

基于 AP 指纹的 RAP 检测方法

李晴, 叶阿勇, 姚志强, 陈爱民

(福建师范大学数学与信息学院, 福建 福州 350007)

摘要: 无线接入点 (AP, access point) 是基础设施模式中不可或缺的一部分, 而流氓 AP (RAP, rogue AP) 普遍存在的攻击在很大程度上泄露了用户隐私, 如用户的位置信息、上网行为和社交关系等。提出一种基于指纹的 RAP 检测算法, 利用 Beacon 帧参数的不可伪造性和稳定性判断 AP 的合法性, 并通过方案对比和实验分析进一步验证了方法的可行性和有效性。

关键词: 无线局域网; 隐私泄露; RAP 检测; 指纹检测; Beacon 帧

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2018023

RAP detection method based on AP fingerprint

LI Qing, YE Ayong, YAO Zhiqiang, CHEN Aimin

College of Mathematics and Informatics, Fujian Normal University, Fuzhou 350007, China

Abstract: The access point (AP) is an integral part of the infrastructure mode in wireless network. While the attacks caused by rogue AP (RAP) divulge a lot of users' privates in a large extent, such as the user's location information, surfing behavior on the Internet and social relations. A RAP detection algorithm based on AP fingerprint was proposed. The validity of AP was judged by the unforgeability and stability of the parameters of beacon frames. And the feasibility and effectiveness of the proposed method were further verified by scheme comparisons and experimental analysis.

Key words: WLAN, privacy disclosure, RAP detection, fingerprint-based detection, Beacon frame

1 引言

随着无线技术的快速发展, 无线局域网 (WLAN, wireless local area network) 普遍应用于诸多领域和公众场所, 如机场、商场、餐厅、医院等^[1]。AP 是无线局域网络基础设施模式不可或缺的一部分, 它有效地将移动用户与有线网络进行连接。然而, AP 被广泛使用的同时也给信息

安全带来了大量安全隐患。Sandeep^[2]指出一项关于 WLAN 安全的全球调查, 结果显示, 超过 32% 的用户在使用公共 AP 时不会关注其安全问题。

由于无线信号固有的辐射性以及空间信道的开放性, 公众 AP 本身存在不可信的安全隐患也日益突出。RAP 已被用于网络嗅探攻击和中间人攻击等多种攻击, 严重威胁着公共无线网络中用户隐私安全。一方面, 移动用户的上网数据是经

收稿日期: 2018-01-03; 修回日期: 2018-02-27

通信作者: 叶阿勇, yay@fjnu.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61771140); 福建省自然科学基金资助项目 (No.2018J01780); 福建省高校自然基金青年重点资助项目 (No.JZ160430)

Foundation Items: The National Natural Science Foundation of China (No.61771140), The Natural Science Foundation of Fujian Province (No.2018J01780), The Key Natural Science Foundation of Fujian Educational Bureau for Young Scholars (No.JZ160430)

RAP 转发到无线网中, 用户的账号密码等敏感信息存在泄露风险^[3]; 另一方面, 也暴露了位置信息, 从而导致用户其他隐私泄露。因此, 在 WLAN 中对合法 AP 的筛选至关重要。

本文探讨的 RAP 主要是未经授权的 AP 和钓鱼 AP, 即不是由合法运营商或服务提供商提供的 AP。本文提出了一种基于指纹的 RAP 检测算法, 该算法获取本地合法 AP (LAP, local legal AP) 的特征, 根据特征参数生成 LAP 指纹, 终端根据 LAP 指纹检测 RAP。

2 相关工作

Airtight 报告显示了由于用户缺乏无线网络安全知识而引发的许多安全隐患^[2]。而且当前可用的 AP 中将近 20% 的 AP 是恶意的。攻击者通常在无线环境中伪造 RAP, 用于扰乱无线网络并试图窃取敏感信息。目前的 RAP 检测技术^[4-8]主要包括信标帧时钟偏差、时序特性、无线嗅探、指纹识别等方式。

