**参考文献**

[1] 第41次《中国互联网络发展状况统计报告》发布[J]. 中国广播, 2018(3).

[2] 俞佳宝, 胡爱群, 朱长明, 等. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报, 2016(05):433-446.

[3] 袁红林. 基于射频指纹的无线网络物理层认证关键技术研究[D]. 东南大学, 2011.

[4] Chaabouni R. Break WEP Faster with Statistical Analysis[J]. Epfl, 2006.

[5] Mavridis I P, Androulakis A I E, Halkias A B, et al. Real-Life Paradigms of Wireless Network Security Attacks: Panhellenic Conference on Informatics, 2011[C].

[6] Ross A, Jain A. Information fusion in biometrics[J]. Pattern Recognition Letters, 2003,24(13):2115-2125.

[7] Tuyls P, Goseling J. Capacity and Examples of Template-Protecting Biometric Authentication Systems[M]. Springer Berlin Heidelberg, 2004.

[8] Talbot K I, Duley P R, Hyatt M H. Specific emitter identification and verification[J]. Technology Review, 2003.

[9] Riezenman M J. Cellular security: better, but foes still lurk[J]. Spectrum IEEE, 2000,37(6):39-42.

[10] Langley L E. Specific emitter identification (SEI) and classical parameter fusion technology: Wescon/'93. Conference Record, 2002[C].

[11] Guo F, Chiueh T. Sequence Number-Based MAC Address Spoof Detection[J]. Lecture Notes in Computer Science, 2005,3858:309-329.

[12] 顾杨. 基于无线设备特征指纹的无线钓鱼接入点检测技术研究[D]. 南京邮电大学, 2014.

[13] Desmond L C C, Yuan C C, Tan C P, et al. Identifying unique devices through wireless fingerprinting: ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, Va, Usa, March 31 - April, 2008[C].

[14] Pang J, Greenstein B, Gummadi R, et al. 802.11 user fingerprinting: Annual ACM international conference on Mobile computing and networking, Montreal(CA), 2007[C].

[15] Sieka B. Active fingerprinting of 802.11 devices by timing analysis: Ccnc 2006. 2006 IEEE Consumer Communications and NETWORKING Conference, 2006[C].

[16] Gao K, Corbett C, Beyah R. A passive approach to wireless device fingerprinting: Ieee/ifip International Conference on Dependable Systems and Networks, 2010[C].

[17] Lyon G. Nmap: a free network mapping and security scanning tool[EB/OL]. [11-5]. https://nmap.org/.

[18] Yarochkin F, Kydyraliev M, Arkin O. Xprobe project[EB/OL]. http://ofirarkin.wordpress.com/xprobe/.

[19] Eckersley P. How Unique Is Your Web Browser? Privacy Enhancing Technologies, International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings, 2010[C].

