计量, 使得门限值的计算更为简单. 此外, 对初始认证后的数据包本文采用基于哈希链的认证方案, 使得在丢包情况下, 仍能实现连续的认证, 性能分析表明, 与现有的方案相比, 本文的方案只需更小的计算代价, 并且具有更高的认证准确性和认证效率, 更加适用于认知无线网络.

1 预备知识

1.1 系统模型

在基于正交频分复用 (Orthogonal Frequency Division Multiplexing, OFDM) 通信系统的单跳的认知无线网络中, 认知用户通过无线信道进行通信. 如图 1 所示, Alice 为合法的发送者, Bob 为合法接收者, 两者通过无线信道传输信息. Eve 是一个极强的攻击者, 由于无线信道的开放特性, Eve 可能对 Alice 所发送的数据包进行篡改、伪造、重放等攻击. 在 OFDM 系统中, 为了与 Bob 进行通信, Alice 在一次数据传输过程中需要发送多个数据包给 Bob. 其中, 每个数据包含多个 OFDM 符号, 每个 OFDM 由多个子载波构成. 因此 Bob 在收到 Alice 发送的数据包时, 需要对 Alice 发送的每个数据包都进行认证.

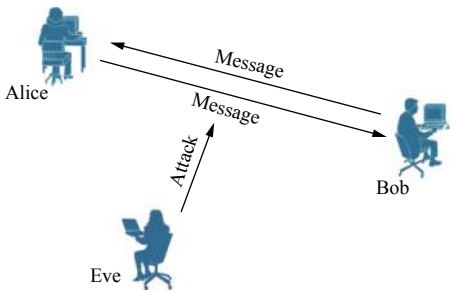

图 1 系统模型

假定在 OFDM 系统中, Alice 在一次数据传输中需要连续地给 Bob 发送 N 个数据包 $X_1, X_2, \cdots, X_N$ 以完成通信. 为了保证在一次数据传输时间内, Bob 接收的每一个数据包的合法真实性, Bob 需要对 Alice 发送的每一个数据包进行连续认证. 对于 Alice 发送的第 1 个数据包, Bob 首先通过密码学认证技术完成对 Alice 的初始认证 (具体方案在 2.1 节介绍). 其次, 由于 Alice 与 Bob 是在 OFDM 的系统中进行数据传输, 因此每个数据包都会经过多个子载波传输, 最终到达 Bob. 通过第一个数据包, Bob 便可提取 Alice 到 Bob 的初始信道估计值矩阵, 并对初始信道估计值矩阵按行取均值得到:

$$\hat{H}_{AB,1} = [\hat{H}_{AB,1}(1), \hat{H}_{AB,1}(2), \cdots, \hat{H}_{AB,1}(n)]^T \quad (1)$$

其中, $\hat{H}_{AB,1}(n)$表示第一个数据包各子载波上的信道估计值, Bob 利用密码学技术完成对 Alice 的第一个数据包的初始认证, 并保存初始信道响应后, 便可开始后续数据包的认证. Bob 收到第 2 个数据包后, 按式 (1) 提取当前信道响应均值, 并与第一个数据包的信道响应均值进行比较. 根据无线信道响应在相干时间内的相关性可知[14], 若第一个数据包提取的信道响应向量与第二个数据包提取的信道响应向量接近, 则表明发送者是 Alice; 若不接近, 则表明发送者是 Eve. 以此类推, 当 Bob 收到第 k 个数据包后, 将提取的信道响应与上一个数据包的信道响应进行比较, 从而实现对 Alice 发送消息的连续认证, 认证模型如图 2 所示.

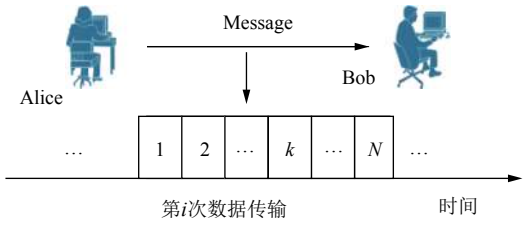

图 2 认证模型

1.2 假设检验

上述 Bob 对 Alice 发送消息的连续单向物理层认证可以通过二元假设检验来实现:

$$\begin{cases} H_0 : \tilde{H}_{t,k} = \tilde{H}_{AB,k-1} \\ H_1 : \tilde{H}_{t,k} \neq \tilde{H}_{AB,k-1} \end{cases} \quad (2)$$

