计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.190900095

基于物理层信道特征的无线网络认证机制

李兆斌　崔　钊　魏占祯　赵　洪　郭　超
北京电子科技学院　北京 100070
(bestibesti@163.com)

摘　要　在轻量级物联网中,针对传统认证方式存在的高能耗、高时延等问题,文中提出一种基于物理层信道特征的无线网络认证机制。该方案利用信道冲激频率响应(Channel Impulse Response,CIR)进行身份认证,并将其作为初始消息认证码(Message Authentication Code,MAC)进行消息认证;采用"哈希链"迭代的方式生成标签信号,进而实现 MAC 的更新,提高通信双方对数据包调换、篡改等攻击行为的敏感度;将身份认证与消息认证、标签信号与数据包紧密结合,适用于工业物联网、智能家居等安全要求高、设备资源有限的通信环境。安全性分析与仿真结果表明,与 HMAC(Hash-based Message Authentication Code)、祖冲之完整性算法(EIA3)等相比,该方案的认证时延较短,具有一定的实用性。

关键词:物理层信道特征;消息认证码;标签信号;身份认证;消息认证
中图法分类号　TP309

Wireless Network Authentication Method Based on Physical Layer Channel Characteristics

LI Zhao-bin,CUI Zhao,WEI Zhan-zhen,ZHAO Hong and GUO Chao
Beijing Electronic Science and Technology Institute,Beijing 100070,China

Abstract　In lightweight Internet of Things (IoT),the traditional authentication method has problems such as high energy consumption and high delay. Therefore,this paper proposed a wireless network authentication mechanism based on physical layer channel characteristics. The channel impulse frequency response (CIR) is used for identity authentication,and it is used as the initial message authentication code (MAC) for message authentication. It uses "Hash chain" to generate tag signals,so as to realize MAC updating and improve the sensitivity of packet exchange,tampering and other attacks. This method combines identity authentication with message authentication,tag signal and communication information,and is suitable for the communication environment with high security requirements and limited equipment resources,such as industrial Internet of Things and smart home. The security analysis and simulation results show that compared with HMAC,EIA3 and other algorithms,the authentication delay of this scheme is small and it has certain practicability.

Keywords　Physical layer channel characteristics,Message authentication code,Label signal,Identification,Message authentication

1　引言

随着无线网络技术的不断成熟及其规模的不断壮大,无线网络在人们的生活中发挥着愈发重要的作用。然而,与有线网络相比,无线网络中的数据更容易受到攻击者的监听和破坏。而认证是通信安全的第一道防线,也是成功运用其他安全保护措施的前提。一般来说,认证包括用户的身份认证和消息认证,前者用于鉴别用户身份,后者用于保证消息的完整性和不可抵赖性。现有的认证技术都是将安全逻辑协议和密码算法相结合,这些技术在保证通信实体安全的同时,带来了较高的计算负荷与资源消耗,这在物联网等通信实体计算能力有限的网络中是难以应用的。

文献[1]指出传统的高层认证需要使用非对称算法交换会话密钥,计算时间长。在物联网环境中,这对于大部分对响应时间要求严格的应用程序是不可接受的。另一方面,若在嵌入式设备中实现非对称算法,也将造成不可忽略的内存空间开销,即使采用对称算法,通信双方需要依赖伪随机数生成器或根据用户指定输入来生成具有高熵的对称密钥,但由于种子或用户给定输入的高可预测性和密钥生成算法的确定性,这些方法无法提供足够的熵[2]。除此之外,在无线环境中攻击者可采用伪装手段,在通信双方"透明"转发数据,并在后台进行数据分析,可暴力破解或修改相关参数。而且现有的认证体系大多部署在高层,合法通信双方无法感知这种通信链路的改变。上述问题都会给无线网络认证和数据带来安全隐患。

近年来,物理层安全技术利用无线信道的唯一性、互易

到稿日期:2019-09-16　返修日期:2019-12-27　本文已加入开放科学计划(OSID),请扫描上方二维码获取补充信息。
基金项目:国家重点研发计划项目(2017YFB0802705,2017YFGX110123);中央高校基本科研业务费项目(328201911)
This work was supported by the National Key Research and Development Project (2017YFB0802705,2017YFGX110123) and Fundamental Research Funds for the Central Universities (328201911).
通信作者:崔钊(xtcz_3103@163.com)

