继续通信；否则，说明该消息产生错误或者该消息来自攻击者 Eve，重新进行身份认证。

4) 后续通信中，Bob 将密钥流 s_B 添加到消息上发送给 Alice；Alice 采用相同的方法对接收消息进行认证。

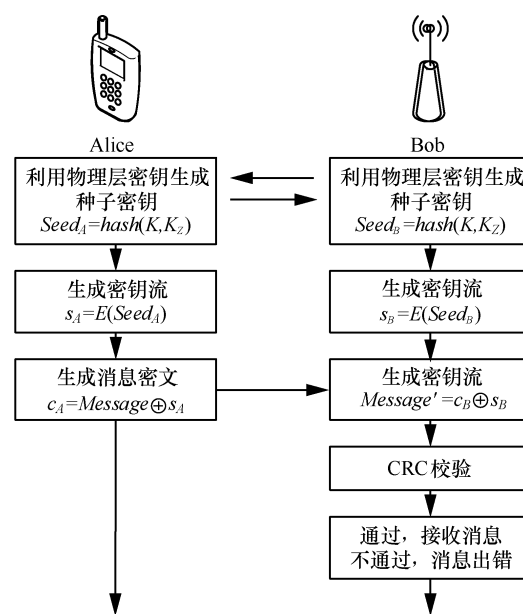


图2 加密及认证流程

3.2 物理层种子密钥生成

现有的文献针对物理层密钥生成技术进行了深入的研究，本文前期工作也验证了物理层密钥

提取的安全性和可行性^[15], 本文主要研究基于物理层信息的信息加密和认证机制, 对物理层密钥提取过程不进行详细的说明。根据前期提出的物理层密钥生成方案^[16]选择自适应量化精度 $L = \lceil 2^{I(H_{AB}, H_{BA})} \rceil$, 其中 $\lceil \cdot \rceil$ 表示取整, H_{AB} 和 H_{BA} 分别表示 Bob 和 Alice 提取的信道特征。随后采用均匀量化器对 H_{AB} 与 H_{BA} 进行量化产生物理层密钥。消息认证开始之前, 假设合法通信方已经通过身份认证建立信任关系, 并已经提取到了一组与位置相关的一致的物理层密钥 $K_Z = \{z_1, z_2, \dots, z_N\}, z_i = 0, 1$, 用于生成物理层种子密钥。

如图3所示, Alice 将身份密钥 K 和物理层密钥 K_Z 通过散列函数生成物理层种子密钥 $Seed_A$, Bob 通过同样的方法生成 $Seed_B$, 即

$$Seed_A = Seed_B = \text{hash}(K, K_Z) \quad (3)$$

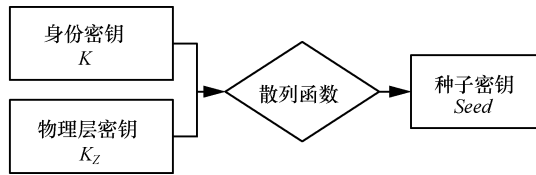


图3 物理层种子密钥生成方法

3.3 消息加密

考虑到数据吞吐量的增加, 消息加密和认证过程要求尽量简单, 尽可能减少对时延和计算开销的影响, 故采用流密码的方式用 $Seed_A$ 对发送消息 $Message$ 提供保护。流密码为对称加密完美保密性的实现提供了一种可行的方案, 其主要思想是将密钥流和明文通过逐位处理操作得到密

文, 最简单的处理方法是异或计算。作为一种对称加密算法, 流加密方法简单、加密速度快, 可以通过硬件实现, 并且能够在传输过程中不产生错误扩散, 同时可以对原始明文的统计特性进行扰乱。