其中, $\tilde{H}_{t,k}$和$\tilde{H}_{AB,k-1}$分别表示在 t 时刻前后两个数据包的无误信道响应值. H_0 表示前后两个数据帧来自同一个消息源, 即发送者是 Alice; H_1 表示前后两个数据帧来自不同的消息源, 即发送者是 Eve. 现实中, 由于噪声的影响, 导致 Bob 提取保存的连续信道响应估计值与真实信道响应存在偏差, 即:

$$\begin{cases} \hat{H}_{t,k} = \bar{H}_{t,k} + N_k \\ \hat{H}_{AB,k-1} = \bar{H}_{AB,k-1} + N_{k-1} \end{cases} \quad (3)$$

其中, N_k 和 N_{k-1} 分别表示前一个数据包和当前数据包独立同分布的复高斯白噪声, 且服从 $N(0, \sigma^2)$ 分布. 因此, 物理层认证转化为计算前后两个数据包的信道响

应估计值的差值, 并将差值与设定的门限值进行比较, 即:

$$T = diff(\hat{H}_{AB,k-1}, \hat{H}_{t,k}) \begin{matrix} > H_1 \\ < H_0 \end{matrix} \eta \quad (4)$$

其中, T 表示两个信道响应的差值, η 为门限值. 当差值小于门限值时, 假设 H_0 成立, 发送者为 Alice.

差值大于门限时, 假设 H_1 成立发送者为 Eve. 故式 (4) 中两个信道响应差值的计算和检测门限值 η 的确定成为物理层认证的关键. 同时, Alice 和 Bob 之间的相对移动或通信环境中其他物体的移动可能导致信道响应产生时变, 所以必须保证进行连续认证的两个数据包之间的时间间隔小于相干时间 t_c. 即 t_k-$t_{k-1} \le t_c$. 认证过程中的虚警概率 (合法的数据包被判定为非法) 定义为 $\alpha=Pr(H_0|H_1)$; 漏报概率 (非法的数据包被判定为合法) 定义为 $\beta=Pr(H_0|H_1)$.

2 提出的方案

本文所提出的基于哈希链的跨层认证方案, 采用消息认证码技术进行初始认证, 后续数据包的认证均采用物理层技术, 减少了计算复杂度, 达到了轻量级的目的; 通过在连续认证的过程中插入哈希链, 保证了在发生数据包丢失的情况时仍能实现连续的认证, 减少了认证时延, 提高了认证的效率.

2.1 跨层认证方案

该方案的流程图如图 3 所示, 当 Alice 需要与 Bob 进行通信时, Alice 向 Bob 连续发送 N 个数据包 $X_1, X_2, \cdots, X_N$. Bob 需要对 Alice 的 N 个数据包进行认证, 以确保消息的真实性和有效性. 具体步骤如下:

定义 1. 首先 Alice 与 Bob 将自己真实的 ID 提交给密钥中心 CA, CA 根据系统密钥计算出 Alice 与 Bob 的共享密钥 K_{AB}.

(1) Alice→Bob:

① Alice 选择一个随机数 r_A.

② Alice 计算 V_A=MAC$_{KAB}(r_A||t_1)$,其中 t_1 为当前时间戳.

③ Alice 将$\{r_A, t_1, V_A\}$发给 Bob.

(2) Bob→Alice:

① Bob 用 K_{AB} 计算 MAC'$_{KAB}(r_A||t_1)$ 与收到的 V_A 进行比较, 若相等, 则 Alice 通过 Bob 认证, 否则 Bob 拒绝 Alice 的请求.

② Bob 选择一个随机数 r_B.

③ Bob 计算 V_B=MAC$_{KAB}(r_A||r_B||t_2)$,其中 t_2 为当前时间戳.

④ Bob 将$\{r_B, t_2, V_B\}$发送给 Alice.

(3) Alice:

计算 MAC$_{KAB}(r_A||r_B||t_2)$,与收到的 V_2 进行对比, 若不同, 则丢弃, 若相同, 则 Bob 通过了 Alice 的认证.