性、多样性等特点，为安全认证提供了新思路。物理层安全技术的核心思想是利用合法信道与窃听信道的区别，在物理层实现数据保密，而信道是由无线介质固有的随机性(如信道衰落、噪声等)或人为设计的传输策略产生的。与基于加密的安全技术不同，物理层安全技术降低了计算复杂度和资源消耗，因为该技术不严重依赖于移动设备的计算能力[1]。Xiao等[3-4]提出了基于“信道指纹”的认证方法，在高层实现初次认证后，对后续数据包采用基于无线信道特征指纹的物理层认证方法，即在短时间内通过比较前后两次数据包的信道特征是否一致，来判断通信链路是否受到攻击。文献[5-7]提供了物理层密钥生成思路。文献[8-11]紧密结合了物理层信道特征与高层认证流程，将量化后的信道特征作为参数参与高层认证。

当前复杂的应用层信令标签认证不适应高速连接、高可靠性的传输要求与发展趋势。文献[12]提出了一种新的MAC生成方式，用于实现电力系统中GOOSE报文的认证。文献[13]设计了新的动态化会话密钥，并用祖冲之算法实现物联网中的双向认证。文献[14]将哈希链插入连续的数据包，保证了认证的连续性。然而，上述方法不能保证MAC与消息的严格同步，若中间人改变哈希链与数据包的对应顺序，则接收方不能及时发现；若更改哈希值，则接收方可能将正确的数据包丢弃，降低了认证效率。

基于此，本文提出了一种基于物理层特征的消息认证方案。在多径丰富的物联网环境下，通信双方提取信道特征，利用预共享密钥加密来实现身份互认证。在初次消息认证过程中以信道特征为初始MAC，“绑定”通信消息，生成标签信号，在接下来的通信中利用上一步生成的标签信号与消息更新MAC。从计算开销角度来看，双方只需要结合共享密钥与信道特征，增加认证维度，并采用对称密码方法即可实现身份认证。安全性分析和仿真结果表明，双方将消息与标签牢牢“绑定”在一起，可抵抗多种中间人攻击，可保证MAC与消息的严格同步。与HMAC、EIA3等消息认证算法相比，本文方案的计算开销小，认证时延明显缩短，有较好的认证性能。

2 系统模型

系统模型如图1所示，其中用户A和B是合法用户，E是窃听者。假设E知道A和B通信时使用的时隙、频段、调试解调方式等信道参数。其中，A与B，A与E，B与E之间存在着经反射体反射后的无线通信信道，其可模拟为多径衰落信道。以用户A与用户B为例，$\boldsymbol{h}_{BA}$是B向A通信的信道特征，$\boldsymbol{h}_{AB}$是A向B通信的信道特征。K是A和B之间的预共享密钥，用于初始身份认证，且仅A和B可知。E在无线环境中可接收用户A和B发出的消息，并进行消息转发。

A和B通过高层共享密钥K建立信任关系，而E与合法用户A和B间不存在相互认证。攻击者E可“串接”在二者间，进行透明转发并窃听数据。E在收集到大量信息样本后，可伪装成A或B向对方发送虚假信息，以达到攻击的目的。

该模型结合共享密钥K与物理层信道特征，来实现初次身份认证；随后结合MAC与通信消息，实现消息认证；可通过信道特征更新实现初始MAC的不断更新。当身份认证或消息认证失败时，用最新生成的MAC继续进行认证。

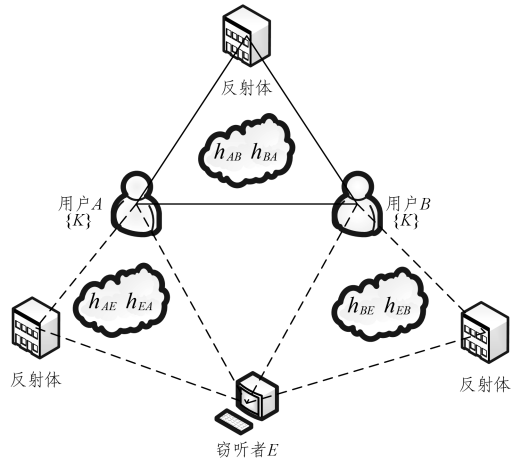


图1 系统模型

Fig. 1 System model

3 基于物理层特征的认证方法

本文的物理层认证用于鉴别不同的发送者，而且必须同传统的握手认证结合才能完备地识别一个实体，因此可以将所提方法看作认证的跨层设计方法。发送端产生标签信号与通信信号，接收端可正常接收并检验信号。为了更好地描述本文方案，表1列出了各符号的含义。