如图4所示, 为了将较短的种子密钥比特扩展成足够长的密钥流以实现数据的保护, Alice 使用密钥流生成器产生密钥流 $s_A = E(Seed_A)$, 并通过逐位异或 (XOR) 处理将密钥流 s_A 添加到要发送的消息 $Message$ 上生成密文数据流 c_A 。

$$c_A = Message \oplus s_A \quad (4)$$

随后 c_A 经过信道 h_{AB} 发送给接收方 Bob。Bob 通过相同的步骤产生密钥流 $s_B = E(Seed_B)$, 并将密钥流 s_B 与接收消息密文 c_B 进行逐位异或, 得到接收的消息 $Message'$, 即

$$Message' = c_B \oplus s_B = Message \oplus s_A \oplus s_B \quad (5)$$

3.4 消息认证

如果 Bob 收到的消息来自合法通信方, 即 $s_A = s_B$, 并且在信道 h_{AB} 传输过程中没有产生错误, 则 $Message' = Message$, 密钥流可以完全抵消; 如果消息来自攻击者, 由于攻击者无法产生与发送者相同的密钥流, 即 $s_E \neq s_B$, 则此时接收的消息 $Message' \neq Message$ 。因此, Bob 可以通过检测 $Message'$ 中是否产生了错误比特对接收消息的真实性和完整性进行认证。具体的认证过程通过循环冗余校验码 (CRC, cyclic redundancy check) 实现, 假设原始消息 $Message$ 是一个 k bit 二进制数据序列, CRC 校验的基本原理是在

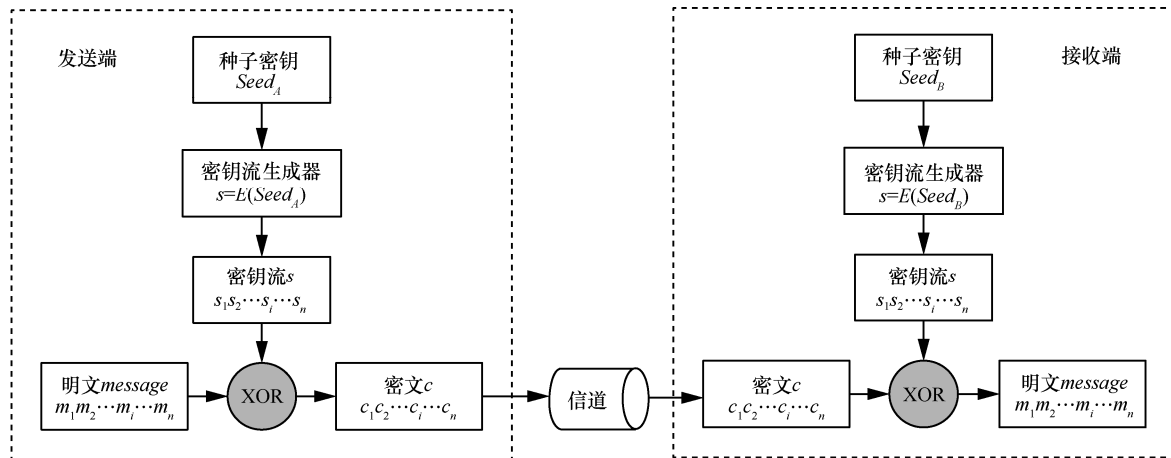


图4 利用密钥流对消息加密

Message 后附加一个与消息内容有某种特定关系的 r bit 二进制校验码, 添加校验码后的消息序列的总长为 $n = k + r$ 。如果接收消息由于受到攻击或噪声影响等原因使比特序列中的一个或多个位发生翻转, 数据序列和校验码的对应关系将不再满足。因此通过检查这种特定的对应关系是否成立即可对接收消息是否产生了错误位进行检验。

假设要发送的消息 $M(x) = \{M_0 M_1 \cdots M_k\}$, 采用的 CRC 生成多项式为 $G(x) = g_0 x^0 + g_1 x^1 + \cdots + g_r x^r$, 得到 CRC 校验码 $C_r(M(x))$, 并附在 $M(x)$ 后面组成发送的消息 *Message*。