Alotaibi 等^[4]通过检查每一个信标 (Beacon) 帧来检测 RAP, 将其值与一个阈值比较, 小于该阈值的 AP 则被判定为 RAP。Kim 等^[5]提出利用移动网络和有线网络中 RTT 值的不同检测 RAP, 通过报文分组测量 AP 和后续节点之间的等待时间, 从而获得对应的 RTT 值, 而不依赖于 AP 或用户授权列表的信息。即使路由跟踪过程并不能保证找到一个合适的后继节点, 也可测量 RTT 值。Dahiya 等^[6]提出一种在 WLAN 中自动检测 RAP 的霍普菲尔德神经网络方法。Jadhav 等^[7]根据具有 IEEE 802.11 时间同步功能的时间戳计算 AP 信标、探测响应帧中的偏移间隔作为指纹, 使用基于线性规划和基于最小二乘拟合这 2 种方法计算信标帧的时钟偏移。但收集 AP 数据帧的时钟偏差需要预先建立相应数据库, 再进行比较, 且无法有效地检测媒体访问控制地址欺骗。Zheng 等^[8]利用细粒度信道状态信息, 对 RAP 进行方向确定和位置估计, 检测并定位 RAP。Kim 等^[9]为了防止客户端中敏感数据被窃取, 将收集到附近合法 AP 的 RSS 序列进行归一化处理, 并根据预期迭代次数设定阈值, 比较判断 RAP。但由于无线信号的不稳定性且易受环境影响, 如不同温度、

湿度、遮挡物都会对其造成差异, 从而会造成数据不精确, 影响检测效果。

3 安全威胁

RAP 的攻击主要通过伪造大量虚假无线信号来破坏良性 WLAN 用户的正常使用。若多个 AP 的 SSID 或 MAC 地址相同, 用户和设备本身难以判定该 AP 信号是否来自 LAP, 将造成安全威胁。

1) 安全隐患

根据 RAP 部署的情况不同, 给用户造成的威胁也有所不同, 具体如下。

① 用户不接入 RAP

攻击者在 WLAN 环境中广播 RAP 信号, 该 RAP 可以不具备完整的 AP 功能, 此类攻击以定位欺骗攻击为典型。由于服务器在定位阶段并未对用户上传的 AP 信息进行合法性验证, 攻击者通过伪造 RAP, 欺骗用户定位至特定地点。而基于位置的社交网络将信息共享与位置相结合, 用户受到定位欺骗攻击后发布的与位置相关的信息将造成其隐私泄露威胁。

② 用户接入 RAP

攻击者伪造 RAP 并诱使用户接入, 从而进行监听、嗅探用户上网数据等攻击。此类攻击主要针对用户接入 RAP 后的一系列操作, 对用户的上网行为和身份隐私泄露造成隐患^[10,11]。例如, 一些网站的数据传输方式采用明文传输, 导致未加密数据在传输过程中完全暴露。由于无线信号的传输范围有限, 用户接入某个 RAP 暴露了大致的位置信息。单个 AP 接入可初步估计用户所在区域, 多个 AP 接入区域的重叠部分可更精确地定位用户。

2) RAP 攻击

终端通常会选择信号比较强或者信噪比低的 AP 进行连接, 攻击者可通过对 LAP 进行 DoS 攻击或者提供比 LAP 更强的信号, 迫使无线客户端连接到 RAP。RAP 攻击通常包括以下步骤。

① 获取无线网络的密钥。对于采用 WEP 或 WPA 认证的无线网络, 攻击者可以通过无线破解工具或者采用社会工程的方法窃取目标无线网络的密钥, 并用于设置 RAP 密钥。

② 伪造目标无线网络。在目标 WLAN 环境附近架设一个与 LAP 的 SSID 完全一样或极其相似的 RAP。当终端历史连入该 SSID 对应的网络, 便会自动连接该网络, 但由于采用相同的 SSID, 用户很难辨别真伪。

③ 干扰合法无线网络。为了提高攻击成功率, 攻击者对本地无线网络进行 DoS 攻击, 使其处于瘫痪状态。这时, 终端会重新扫描无线网络, 并主动连接附近信号强度最好的 AP。

4 预备知识

Beacon 帧的 MAC 头部通常包含 Frame Control、Duration、Destination Address、Source Address、BSSID and Sequence Control 这几个部分。用于检测 RAP 的 AP 指纹需具有不可伪造性、稳定性和标识性, 即该指纹不能随意被更改, 不随时间空间或其他因素无规律改变, 并且能体现该特征是属于 LAP 的。因此本文算法用到 BI (Beacon interval)、length 和 Timestamp 这几个字段, 具体介绍如下。