表1 本文方案的符号含义

Table 1 Label meaning of proposed scheme

符号	含义
K	预共享密钥
RES	身份认证消息
k	认证门限
L	信道检验统计值
$\boldsymbol{h}_{AB}$	A到B的信道特征
M	信道特征长度
h_{new}	新认证的信道特征
E_K	加密运算符
D_K	解密运算符
$h(,)$	哈希运算符
H_n	第n个标签信号
H_n'	收到的第n个标签信号
C_n	第n个信息
C_n'	收到的第n个信息

本文提出利用物理层信道冲激响应(CIR)进行认证的方案，其包含4个部分：信道特征交换、身份认证、消息认证、认证更新。具体认证过程如图2所示。

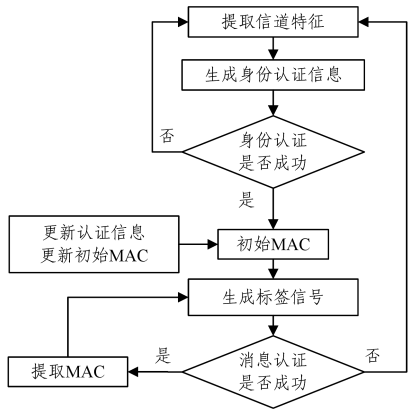


图2 认证流程

Fig. 2 Certification process

3.1 信道特征交换

信道特征是实现本文认证方案的基础，交换信道特征相当于无线网络中的密钥预分配过程[15]。以用户 A 主动向用户 B 发起认证为例，具体流程如图 3 所示。图 3 中，实线箭头表示 A 和 B 发送消息的过程，虚线箭头表示数据处理过程。

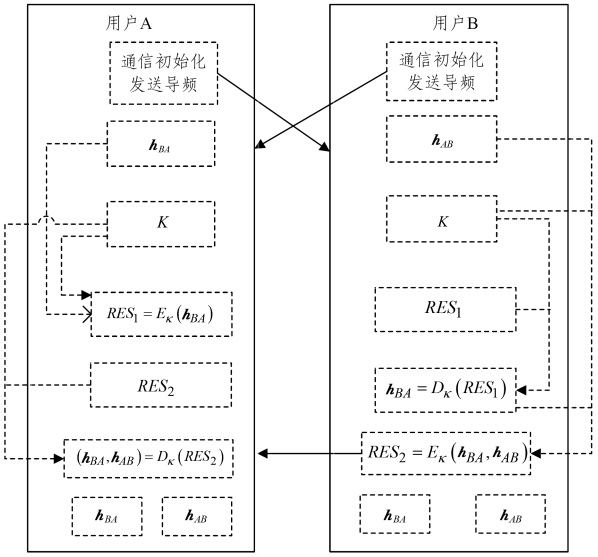


图 3 信道特征交换

Fig. 3 Channel feature exchange

3.1.1 处理导频信号

在通信双方初始化后，互相发送冲激导频信号。以 A 处理导频为例，多径衰落信道[16]可表示为 $h(t)=\sum_{n=1}^{T}c_n e^{j(2\pi f_n+\vartheta_n)}$，其中 ϑ_n 为第 n 条路径的相位，c_n 为相对应的衰减量，T 为路径数。A 提取 CIR 曲线得到 $H_A(f)$，$H_A(f)$ 可表示为：

$$H_A(f)=H(f)+N_A(f) \tag{1}$$

其中，$H_A(f)$ 为 A-B 信道的实际 CIR，当路径数 T 趋于无穷大时，$H_A(f)$ 可等效为服从 $(0,\sigma_H^2)$ 的复高斯随机过程；$N_A(f)$ 为噪声，服从 $(0,\sigma_N^2)$ 的复高斯分布。

A 对 $H_A(f)$ 进行 N 点采样，若 N 与采样间隔足够大，则采样值 H_A 可用于表征 $H_A(f)$，且每个采样值都独立服从 $(0,\sigma_H^2)$ 的复高斯分布。

将长为 N 的 H_A 映射为长度为 M 的哈希矢量，即 $\boldsymbol{h}_{BA}=[\boldsymbol{P}_1,\boldsymbol{P}_2,\cdots,\boldsymbol{P}_M]$，$N>M$。每个元素 $\boldsymbol{P}_m$ 的计算方式如下：

$$P_m=a\sum_{i=1}^{N}H_{A_i}\cos(2\pi m(i-1)/N) \tag{2}$$

其中，$m=1,2,\cdots,M$。由于 H_A 元素服从 $(0,\sigma_H^2)$ 的复高斯分布，因此每个元素服从均值为 0、方差为 $\frac{a^2\sigma_H^2}{2}N$ 的复高斯分布。