1. 第41次《中国互联网络发展状况统计报告》发布[J]. 中国广播, 2018(3).
2. 俞佳宝, 胡爱群, 朱长明,等. 无线通信设备的射频指纹提取与识别方法[J]. 密码学报, 2016, 3(5).
3. 袁红林. 基于射频指纹的无线网络物理层认证关键技术研究[D]. 东南大学, 2011.
4. Chaabouni R. Break WEP Faster with Statistical Analysis[J]. Epfl, 2006.
5. Mavridis I P, Androulakis A I E, Halkias A B, et al. Real-Life Paradigms of Wireless Network Security Attacks[C]// Informatics. IEEE, 2011:112-116.
6. Ross A, Jain A. Information fusion in biometrics[J]. Pattern Recognition Letters, 2003, 24(13):2115-2125.
7. Tuyls P, Goseling J. Capacity and Examples of Template-Protecting Biometric Authentication Systems[C]// Biometric Authentication, ECCV 2004 International Workshop, BioAW 2004, Prague, Czech Republic, May 15, 2004, Proceedings. DBLP, 2004:158-170.
8. Talbot K I, Duley P R, Hyatt M H. Specific emitter identification and verification[J]. Technology Review, 2003.
9. Riezenman M J. Cellular security: better, but foes still lurk[J]. Spectrum IEEE, 2000, 37(6):39-42.
10. Langley L E. Specific emitter identification (SEI) and classical parameter fusion technology[C]// Wescon/'93. Conference Record. IEEE, 2002:377-381.
11. Guo F, Chiueh T. Sequence Number-Based MAC Address Spoof Detection[J]. Lecture Notes in Computer Science, 2005, 3858:309-329.
12. 顾杨. 基于无线设备特征指纹的无线钓鱼接入点检测技术研究[D]. 南京邮电大学, 2014.
13. Desmond L C C, Yuan C C, Tan C P, et al. Identifying unique devices through wireless fingerprinting[C]// ACM Conference on Wireless Network Security, WISEC 2008, Alexandria, Va, Usa, March 31 - April. DBLP, 2008:46-55.
14. Pang J, Greenstein B, Gummadi R, et al. 802.11 user fingerprinting[C]// International Conference on Mobile Computing and Networking, MOBICOM 2007, Montréal, Québec, Canada, September. DBLP, 2007:99-110.
15. Sieka B. Active fingerprinting of 802.11 devices by timing analysis[C]// Ccnc 2006. 2006, IEEE Consumer Communications and NETWORKING Conference. IEEE, 2006:15-19.
16. Gao K, Corbett C, Beyah R. A passive approach to wireless device fingerprinting[C]// Ieee/ifip International Conference on Dependable Systems and Networks. IEEE, 2010:383-392. Yen T F, Xie Y, Yu F, et al. Host Fingerprinting and Tracking on the Web:Privacy and Security Implications[J]. 2012, 11(1):111 - 124.
17. Lyon G. Nmap: a free network mapping and security scanning tool[EB/OL]. [11-5]. <https://nmap.org/>.
18. Yarochkin F, Kydyraliev M, Arkin O. Xprobe project[EB/OL]. <http://ofirarkin.wordpress.com/xprobe/>.
19. Eckersley P. How Unique Is Your Web Browser? Privacy Enhancing Technologies, International Symposium, PETS 2010, Berlin, Germany, July 21-23, 2010. Proceedings, 2010[C].
20. Yen T F, Xie Y, Yu F, et al. Host Fingerprinting and Tracking on the Web:Privacy and Security Implications[J]. 2012, 11(1):111 - 124.
21. Mowery K, Bogenreif D, Yilek S, et al. Fingerprinting Information in JavaScript Implementations[C]// Acoustics, Speech and Signal Processing, 2009. ICASSP 2009. IEEE International Conference on. IEEE, 2011:9-12.
22. Acar G, Juarez M, Nikiforakis N, et al. FPDetective:dusting the web for fingerprinters[C]// ACM Sigsac Conference on Computer & Communications Security. ACM, 2013:1129-1140.
23. Łukasz Olejnik, Castelluccia C, Janc A. Why Johnny Can't Browse in Peace: On the Uniqueness of Web Browsing History Patterns[J]. Hot Topics in Privacy Enhancing Technologies, 2012, 69(1-2):63-74.
24. Bratus S, Cornelius C, Kotz D, et al. Active behavioral fingerprinting of wireless devices[C]// ACM Conference on Wireless Network Security. ACM, 2008:56-61.
25. Radhakrishnan S V, Uluagac A S, Beyah R. GTID: A Technique for Physical Device and Device Type Fingerprinting[J]. IEEE Transactions on Dependable & Secure Computing, 2015, 12(5):519-532.
26. Khlifi H, Gregoire J C. Estimation and removal of clock skew from delay measures[C]// IEEE International Conference on Local Computer Networks. IEEE, 2004:144-151.
27. Kohno T, Broido A, Claffy K C. Remote Physical Device Fingerprinting[C]// Security and Privacy, 2005 IEEE Symposium on. IEEE, 2005:211-225.
28. Cristea M, Groza B. Fingerprinting Smartphones Remotely via ICMP Timestamps[J]. IEEE Communications Letters, 2013, 17(6):1081-1083.
29. Langley L E. Specific emitter identification (SEI) and classical parameter fusion technology[C]// Wescon/'93. Conference Record. IEEE, 2002:377-381.
30. Lanze F, Panchenko A, Braatz B, et al. Clock skew based remote device fingerprinting demystified[C]// Global Communications Conference. IEEE, 2012:813-819.
31. Neumann C, Heen O, Onno S. An Empirical Study of Passive 802.11 Device Fingerprinting[J]. 2014:593-602.
32. Franklin J, Mccoy D, Tabriz P, et al. Passive data link layer 802.11 wireless device driver fingerprinting[C]// Conference on Usenix Security Symposium. USENIX Association, 2006:167--178.
33. Gerdes R M, Daniels T, Mina M, et al. Device Identification via Analog Signal Fingerprinting: A Matched Filter Approach.[C]// 144 Proceedings of the Network and Distributed System Security Symposium. 2004:78.
34. Brik V, Banerjee S, Gruteser M, et al. Wireless device identification with radiometric signatures[C]// ACM International Conference on Mobile Computing and NETWORKING. ACM, 2008:116-127.
35. Nguyen N T, Zheng G, Han Z, et al. Device fingerprinting to enhance wireless security using nonparametric Bayesian method[C]// INFOCOM, 2011 Proceedings IEEE. IEEE, 2011:1404-1412.
36. Li Z, Xu W, Miller R, et al. Securing wireless systems via lower layer enforcements[C]// ACM Workshop on Wireless Security. ACM, 2006:33-42.
37. Shi Y, Jensen M A. Improved Radiometric Identification of Wireless Devices Using MIMO Transmission[J]. IEEE Transactions on Information Forensics & Security, 2011, 6(4):1346-1354.
38. Das A, Borisov N, Caesar M. Do You Hear What I Hear?: Fingerprinting Smart Devices Through Embedded Acoustic Components[C]// ACM Sigsac Conference on Computer and Communications Security. ACM, 2014:441-452.
39. Dey S, Roy N, Xu W, et al. AccelPrint: Imperfections of Accelerometers Make Smartphones Trackable[M]. 2014.
40. Breiman L I, Friedman J H, Olshen R A, et al. Classification and Regression Trees (CART)[J]. Encyclopedia of Ecology, 1984, 40(3):582-588.
41. Breiman L. Random Forests[J]. Machine Learning, 2001, 45(1):5-32.
42. Cortes C, Vapnik V. Support-vector networks[J]. Machine Learning, 1995, 20(3):273-297.
43. Hsu C W. A practical guide to support vector classification[J]. 2003, 67(5).
44. 周志华. 《机器学习》[J]. 中国民商, 2016(3).
45. Kohavi R. A study of cross-validation and bootstrap for accuracy estimation and model selection[C]// International Joint Conference on Artificial Intelligence. Morgan Kaufmann Publishers Inc. 1995:1137-1143.