接收者收到 *Message* 后, 通过 $G(x)$ 进行 CRC 校验, 如果 CRC 校验通过, 此时认为 $s_A = s_B$, 消息认证成功; 否则, CRC 校验不通过, 认为 $s_A \neq s_B$, 该消息作为不可靠的消息不被接收, 消息认证失败。因此, 可以通过 CRC 实现认证判决。

CRC 具有良好的检错特性, 并且具有线性的计算复杂度。CRC 具有如下检错特点: 单比特错误一定可以被检测, 可以以 $1 - \frac{1}{l^r}$ 的概率检测出成对错误, 可以以 $1 - 2^{-r}$ 的概率检测出其他错误, 如果含有 $x+1$ 因子可以检测出所有的奇数错误^[17]。表 1 列出了几个常用的 CRC 多项式及它们的主要性能。 r 表示 CRC 的比特数, l^* 表示生成多项式的周期。

表 1 常用的 CRC 生成多项式

生成多项式	数值式	r	l^*
$x+1$	0x3	1	1
x^2+1	0x5	2	2
x^4+x^2+x+1	0x17	4	7
x^8+x^2+x+1	0x107	8	127
$x^{16}+x^{12}+x^5+1$	0x11021	16	32767
$x^{16}+x^{15}+x^2+1$	0x18005	16	32767

4 安全性分析与仿真

本节针对本文所提方案的安全性进行分析与仿真验证, 假设 Eve 能够采取 2 种攻击方式: 被动窃听和主动攻击。Eve 采用被动窃听攻击时, 窃取 Alice-Bob 间的通信数据分组, 并试图通过概率分析等手段获取消息内容或用户的身份密

钥; 采用主动攻击时, Eve 通过发送虚假数据分组的方式进行攻击, 试图骗过 Alice 或 Bob 的认证, 使其接受虚假消息。

4.1 抗被动窃听的安全性

文献[10-12]提出的认证方案, 虽然利用了物理层信道信息, 但仅限于对消息来源真实性的判别, 没有考虑消息私密性的保护, 当 Eve 进行被动式窃听攻击时, 该消息认证方法与传统认证机制相比没有额外的安全增益, 消息的私密性面临的威胁仍然存在。

本文所提的方法利用信道信息对消息内容加密保护, 由于 Eve 与 Bob 的位置不同, 当 Eve 与 Alice 及 Bob 间的距离大于半个信号波长时, 可以认为窃听信道 h_{AE} 与合法信道 h_{AB} 不相关。所以 Eve 无法通过窃听信道 h_{AE} 获取合法信道的信息, 因此也无法提取与合法通信方相同的物理层密钥。另外, Alice 和 Bob 的共享密钥 K 是通过安全方式预先分配的, Eve 无法获得。种子密钥由信道信息和密钥共同产生, 相当于为种子密钥提供了高层和物理层两层保障, Eve 通过密钥流分析种子密钥变得几乎不可能。此外, 本文所提的方法含有物理层信道信息和用户身份信息, 在保证种子密钥私密性的同时又具有动态性, 每产生一段密钥流种子密钥就会改变, 并且与原来的种子密钥不相关, 因此可以有效地防止密钥预测攻击。即使 Eve 分析出了一个种子密钥, 也只能获取一段消息, Eve 既不能获取在此之前和后续的通信内容, 也无法根据种子密钥获得用户身份密钥的信息。

为了验证本文所提方法产生密钥流的安全性, 分别用物理层种子密钥和固定种子密钥作为生成种子产生密钥流, 并采用密码学中随机性测试的方法, 对 2 种方法产生的密钥流分别进行随机性测试。根据 NIST 的测试方法, 可以对比特流进行频率测试 (FT, frequency test)、块内频率测试 (BFT, block frequency test)、累积和测试 (CST, cumulative sum test)、游程测试 (RT, runs test) 等多项测试, 每项测试后会产生一个 P -value, 当该值大于显著性水平 0.01 时, 认为该比特流通过了该项测试, 具有随机性; 否则, 不具有随机性。