B 以同样的方式处理从 A 发来的冲激导频，并生成 $\boldsymbol{h}_{AB}$。

3.1.2 获取信道特征

双方处理完导频消息后，A 用密钥 K 将量化得到的 $\boldsymbol{h}_{BA}$ 加密，将加密结果发送至 B。B 收到 RES_1 并用密钥 K 解密后得到 $\boldsymbol{h}_{BA}$。

$$RES_1=E_K(\boldsymbol{h}_{BA}) \tag{3}$$

此时，用户 B 需要对用户 A 进行身份认证，具体过程见第 3.2 节。若认证成功，则将 $\boldsymbol{h}_{BA}$ 与 $\boldsymbol{h}_{AB}$ 一并加密发送给 A，此时 A 和 B 都获得了 $\boldsymbol{h}_{BA}$ 与 $\boldsymbol{h}_{AB}$。

3.2 身份认证

身份认证为消息认证提供安全可靠的初始 MAC，这是提高本文方案安全性能的关键，其具体流程如图 4 所示。

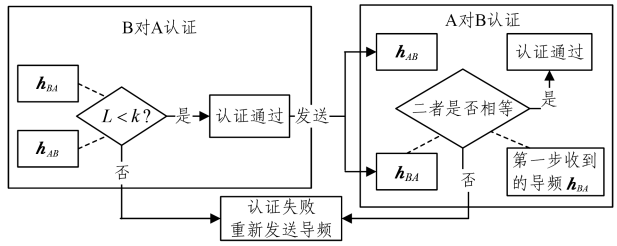


图 4 身份认证

Fig. 4 Identity authentication

由第 3.1 节可知，用户 B 收到 $\boldsymbol{h}_{BA}$ 后，B 对 A 进行身份认证。由于噪声及量化误差的影响，B 需要比较 $\boldsymbol{h}_{BA}$ 与 $\boldsymbol{h}_{AB}$。B 通过一个简单的假设检验[17]来判断用户 A 是否合法。为了进行假设检验的判决，需要两个参与比较的参数。以检验统计值 L 来刻画两者的不一致程度，以认证门限 k 为标准参数，则有：

$$\begin{cases}\text{若 } L<k, & \text{认证通过}\\ \text{若 } L>k, & \text{认证失败}\end{cases} \tag{4}$$

检验统计值 L 的计算式如下：

$$L=\min_{\phi}\frac{1}{\sigma^2}\sum_{m=1}^{M}|H_{BAm}-H_{ABm}e^{j\phi}|^2 \tag{5}$$

其中，ϕ 表示前后两次信道频率响应间的相位差。

根据式(4)，若 B 对 A 的身份认证通过，则 B 向 A 发送 $\boldsymbol{h}_{BA}$ 与 $\boldsymbol{h}_{AB}$。此时，$\boldsymbol{h}_{BA}$ 可以看作 PKI 认证模型中服务器与客户机之间的随机数[18]。

A 通过对比前后收到的 $\boldsymbol{h}_{BA}$ 是否一致来判断信息源 B 是否合法。若两次收到的信道特征一致，则 B 通过 A 的身份认证，并用 $\boldsymbol{h}_{AB}$ 实现消息认证，具体过程见第 3.3 节。

在双向身份认证过程中，无论哪个环节出现失败，做废此时的 $\boldsymbol{h}_{BA}$ 与 $\boldsymbol{h}_{AB}$，通信双方重新互发导频，交换信道特征。

3.3 消息认证

通过身份认证后，A 与 B 共有信道特征 $\boldsymbol{h}_{AB}$，双方以 $\boldsymbol{h}_{AB}$ 为消息认证的“可信根”。下面以用户 A 的首次消息认证为例介绍具体的消息认证过程。

步骤 1 双方将 $\boldsymbol{h}_{AB}$ 作为初始 MAC，即 $MAC_A=MAC_B=\boldsymbol{h}_{AB}$。$A$ 结合通信信号 C_1 进行 hash 运算，生成标签信号：

$$h_1=h(MAC_A,C_1) \tag{6}$$

再将标签信号与通信信号叠加，即 (h_1,C_1)，并发送至 B。同时更新 MAC，$MAC_A=h_1$。

步骤 2 B 收到信号解调后得到 h_1' 与 C_1'，对 A 进行消息检验。B 将 $\boldsymbol{h}_{AB}$ 与 C_1' 进行 hash 运算，得到：