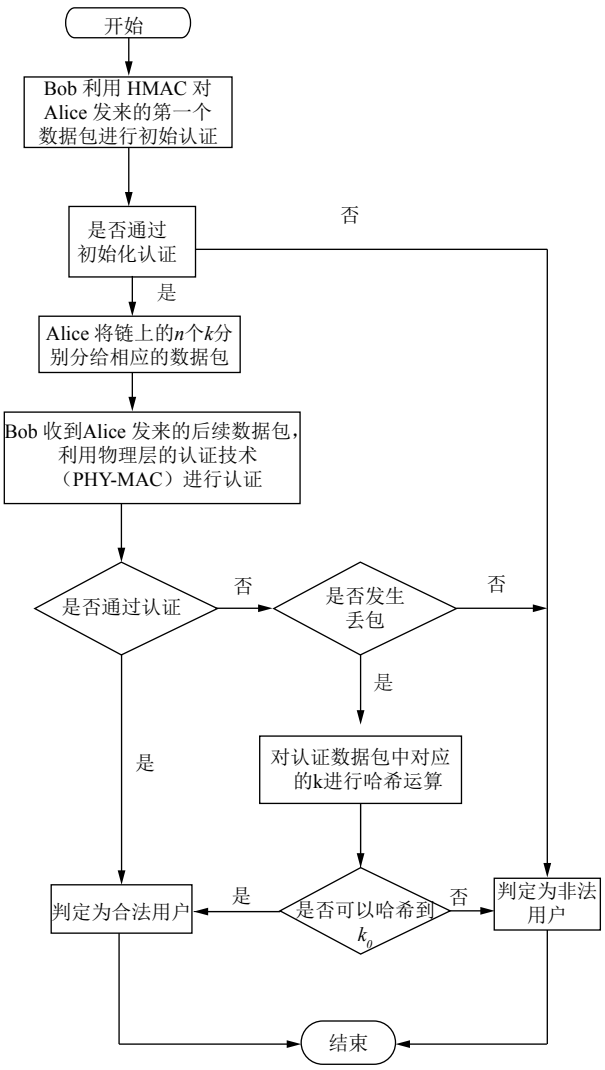

图 3 方案流程图

定义 2. Alice 继续发送第二个数据包 X_2, Bob 提取信道估计值, 利用改进的归一化的 LRT 统计量继续认证下一个数据包, 若认证失败或当接收到某个数据包 X_k 的时间超过了信道相干时间时则返回定义 1 进行重新的初始认证.

假设在初始认证成功后, Bob 发来的第 n 个数据

包 X_n 丢失, 下一个数据包 X_{n+1} 就不会被认证成功, 导致认证中断, 就要重新利用消息认证码来进行初始认证. 如果在一次数据的传输中, 丢包的次数很多, 就会延长认证的时延, 降低认证的效率. 本文提出了一种基于哈希链的跨层认证方案, 该方案可以保证认证在数据包丢失的情况下仍能进行连续的认证.

定义 3. 发送方 Alice 向接收方 Bob 发送数据之前, 首先要通过 $H(K_n)=K_{n-1}$ 自发的产生一个哈希链, 即:

$$K_0 \overset{H(K_1)}{\leftarrow} \cdots \leftarrow K_{i-1} \overset{H(K_i)}{\leftarrow} K_i \overset{H(Ki+1)}{\leftarrow} K_{i+1} \leftarrow \cdots \overset{H(K_n)}{\leftarrow} K_n \quad (5)$$

定义 4. 发送方 Alice 在发送数据之前, 分别将 K_{n-1} 插入数据包 X_n, 若数据包 X_n 丢失, 接收方 Bob 接收下一个数据包 X_{n+1} 就会认证失败.

定义 5. 在相干时间内, Bob 通过 K_n 能否哈希还原到 K_0 来判断 X_{n+1} 是否来自合法的发送方. 如果可以还原到 K_0, 就可以判断出发生了数据包丢失, 接下来对数据包中的信道响应向量进行提取和保存. 继续接收下一个数据包之后再进行认证, 从而保证了认证的连续性, 提高了认证的效率

2.2 改进的归一化的统计量

由于上述算法的好坏很大程度上取决于信道响应差值的计算和门限值 η 的选择, 文献[16]中提出似然比检验 (LRT) 统计量, 但这种 LRT 统计量的门限值计算较为困难, 主要通过在较大的门限范围内遍历来寻求最优门限值, 文献[17]对文献[16]进行了改进, 用机器学习算法来进行门限值的选取, 虽然提高了系统认证的准确性, 但不适用于资源受限且对实时性要求很高的认知无线网络. 本文将文献[15]改进的 LRT 统计量的归一化方法应用于认知无线网络中的物理层认证过程来进行门限值的选取, 在提高认证准确性的同时达到了轻量级的目的.