图 5 为截取不同长度的 2 种密钥流的测试

P -value, 图 6 为不同长度的 2 种密钥流进行多次重复测试的随机性通过率; 图中实线为采用物理层种子生成的密钥流测试结果, 虚线为采用固定种子生成的密钥流测试结果, 可以发现, 随着密钥流长度的增加, 采用固定种子密钥产生的密钥流的 P 值与测试通过率均在下降, 说明随机性在逐渐变差, 而采用物理层种子密钥生成的密钥流的随机性依旧很好, 因此本文所提方法相比固定种子密钥的方法具有明显的优势。

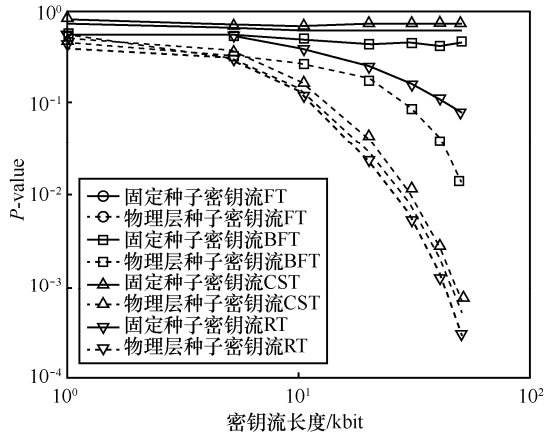


图 5 随机性测试 P -value

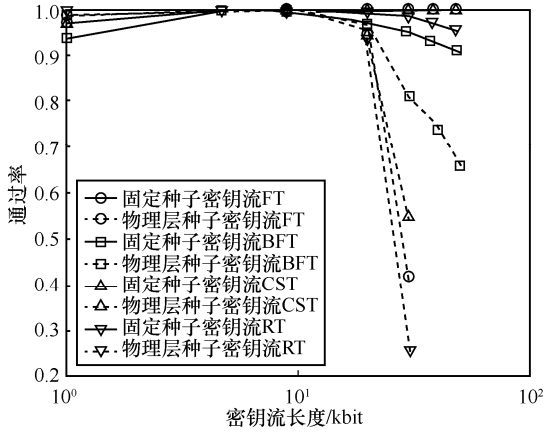


图 6 随机性测试通过率

4.2 抗主动攻击的安全性

抗主动攻击安全性可以通过虚警率和攻击率表示。虚警率为对 Alice 认证失败的概率, 即 Bob 误判 Alice 发送的数据分组非法的概率, 这是由噪声等因素导致双方提取的信道特征不一致, 从而使产生的密钥流存在错误位造成的; 攻击率为 Eve 攻击成功的概率, 即 Bob 没有检测出 Eve, 误判 Eve 发送的数据分组合法的概率。

虚警率用来表征将合法通信方误判定为攻击

者的概率。在没有噪声的理想信道中, 接收方收到的消息与发送方完全相同, 造成 CRC 校验不通过的原因只有接收消息不是 Alice 发送的原始消息, 即遭到了 Eve 的攻击, 此时虚警率为 0。但是理想信道在实际中是不存在的, 信道中的噪声也会造成接收消息与发送消息的不同, 下面对采用 PSK 调制时, 该认证方法的虚警率进行分析。对任意 M 进制信噪比为 u 的 PSK 信号, 误码率为^[18]

$$P_e = 1 - \frac{1}{2\pi} \int_{-\frac{\pi}{M}}^{\frac{\pi}{M}} e^{-u} [1 + \sqrt{4\pi u} \cos \theta e^{u \cos^2 \theta}] \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\sqrt{2u} \cos \theta} e^{-\frac{x^2}{2}} dx d\theta \quad (6)$$