$$H=h(MAC_B,C_1') \tag{7}$$

当 $H=h_1'$ 时，若标签信号相同，则消息认证成功，并将 h_1' 作为新的消息认证码，$MAC_B=h_1'$。

步骤 3 A 结合 h_1 与 C_2 做 hash 运算，生成新的标签信号，即：

$$h_2=h(MAC_A,C_2) \tag{8}$$

再将标签信号与通信信号叠加，即(h_2，C_2)，并发送至 B。B 对 A 进行消息检验的方法与上文相同。

在 A 和 B 之后的连续通信中，消息验证方式都是如此，若标签信号验证失败或停止产生消息，则重新进行身份认证。整个消息认证过程如算法 1 所示。

算法 1 消息认证

输入：信道特征 $\mathbf{h}_{AB}$

输出：消息认证结果

1. 初始状态 $h_0=\mathbf{h}_{AB}$，$n=1$。
2. 发送方：产生消息 C_n，若无消息，则转步骤 4；生成标签信号 $h_n=h(h_{n-1},C_n)$；发送(h_n，C_n)。
3. 接收方：收到 h_n' 和 C_n'；计算 $H=h(h_{n-1},C_n')$。若 $H=h_n'$，则 C_n 消息认证成功，$n=n+1$，然后转步骤 2；若 $H\neq h_n'$，则 C_n 消息认证失败，转步骤 4。
4. 消息认证结束，双方继续互发导频，更新初始 MAC。

3.4 认证更新

在 TDD 系统中，一般相邻的帧之间的信道满足互易性，如果间隔时间超过几个数据帧的长度，则可以认为信道发生了改变。另外，信道也会受到外界不确定因素的干扰而产生变化。因此，A 和 B 在连续进行数据通信时，也要保持导频信号的正常发送与信道量化估计，定时进行身份认证。其一方面为了确保消息来自正常用户；另一方面，通过消息认证更新初始 MAC，以提高中间人转发攻击的难度。

在该方案中，若在通信过程中出现了较长的间隔，则重新互发导频交换信道特征。

若标签信号验证不匹配，即消息认证未通过，则将当前最新的已通过身份认证的信道特征 h_{new} 作为初始 MAC，即在算法 1 中有：

$$h_0=h_{new} \tag{9}$$

具体的认证更新流程如图 5 所示。

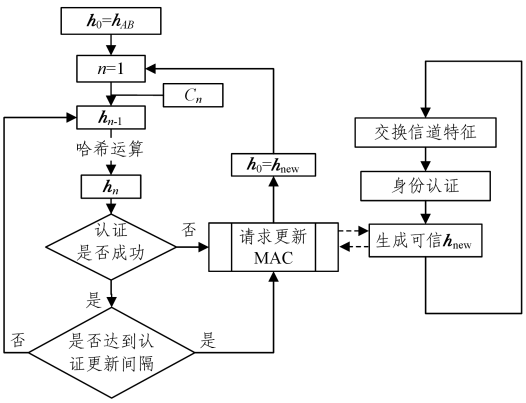


图 5 认证更新过程

Fig. 5 Process of certification update

4 认证方案分析

4.1 双向认证

在高层双向认证过程中，需要产生大量的随机数作为认证参数，而目前该过程均是伪随机进程，容易遭到暴力破解[19]。由于用户位置变化，各种反射体、衍射体等客观存在，接收信号为不同时延的多径之和，量化后物理信道特征有着较好的随机性[20]。

本文方案使用量化后的物理层信道参数(如信号相位、射频等)来代替随机数作为认证参数，并将其嵌入到高层认证流程。通信双方用预先共享密钥 K 加解密信道特征来实现双方的身份验证。在消息认证过程中，MAC 是用“类哈希链”方式生成的，通信双方用之前验证成功的信道特征与新收到的消息做哈希运算，以验证消息来源的合法性。另一方面，预共享密钥 K 是双方共有的，K 的高安全性使得仅 A 和 B 可破解身份认证消息，以在后续消息认证中保障双方都可安全获得相同的初始 MAC。

4.2 抗攻击

没有 E 时，A 和 B 间提取的信道特征大致一致，并且其余实体无法复制。若 E 存在，则 E 收到传递信号后可进行重放伪造替代等攻击行为。

4.2.1 被动攻击

在本文模型中，身份认证过程的“随机数”从时变信道中提取。在无线介质中，信道衰落、噪声等固有的随机性或其他人为干扰都会导致信道改变。此外，在多径丰富的典型无线环境下，信道响应具有位置特异性，即只要两条收发路径的间隔超过一个以上的射频波长，就可以认为这两条路径的信道响应不相关，因此每次认证时的信道特征是不一致的，窃听者无法根据相关性推测出下一次通信的信道特征。因此，若合法用户前后收到相同的认证消息，或者认证参数检验失败，则可判断该通信请求异常而不予以响应。