【11,-23】【24-39】

[图 2‑1 网络数据帧的生成过程 7](#_Toc513572464)

[图 2‑2 无线网络设备识别方案 8](#_Toc513572465)

[图 3‑1 TCP/IP参考模型与OSI参考模型对比 10](#_Toc513572466)

[图 3‑2 流量数据帧结构示意图 11](#_Toc513572467)

[图 3‑3 网络环境模型 13](#_Toc513572468)

[图 3‑4 数据采集环境 14](#_Toc513572469)

[图 3‑5 WireShark主界面 14](#_Toc513572470)

[图 3‑6 数据帧数目统计图 17](#_Toc513572471)

[图 3‑7 数据预处理流程图 17](#_Toc513572472)

[图 3‑8 帧间隔时间的PDF曲线 20](#_Toc513572473)

[图 3‑9 不同阈值的降噪效果对比（IAT） 20](#_Toc513572474)

[图 3‑10 帧大小降噪效果对比 21](#_Toc513572475)

[图 3‑11 传输速率降噪效果对比 21](#_Toc513572476)

[图 3‑12 三台设备传输速率的PDF曲线 22](#_Toc513572477)

[图 3‑13 特征指纹生成过程 23](#_Toc513572478)

[图 4‑1 随机森林示例 26](#_Toc513572479)

[图 4‑2 支持向量机原理 27](#_Toc513572480)

[图 4‑3 K最近邻原理 28](#_Toc513572481)

[图 4‑4 交叉验证过程示意图 29](#_Toc513572482)

[图 4‑5 group\_size变化对识别效果的影响（IAT） 32](#_Toc513572483)

[图 4‑6 group\_size变化对识别效果的影响（FrameSize） 33](#_Toc513572484)

[图 4‑7 group\_size变化对识别效果的影响（TransRate） 33](#_Toc513572485)

[图 4‑8 group\_size变化对识别效果的影响（融合特征） 34](#_Toc513572486)

[图 4‑9 bin\_size变化对识别效果的影响（IAT） 34](#_Toc513572487)

[图 4‑10 bin\_size变化对识别效果的影响（FrameSize） 35](#_Toc513572488)