当 M 较大时

$$P_e \approx \operatorname{erfc} \left(\sqrt{u} \sin \frac{\pi}{M} \right) \quad (7)$$

由于认证数据是基于比特的, 只要有一个比特传输错误, 则认证失败, 因此, 采用 MPSK 调制时的虚警率可表示为 $\alpha_{\text{MPSK}} = 1 - (1 - P_e)^{N/\log(M)}$, 与基于消息认证码方法的虚警率相同, 通过采用适当的信道纠错编码, 可以进一步降低认证的虚警率, 从而提高认证性能。

漏检率即认证方误将虚假消息判定为合法消息的概率。Eve 由于无法从接收的消息中获取密钥流和生成种子的信息, 只能采取对接收消息进行随机篡改或者猜测种子生成替换消息的方式进行攻击。

传统的消息认证码可以以 $1 - 2^{-r}$ 的概率检测出任何错误模式^[18], 本文所提方法的主要优点是利用了 CRC 校验, 从而保证可以检测出每个单个错误, 并可以以 $1 - \frac{1}{l^*}$ 的概率检测出成对错误, 以

$1 - 2^{-r}$ 的概率检测出其他错误模式, 生成多项式含有 $x+1$ 因子时可以检测出所有的奇数错误。假设接收消息含有 N 比特 (N 为偶数), 每比特出错是独立事件且概率相同, 记为 p , 则该消息共有 $N+1$ 种错误模式, 如表 2 所示。

采用传统的消息认证码的漏检率为

$$\beta_{\text{MAC}} = 2^{-r} \sum_{i=1}^N C_N^i p^i (1-p)^{N-i} = 2^{-r} (1 - (1-p)^N) \quad (8)$$

本文所提方法的单比特错误漏检率为

$$0 \cdot C_N^1 p^1 (1-p)^{N-1} \quad (9)$$

成对错误漏检率为

$$\frac{1}{l^*} C_N^2 p^2 (1-p)^{N-2} \quad (10)$$

奇数错误漏检率为

$$0 \cdot \sum_{i=2}^{\frac{N}{2}} C_N^{2i-1} p^{2i-1} (1-p)^{N-(2i-1)} \quad (11)$$

其他错误漏检率为

$$2^{-r} \sum_{i=2}^{\frac{N}{2}} C_N^{2i} p^{2i} (1-p)^{N-2i} \quad (12)$$

由式(9)-式(12)可得, 本文所提方法总的漏检率为

$$\begin{aligned} \beta_{PHY} &= 0 \cdot C_N^1 p^1 (1-p)^{N-1} + \frac{1}{l^*} C_N^2 p^2 (1-p)^{N-2} + \\ &2^{-r} \sum_{i=2}^{\frac{N}{2}} C_N^{2i} p^{2i} (1-p)^{N-2i} + 0 \cdot \sum_{i=2}^{\frac{N}{2}} C_N^{2i-1} p^{2i-1} (1-p)^{N-(2i-1)} \\ &= \left(1 - \frac{1}{l^*}\right) C_N^2 p^2 (1-p)^{N-2} + 2^{-r} \sum_{i=2}^{\frac{N}{2}} C_N^{2i} p^{2i} (1-p)^{N-2i} \quad (13) \end{aligned}$$

采用 $x^{16} + x^{12} + x^5 + 1$ 作为 CRC 生成多项式, 此时 $r=16, l=32767$, 取 $N=1024, p \in [0, 0.01]$, 上述 2 种方法的漏检率如图 7 所示, 由图可知本文所提方法与传统的消息认证码相比具有明显的优势, 可以在不提高虚警率的情况下, 使漏检率降低为约传统方法的 $\frac{1}{2}$ 。图 8 为本文所提的方法