4.2.2 转发攻击

在消息认证中，h_n 为：

$$h_n=h(h_{n-1},C_n) \tag{10}$$

由于哈希函数具有较好的单向性，每次通信时信息互不相关，每次认证中的标签信号都不相关，因此即使 E 窃取了(h_n，C_n)并试图发起请求，也很难由 h_n 与 C_n 推出合法 h_{n-1}。

若 E 伪造合法标签信号发起攻击，则根据相关研究[21]，攻击成功率为：

$$P_l=\sum_{i=1}^{M}C_M^i\left(\frac{1}{2}\right)^M \tag{11}$$

从信息论的角度来看，E 缺少 A 和 B 从物理层信道获取的安全熵[2]，即使窃听了小部分物理层密钥，仍然有绝大部分密钥信息未知。若 E 拥有大量样本和强计算能力，其可用盲估计[22]的方法获取大部分甚至全部的导频信号。但这种情况的可能性极小，因为只有在样本达到一定数量时才能计算出发送的信号，而样本不够时不足以构成威胁。盲估计的威胁是一个突变的过程，也就是说在样本达到相应数量前，攻击者只能猜测导频信号，其攻击能力一直处于较低的水平。

即使 E 破解身份认证中的信道特征，即初始 MAC，在更新认证参数的间隙也会受到计算能力和时间的局限，依靠猜测很难及时破解信道特征。当 E 无法跟上合法参数的更新速度时，也就无法窃取通信过程的所有消息。除此之外，中间人转发攻击很可能叠加更多的噪声，有用信号的功率比例降低，这也给 E 的攻击增加了难度。

4.3 消息认证码与数据包严格匹配

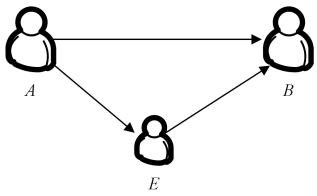
文献[14]提出发送方向接收方发送数据前，首先要自发地产生一个哈希链，即：

$$H_n(K_n)=K_{n-1} \tag{12}$$

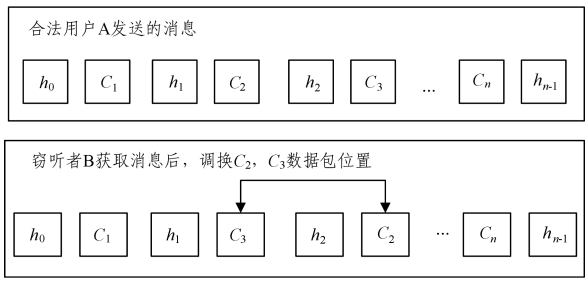
然后分别将 K_{n-1} 插入数据包 X_n，接收方通过计算能否将

K_n 哈希还原到K_0 来判断X_{n+1}是否来自合法方。由于哈希函数具有良好的单向性，若窃听者不知合法通信方使用的具体哈希算法，即使截获多组数据包，也很难还原出数据内容。

然而，倘若窃听者 E 得知通信双方具体使用的哈希算法，即使窃听者不能破解哈希链，也可根据最终哈希值的比特数，成功地将哈希链与数据包分开。这样一来，在保持哈希链不变的情况下，攻击者可以改变数据包的前后顺序，甚至改变数据包的内容。由于哈希链顺序不变，接收方收到消息后可将K_n 哈希还原到K_0，即误将窃听者发来的消息X_{n+1}判断为其来自合法方。当通信结束时，接收者收到的数据包顺序可能与正常发送时的顺序不同。这一攻击行为较为隐蔽，以窃听者调换数据包顺序为例，具体攻击原理如图 6 所示。消息验证过程如图 7 所示。



(a)攻击模型



(b)攻击原理

图 6 消息认证攻击

Fig. 6 Attack of message validation

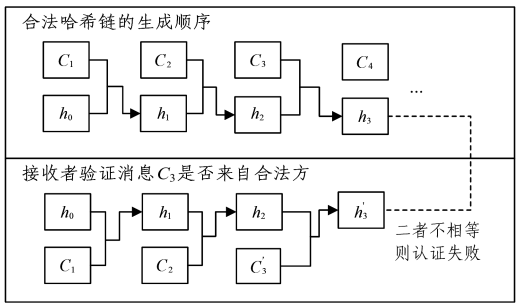


图 7 消息验证过程

Fig. 7 Process of message validation

窃听者 E 劫取发送者 A 的消息后，分离每个消息中的 MAC 与数据，保持 MAC 不变，改变C_2 和C_3 的顺序，再重新与合法接收者 B 通信。由图 6 可知，接收者 B 收到消息，并根据哈希链确认通信消息合法，却不知原消息已被修改，误将原消息认为$[C_1, C_3, C_2, \cdots, C_n]$，存在安全隐患。