[图 4‑11 bin\_size变化对识别效果的影响（TransRate） 35](#_Toc513572489)

[图 4‑12 bin\_size变化对识别效果的影响（融合特征） 36](#_Toc513572490)

[图 5‑1 原型系统用例图 38](#_Toc513572491)

[图 5‑2 原型系统框架图 39](#_Toc513572492)

[图 5‑3 流量数据捕获模块时序图 40](#_Toc513572493)

[图 5‑4 特征指纹生成模块时序图 41](#_Toc513572494)

[图 5‑5 无线设备识别模块时序图 43](#_Toc513572495)

[图 5‑6 指纹库更新时序图 44](#_Toc513572496)

[图 5‑7 Django处理流程图 45](#_Toc513572497)

[图 5‑8 数据库表之间的关系 47](#_Toc513572498)

[图 5‑9 流量数据捕获页面设计 48](#_Toc513572499)

[图 5‑10 特征指纹提取页面（1） 49](#_Toc513572500)

[图 5‑11 特征指纹构建页面（2） 50](#_Toc513572501)

[图 5‑12 特征指纹构建页面（3） 50](#_Toc513572502)

[图 5‑13 特征指纹构建页面（4） 51](#_Toc513572503)

[图 5‑14 设备识别页面（1） 51](#_Toc513572504)

[图 5‑15 设备识别页面（2） 52](#_Toc513572505)

[图 5‑16 指纹库更新页面 53](#_Toc513572506)

随着无线网络的飞速发展和移动设备的日益普及，无线网络技术在给人们日常生活带来方便的同时，也存在着许多安全隐患。相比于有线网络，无线网络由于其开放性更容易遭受到恶意攻击。隐私泄露、网络欺骗、假冒攻击等问题时刻威胁着网络用户的安全。为了增强无线网络的安全性能，本文提出了基于流量认知分析的无线设备指纹识别技术，在不影响设备正常使用的情况下，实现对无线设备的精确识别。

本文首先分析了无线数据帧与设备个体之间的相关性，并提出了基于流量认知的无线设备指纹识别方案。为了验证方案的可行性，我们捕获到包含个人PC、智能手机、平板电脑在内的23台无线设备的流量数据，创建了设备指纹识别的数据集。本文从TCP流量数据帧中提取出帧时间间隔、帧大小和传输速率三种参数，对每种参数的数据进行降噪和归一化处理，将数据转换成易于提取特征的格式。本文提出了两种特征指纹生成方法：基于概率密度的特征指纹和基于多特征融合的特征指纹。基于概率密度的特征指纹是统计每种参数的概率密度，将其作为特征，三个参数分别形成三类特征指纹。多特征融合的特征指纹是将三个独立的特征指纹组合在一起，以形成能够更加完整表征设备身份信息的特征指纹。

针对无线设备识别问题，本文使用随机森林（RF）、支持向量机（SVM）、K最近邻（KNN）、朴素贝叶斯（NBC）四种分类器进行设备身份模型的构建与评估，并采用准确率（precision）、召回率（recall）和F1值来评估识别的效果。本文分别对两种特征指纹和四种分类器的性能进行比较，实验结果表明：融合特征在标识设备身份方面表现更好，在各种分类器下均能取得较好的效果；在四种分类器中，随机森林更适合无线设备指纹识别问题，无论使用哪种特征指纹均能得到较好的识别精度。当使用融合特征指纹时，随机森林分类器的precision、recall和F1值分别为0.9930、0.976和0.9783。本文还探讨了特征空间的变化对识别效果的影响，即更改特征指纹生成过程中的部分参数，比较各分类器的效果和两种特征指纹的性能。实验结果表明，随机森林的分类效果比较稳定，始终能保持较好的识别结果；相比于基于概率密度的特征指纹，融合特征指纹的鲁棒性更好，当特征指纹生成过程中的参数变化时，融合特征仍能较好地标识设备的身份。

基于上述提出的无线设备指纹识别技术，本文设计并实现了基于B/S架构的无线设备识别原型系统，原型系统包含流量数据捕获、特征指纹生成、无线设备识别和指纹库更新四个功能模块。其中流量数据捕获模块用于实时捕获流量数据；特征指纹生成模块负责特征参数的提取、数据降噪和归一化，并提取出相应的特征指纹；设备识别模块将设备的特征指纹与指纹库中的指纹进行比对，识别出设备类型；指纹库更新模块根据识别的结果将新设备指纹加入指纹库中。