当 H_0 成立时:

$$T_{LRT}=\frac{diff(\hat{H}_{AB,k-1},\hat{H}_{t,k})}{diff(\hat{H}_{AB,k-2},\hat{H}_{AB,k-1})}\in(1-\delta,1+\delta) \quad (6)$$

当 H_1 成立时:

$$T_{LRT}=\frac{diff(\hat{H}_{AB,k-1},\hat{H}_{t,k})}{diff(\hat{H}_{AB,k-2},\hat{H}_{AB,k-1})}\gg 1+\delta \quad (7)$$

由以上分析可得, 基于归一化 LRT 统计量的物理层认证可以表示为:

$$T_{LRT}=\left|\frac{diff(\hat{H}_{AB,k-1},\hat{H}_{t,k})}{diff(\hat{H}_{AB,k-2},\hat{H}_{AB,k-1})}-1\right| \begin{matrix}>H_1\\<H_0\end{matrix} \eta_{LRT} \quad (8)$$

检测门限$\eta_{LRT}\in(0,0+\delta)$,归一化 LRT 统计量不涉及未知参数 σ^2 仅与连续三个数据帧的信道响应有关. 虽然归一化 LRT 统计量不符合现有的随机分布, 无法通过虚警概率计算出检测门限, 但是其检测门限的确定变得更为简单和方便, 只需在较小的范围内遍历就可获得较优的检测门限.

3 性能分析

本文在 IEEE802.15.4g 的物理层规范下对多个认证方案进行仿真, 并通过比较多个方案的认证时延来对本文所提出的认证方案 (Hash-PHY-HMAC) 的认证效率进行分析.

如表 1、图 4 所示, 假定要对 n 个数据包进行连续认证, 传统的密码学认证方案 HMAC 和 PKI 需要进行 n 次密码学认证, 而跨层认证方案 PHY-HMAC 和 PHY-PKI 只需要进行 1 次密码学认证, 并且本文使用非对称密钥 (PHY-HMAC) 进行初始认证的时延是 125 ms,而使用消息认证码进行初始认证时的认证时延只有 4.2 ms. 并且随着需要连续认证的数据包个数的增加, 平均的认证时延逐渐降低.

表 1 各方案认证时延对比 (ms)

方案	i								
	1	2	3	4	5	6	7	8	9
PKI	125	125	125	125	125	125	125	125	125
PHY-PKI	125	65	45	35	22	20	19	18	16
HMAC	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2	4.2
PHY-HMAC	4.2	2.3	1.6	1.1	0.9	0.85	0.76	0.66	0.55

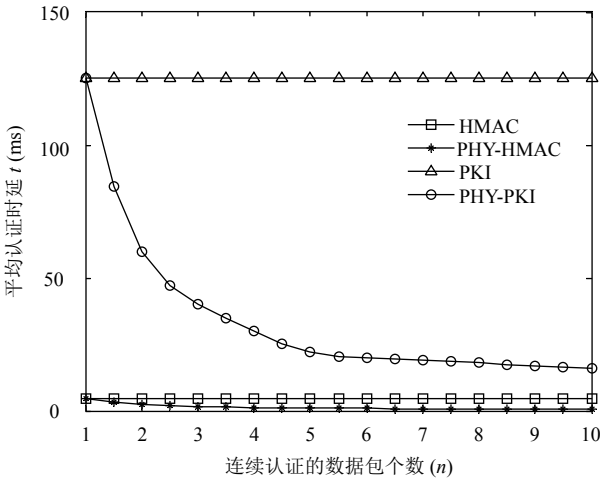

图 4 数据包个数与认证时延之间的关系

本文对认证所需要的认证时延与丢包率之间的关系进行分析, 原始的跨层认证方案和基于哈希链的跨层认证方案认证的平均时延与丢包率ℓ之间的关系式[19]如下:

$$t_1 = \frac{1}{(1-\ell)(1-\ell^N)} - 1 \tag{9}$$

$$t_2 = \frac{1}{(1-\ell)^2} - 1 \tag{10}$$

如图 5 所示, 随着丢包率的增加,我们提出的基于哈希链的认证方案中, 一次数据认证所需要的时延还是很短,而原始的认证方案时延变化很大. 所以, 本文提出的认证方案可以保证在丢包率很高的情况下, 仍能实现连续高效的认证.