本文方案结合物理层信道特征，将 MAC 与数据包产生关联。由哈希函数原理可知，若 MAC 值是由数据包参与生成的哈希值，不论是数据包本身发生变化，还是数据包顺序发生变化，最终产生的哈希链都将大不相同。若存在中间人攻击，数据包顺序被调换，则接收方收到消息后可计算：

$$H = h(h_{n-1}, C_n) \tag{13}$$

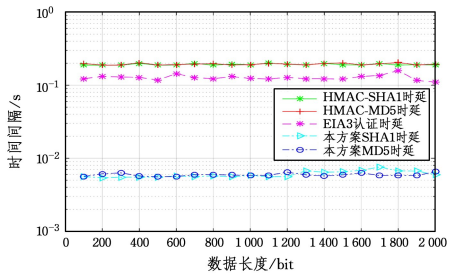
判断消息C_n 是否来自合法方。由于通信双方共有h_{n-1}，若消息C_n 发生变化，则最终计算出的 H 与合法h_n 不匹配，即可判定消息C_n 来自非法用户。

5 仿真结果

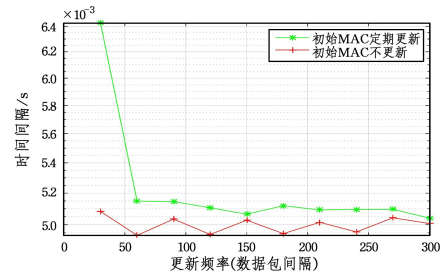
在功率约束值 $E_s = 2$ 的 BPSK 调制环境下，将本文方案分别与采用 MD5、SHA1 算法的 HMAC 针对平均消息认证时延进行对比，同时也与 EIA3 算法进行对比。在仿真中，通信双方相互进行 N 次消息认证的过程可转化为其中一方连续认证 $2N$ 个数据包的过程。假设这 $2N$ 个数据包的长度相同，同时更新 HMAC 中的算法密钥，更新周期与数据包个数有关，且与本文方案保持一致。

连续发送多个数据包取统计平均，图 8(a)给出了数据包长度与平均认证时延的关系。从图 8 中可以看到，随着数据包长度的增加，本文方案的认证时延随之略有增加，但与 HMAC 和 EIA3 方法相比，时延数值至少小一个数量级。这是由于在传统的认证方案中，HMAC 采用动态密钥时，需要通信双方利用密钥管理协议进行密钥更新；而本文方案的初始 MAC 采用的是物理信道特征，后续采用哈希链迭代的方式更新 MAC，不需要密钥更新过程，因此认证时延较低。当数据包长度为 1 000 bit，采用 MD5 哈希算法时，本文方案用时 0.005 s，EIA3 用时 0.13 s，HMAC 用时 0.18 s。

图 8(b)以发送数据包长度为 200 bit 的 300 个数据包为例，给出了认证更新频率与平均认证时延的关系。在仿真过程中假设由于丢包、恶意攻击或定时的身份认证要求，每发送一定数量的数据包后就需要进行重新认证，通信双方重新提取物理层信道特征，更新初始 MAC 值。仿真中用不同的数据包间隔来近似表示认证更新频率。从仿真结果来看，在认证更新间隔较小的情况下，本文方案的认证时延较长，但随着认证更新间隔的增大，认证时延逐渐缩短，能满足实际需要。



(a)各算法时延仿真对比



(b)不同认证更新频率下的时延仿真对比

图 8 时延仿真对比

Fig. 8 Simulation comparison of delay

结束语 本文从通信协议的角度，提出了一种基于物理

层信道特征的身份消息认证方法，将信道特征嵌入高层认证机制中进行身份认证，并结合认证结果与通信信息不断更新MAC，合法通信方可连续进行消息认证，从而有效减小攻击者进行篡改、转发等行为的不良影响。该方案主要应用在安全等级高、计算能力有限的场景中，适用于物联网或无线环境下端到端的通信。由于不需要复杂的非对称密码算法，在安全的前提下，采用对称密码算法与哈希算法更方便应用实现。

物理层认证是一种很有潜力的安全技术，它将在未来的无线通信系统中具有广阔的应用空间。随着各种无线设备的计算能力的增强，计算开销将不再成为制约通信性能的重要因素。物理层安全认证正在从以模型为基础转向以数据为基础，其与机器学习、深度学习的结合将成为物理层安全研究的新热点。

参 考 文 献

[1] 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.