与文献[19]所提的基于散列方法的物理层认证机制的性能比较, 由于本文所提方法充分发掘了信道的随机性和互异性, 在相同的信噪比条件下漏检率性能具有明显优势。

表 2 接收消息的错误模式

错误比特数	概率
0	$C_N^0 p^0 (1-p)^N$
1	$C_N^1 p^1 (1-p)^{N-1}$
...	...
$N-1$	$C_N^{N-1} p^{N-1} (1-p)^1$
N	$C_N^N p^N (1-p)^0$

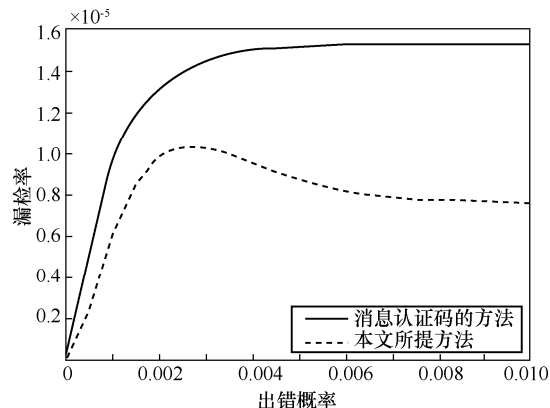


图 7 漏检率仿真结果

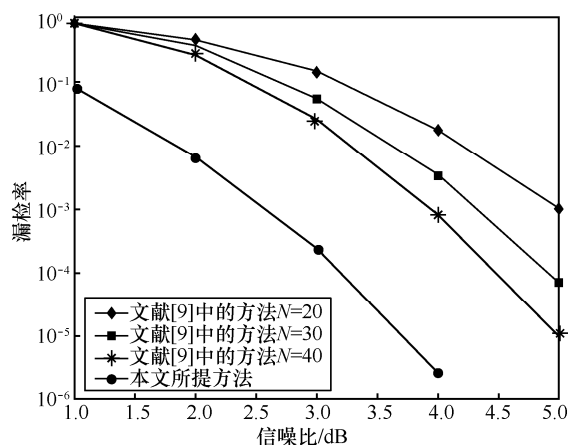


图 8 与现有方法的性能比较

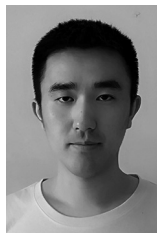
5 结束语

本文从信息比特的角度出发, 利用无线信道特征提取物理层密钥进行消息加密和认证, 利用无线信道时变性、空变性和互易性等“内生”特征, 在防止身份密钥泄露、保证消息真实性的同时, 对接收消息的完整性和私密性进行保护。该方案只需要对现有的认证方案进行较小的改动, 首先利用物理层密钥提取技术提取物理层密钥并与身份密钥结合产生种子密钥, 随后利用密钥流生成器, 根据种子密钥产生随机密钥流对发送的消息进行加密, 最后通过 CRC 校验实现对消息真实性和完整性的认证, 从而避免了现有认证机制中固定密钥带来的密钥信息泄露隐患。下一步将继续研究物理层密钥与星座置乱、循环前缀扰乱、载波抖动等方面结合, 利用物理层信道信息实现安全通信的方法。

参考文献:

- [1] DADDALA B, WANG H, JAVAID A Y. Design and implementation of a customized encryption algorithm for authentication and secure communication between devices[C]//IEEE National Aerospace and Electronics Conference. 2017:258-262.
- [2] MOHINDRU V, SINGH Y. Performance analysis of message authentication algorithms in wireless sensor networks[C]//International Conference on Signal Processing, Computing and Control. 2017: 468-472.
- [3] DANG H V, THUC N D. A privacy preserving message authentication code[C]// International Conference on It Convergence and Security. 2015:1-4.
- [4] ARAZI B. Message authentication in computationally constrained environments[J]. IEEE Transactions on Mobile Computing, 2009, 8(7):968-974.
- [5] CAO J, MA M, LI H, et al. A survey on security aspects for LTE and LTE-A networks[J]. IEEE Communications Surveys & Tutorials, 2014, 16(1):283-302.
- [6] WU X, YANG Z, LING C, et al. Artificial-noise-aided message authentication codes with information-theoretic security[J]. IEEE Transactions on Information Forensics & Security, 2017, 11(6): 1278-1290.
- [7] PATWARI N, KASERA S K. Temporal link signature measurements for location distinction[J]. IEEE Transactions on Mobile Computing, 2011, 10(3):449-462.
- [8] LAI L, EL GAMAL H, POOR H V. Authentication over noisy channels[J]. IEEE Transactions on Information Theory, 2009, 55(2): 906-916.
- [9] JORSWIECK E, TOMASIN S, SEZGIN A. Broadcasting into the uncertainty: authentication and confidentiality by physical-layer processing[J]. Proceedings of the IEEE, 2015, 103(10):1702-1724.
- [10] 张继明. 无线网络中物理层身份认证研究[D]. 武汉: 华中科技大学, 2013.
ZHANG J M. Research on physical-layer identity authentication in wireless networks[D]. Wuhan: Huazhong University of Science and Technology, 2013.
- [11] LIANG X, GREENSTEIN L, MANDAYAM N, et al. Fingerprints in the ether: using the physical layer for wireless authentication[C]// IEEE International Conference on Communications IEEE, 2007: 4646-4651.
- [12] DEMIRBAS M, SONG Y. An RSSI-based scheme for sybil attack detection in wireless sensor networks[C]// International Symposium on World of Wireless, Mobile and Multimedia Networks. 2006: 5pp-570.
- [13] LIU J, WANG X. Physical layer authentication enhancement using two-dimensional channel quantization[J]. IEEE Transactions on Wireless Communications, 2016, 15(6):4171-4182.
- [14] WEN H, WANG Y, ZHU X, et al. Physical layer assist authentication technique for smart meter system[J]. IET Communications, 2013, 7(7): 189-197.
- [15] 王旭, 金梁, 刘璐, 等. 均匀散射环境中物理层安全密钥容量分析[J]. 通信学报, 2016, 37(9):75-81.
WANG X, JIN L, LIU L, et al. Analysis of physical layer secret key capacity in the uniform scattering environment[J]. Journal on Communications, 2016, 37(9):75-81.
- [16] 戴峤, 金梁, 黄开枝. 基于信道特征量化的自适应密钥生成方案设计[J]. 通信学报, 2014(1):191-197.
DAI Q, JIN L, HUANG K Z. Adaptive key distillation from channel characteristics[J]. Journal on Communications, 2014, (1): 191-197.
- [17] LIU Y, BONCELET C. The CRC-NTMAC for noisy message authentication[J]. IEEE Transactions on Information Forensics & Security, 2006, 1(4): 517-523.
- [18] 樊昌信, 曹丽娜. 通信原理(第七版)[M]. 北京: 国防工业出版社, 2012.
FAN C X, CAO L N. Principles of communications (the seventh edition)[M]. Beijing: National Defense Industry Press, 2012.
- [19] 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 X S, YANG J, HUANG K Z, et al. Physical layer authentication scheme based on hash method[J]. Journal of Electronics & Information Technology, 2016, 38(11): 2900-2907.

[作者简介]



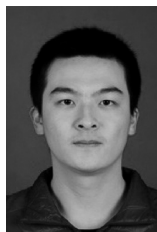
李兴志 (1994-), 男, 山东泰安人, 国家数字交换系统工程技术研究中心硕士生, 主要研究方向为物理层安全、无线通信安全。



金梁 (1969-), 男, 北京人, 国家数字交换系统工程技术研究中心教授、博士生导师, 主要研究方向为物理层安全、通信信号处理和阵列信号处理。



钟州 (1982-), 男, 吉林公主岭人, 国家数字交换系统工程技术研究中心讲师, 主要研究方向为物理层安全。



楼洋明 (1991-), 男, 浙江义乌人, 主要研究方向为物理层安全。