网络流量；设备识别；特征指纹；分类器

目 录

[1 绪论 1](#_Toc513820986)

[1.1 选题意义与应用背景 1](#_Toc513820987)

[1.2 设备识别研究现状 2](#_Toc513820988)

[1.2.1 基于软件的设备识别 2](#_Toc513820989)

[1.2.2 基于硬件的设备识别 3](#_Toc513820990)

[1.3 本文的研究内容 5](#_Toc513820991)

[1.4 论文的组织结构 7](#_Toc513820992)

[2 基于流量认知的无线设备指纹识别原理与框架 8](#_Toc513820993)

[2.1 无线数据帧与设备个体的相关性 8](#_Toc513820994)

[2.2 基于流量认知的无线设备指纹识别框架 9](#_Toc513820995)

[2.3 本章小结 10](#_Toc513820996)

[3 面向设备指纹的流量分析与认知 11](#_Toc513820997)

[3.1 流量帧介绍 11](#_Toc513820998)

[3.2 流量数据采集 13](#_Toc513820999)

[3.2.1 无线网络环境 13](#_Toc513821000)

[3.2.2 数据采集方案 16](#_Toc513821001)

[3.2.3 数据集介绍 16](#_Toc513821002)

[3.3 数据预处理 18](#_Toc513821003)

[3.3.1 数据帧参数提取 19](#_Toc513821004)

[3.3.2 数据降噪 20](#_Toc513821005)

[3.3.3 数据归一化 22](#_Toc513821006)

[3.4 特征指纹生成 23](#_Toc513821007)

[3.4.1 基于概率密度的特征指纹 23](#_Toc513821008)

[3.4.2 基于多特征融合的特征指纹 25](#_Toc513821009)

[3.5 本章小结 25](#_Toc513821010)

[4 无线设备指纹识别 26](#_Toc513821011)

[4.1 无线设备指纹识别概述 26](#_Toc513821012)

[4.2 设备识别分类器 26](#_Toc513821013)

[4.2.1 随机森林 26](#_Toc513821014)

[4.2.2 支持向量机 27](#_Toc513821015)

[4.2.3 K最近邻 28](#_Toc513821016)

[4.2.4 朴素贝叶斯 29](#_Toc513821017)

[4.3 评估方法 29](#_Toc513821018)

[4.3.1 数据集 29](#_Toc513821019)

[4.3.2 训练和测试过程 30](#_Toc513821020)

[4.3.3 评估指标 31](#_Toc513821021)

[4.4 实验结果与分析 31](#_Toc513821022)

[4.4.1 实验1：设备识别实验结果与分析 32](#_Toc513821023)

[4.4.2 实验2：特征空间变化对识别效果的影响 33](#_Toc513821024)

[4.5 本章小结 37](#_Toc513821025)

[5 无线设备指纹识别原型系统的开发与实现 38](#_Toc513821026)

[5.1 原型系统需求分析 38](#_Toc513821027)

[5.2 原型系统架构设计 40](#_Toc513821028)

[5.3 原型系统实现 41](#_Toc513821029)

[5.3.1 流量数据捕获模块 41](#_Toc513821030)

[5.3.2 特征指纹形成模块 42](#_Toc513821031)

[5.3.3 无线设备识别模块 43](#_Toc513821032)

[5.3.4 指纹库更新模块 45](#_Toc513821033)

[5.3.5 Web服务器端开发 46](#_Toc513821034)

[5.4 原型系统功能测试 49](#_Toc513821035)

[5.4.1 流量数据捕获模块功能测试 49](#_Toc513821036)

[5.4.2 特征指纹构建模块功能测试 50](#_Toc513821037)

[5.4.3 无线设备识别模块功能测试 52](#_Toc513821038)

[5.4.4 指纹库更新模块功能测试 53](#_Toc513821039)

[5.5 本章小结 54](#_Toc513821040)

[6 结论与展望 55](#_Toc513821041)

[6.1 论文工作总结 55](#_Toc513821042)

[6.2 不足与展望 56](#_Toc513821043)

[致 谢 57](#_Toc513821044)

[参考文献 58](#_Toc513821045)

[攻读学位期间取得的研究成果 61](#_Toc513821046)

声明