[2] PERAZZONE J, YU P L, SADLER B M, et al. Physical Layer Authentication via Fingerprint Embedding: Min-Entropy Analysis: Invited Presentation[C] // 2019 53rd Annual Conference on Information Sciences and Systems (CISS). Baltimore, MD, USA, 2019: 1-6.

[3] XIAO L, GREENSTEIN L J, MANDAYAM N B, et al. A Physical-Layer Technique to Enhance Authentication for Mobile Terminals[C] // IEEE International Conference on Communications. Beijing, 2008: 1520-1524.

[4] XIAO L, GREENSTEIN L J, MANDAYAM N B, 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.

[5] JIANG W, ANTHONY L, MOHAMMAD A F. Physical Layer Key Generation: Securing Wireless Communication in Automotive Cyber-Physical Systems[J]. ACM Transactions on Cyber-Physical Systems, 2018, 3(2): 1-26.

[6] ZHANG J Q, RAJENDRAN S, SUN Z, et al. Physical Layer Security for the Internet of Things: Authentication and Key Generation[J]. IEEE Wireless Communications, 2018, 26(5): 92-98.

[7] RAHBARI H, LIU J S, Park J M J. SecureMatch: Scalable Authentication and Key Relegation for IoT Using Physical-Layer Techniques[C] // 2018 IEEE Conference on Communications and Network Security (CNS). Beijing, 2018: 1-9.

[8] SONG H W, JIN L, ZHANG S J. Physical Layer Authentication Based on Tag Signal [J]. Journal of Electronics & Information Technology, 2008, 40(5): 1066-1071.

[9] YANG J, JI X S, HUANG K Z, et al. Cross-Layer Authentication Scheme Based on Wireless Channel Characteristics [J]. Journal of Information Engineering University, 2017, 18(3): 267-272.

[10] WANG X, JIN L, HUANG K Z. Cross-Layer Mutual Authentication Scheme Based on Physical Layer Location Information [J]. Journal of Information Engineering University, 2017, 18(3): 279-283, 304.

[11] 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.

[12] HUSSAIN S, FAROOP S M, USTUN T S. Analysis and Implementation of Message Authentication Code (MAC) Algorithms for GOOSE Message Security[J]. IEEE Access, 2019(7): 80980-80984.

[13] WANG M W, WANG L J, XIE W M. Mutual Authentication Scheme Based on Session Key in Wireless Sensor Network [J]. Application Research of Computers, 2014, 31(8): 2506-2509.

[14] YAN S N, XU L, ZENG Y L. Lightweight Physical Layer Auxiliary Authentication in Cognitive Wireless Network [J]. Computer Systems & Applications, 2019, 28(6): 22-28.

[15] YANG G, WANG J T, CHENG H B, et al. A Key Establish Scheme for WSN Based on IBE and Diffie-Hellman Algorithms [J]. Acta Electronica Sinica, 2007(1): 180-184.

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

[17] MAURER U. Authentication Theory and Hypothesis Testing [J]. IEEE Transactions on Information Theory, 2000, 46(4): 1350-1356.

[18] LIU Z G, YANG L C, PU J, et al. The System of Digital Signature Authentication Based on PKI [J]. Application Research of Computers, 2004(9): 158-160.

[19] WANG X, YU H. How to Break MD5 and Other Hash Functions[C] // Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Berlin, Heidelberg, 2005.

[20] SUI L, GUO W B, JIANG W B, et al. Generation and Extraction of Secret Keys Based on Properties of Wireless Channels [J]. Computer Science, 2015, 42(2): 137-141.

[21] SONG H W. Research on Physical Layer Security Authentication Technology in Mobile Communication [D]. Zhengzhou: PLA Strategic Support Force Information Engineering University, 2018.

[22] HUANG X J, BI H J, YU S Y. Subspace-based Blind Channel Estimation for Orthogonal Frequency Division Multiplexing (OFDM) Systems [J]. Journal of Shanghai Jiaotong University, 2004(S1): 6-9.

LI Zhao-bin, born in 1977, Ph.D, associate researcher. His main research interests include network security and so on.

CUI Zhao, born in 1995, graduate student. His main research interests include physical layer communication security and so on.