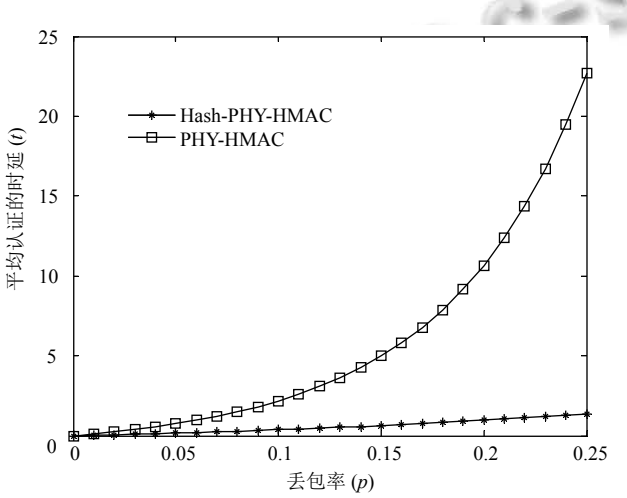

图 5 时间间隔与丢包率之间的关系

4 结束语

本文在认知无线网络中采用跨层认证方案, 该方案将物理层认证技术与高层协议相结合, 采用消息验证码 (HMAC) 技术进行初始认证, 后续的消息采用物理层技术进行认证. 并且该方案采用改进后的 LRT 统计量, 使得门限制的计算更为简单. 此外提出一种基于哈希函链的认证方法, 保证在发生数据包丢失的情况下, 仍能实现连续的认证, 提高了认证效率.

参考文献

1 Mitola J, Maguire GQ. Cognitive radio: Making software radios more personal. IEEE Personal Communications, 1999, 6(4): 13–18. [doi: 10.1109/98.788210]

2 Singhal D, Sharma MK, Garimella RM. Energy efficient localization of primary users for avoiding interference in cognitive network. Proceedings of 2012 International Conference on Computer Communication and Informatics. Coimbatore, India. 2012. 1–5.

3 张静, 蒋宝强, 郑霖. 认知无线网络技术在卫星通信中的应用. 桂林电子科技大学学报, 2013, 33(4): 284–287. [doi: 10.3969/j.issn.1673-808X.2013.04.007]

4 祝思婷. 车辆密集场景下的认知车联网频谱感知研究[硕士学位论文]. 北京: 北京邮电大学, 2017.

5 郎为民. 无线认知电传感器网络研究. 邮电设计技术, 2011, (12): 48–51. [doi: 10.3969/j.issn.1007-3043.2011.12.011]

6 刘超. 认知 Ad-hoc 无线网络的跨层结构设计. 电子测量技术, 2014, 37(11): 122–126. [doi: 10.3969/j.issn.1002-7300.2014.11.029]

7 裴庆祺, 李红宁, 赵弘洋, 等. 认知无线电网络安全综述. 通信学报, 2013, 34(1): 144–158.

8 Shi E, Perrig A. Designing secure sensor networks. IEEE Wireless Communications, 2004, 11(6): 38–43. [doi: 10.1109/MWC.2004.1368895]

9 邱慧敏. Sybil 攻击原理和防御措施. 计算机安全, 2005, (10): 63–65. [doi: 10.3969/j.issn.1671-0428.2005.10.029]

10 刘丽珍. 无线传感器网络中克隆节点攻击检测协议研究[硕士学位论文]. 长沙: 中南大学, 2012.

11 李传目. 安全密码认证机制的研究. 计算机工程与应用, 2003, 39(28): 173–175. [doi: 10.3321/j.issn:1002-8331.2003.28.053]

12 Kahate A. 密码学与网络安全. 金名, 译. 2 版. 北京: 清华大学出版社, 2009.

13 He F, Man H, Kivanc D, *et al*. EPSON: Enhanced physical security in OFDM networks. Proceedings of 2009 IEEE International Conference on Communications. Dresden, Germany. 2009. 1–5.

14 Xiao L, Greenstein L, Mandayam N, *et al*. Fingerprints in the ether: Using the physical layer for wireless authentication. Proceedings of 2007 IEEE International Conference on Communications. Glasgow, UK. 2007. 4646–4651.

15 Wen H, Wang Y F, Zhu X P, *et al*. Physical layer assist authentication technique for smart meter system. IET Communications, 2013, 7(3): 189–197. [doi: 10.1049/iet-com.2012.0300]

16 Xiao L, Reznik A, Trappe W, *et al*. PHY-authentication protocol for spoofing detection in wireless networks. Proceedings of 2010 IEEE Global Telecommunications Conference GLOBECOM. Miami, FL, USA. 2010. 1–6.

17 Xiao L, Yan Li Y, Liu G L, *et al*. PHY-layer spoofing detection with reinforcement learning in wireless networks. IEEE Transactions on Vehicular Technology, 2016, 65(12): 10037–10047. [doi: 10.1109/TVT.2016.2524258]

18 马婷, 周年荣, 高峰, 等. 智能电表系统中的物理层辅助认证技术. 网络安全技术与应用, 2013, (10): 21–22. [doi: 10.3969/j.issn.1009-6833.2013.10.016]

19 Eltaief H, Youssef H. Efficient sender authentication and signing of multicast streams over lossy channels. Proceedings of ACS/IEEE International Conference on Computer Systems and Applications-AICCSA. Hammamet, Tunisia. 2010.