1) BI 字段

AP 每隔一段时间就会发出一个 Beacon 信号, 用来表示其网络的存在。BI 字段用于设定该信号时间间隔的时间单位, BI 默认会被设定为 100 个时间单位, 相当于 100 ms, 即 LAP 每 0.1 s 发送一次 Beacon 信号。

2) Length 字段

Length 字段存在于信息元素中, 用于表示这个帧的长度, 与实际帧长度相关, 并非自定义的。由于 Beacon 帧是管理帧的一种, 不含交换数据信息, 因此每种特定 LAP 的帧长度固定在某个值或某个范围。

3) Timestamp 字段

Timestamp 字段可用于同步 BSS 中的工作站, BSS 的主计时器会定期发送目前已作用的微秒数。当计数器达到最大值时 (超过 584 942 年), 便会从头开始计数, 但很难会遇到从头开始计数的一天, 并且这个字段与 BSS 的工作时间相关, 按规律增长微秒数, 并不能随意被伪造。

5 基于 AP 指纹的 RAP 检测方法设计

5.1 总体方案

为了抵抗 RAP 攻击引发的安全问题, 本文提出一种基于指纹的 RAP 检测方法, 其主要思想是利用 Beacon 帧参数的不可伪造性和稳定性判断 AP 的合法性。不可伪造性指对于特定服务开发商所利用和提供的 LAP 具有一定的特征, 且其 Beacon 帧的一些参数不能人为修改。稳定性是指 AP 部分的 Beacon 帧参数不会随着时间等其他因素而改变, 或者说随时间变化的规律相同, 从而保证特征指纹的稳定。

系统框架如图 1 所示, 管理员终端在安装配

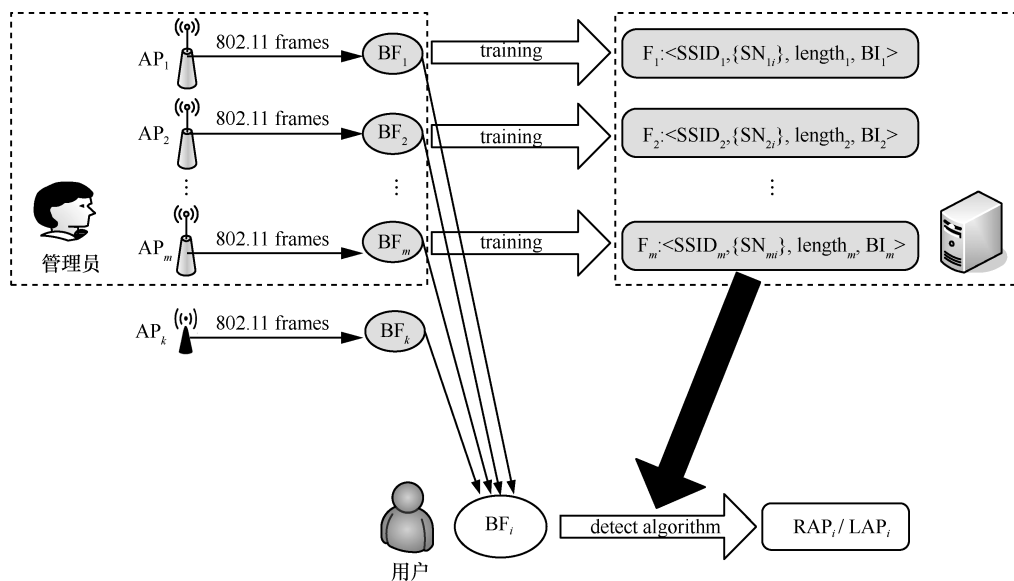


图1 系统框架

置 LAP 时采集其 802.11 帧, 并构造 LAP 指纹库存储在服务器中。用户根据服务器发布的 AP 白名单, 检测其扫描到的 AP 中是否有 RAP。RAP 检测流程分为 3 个阶段, 如图 2 所示, 包括指纹采集、指纹生成和检测 AP 类别。每个阶段采用对应的操作和算法, 并且后一个阶段依赖于前一阶段的结果。

5.2 指纹采集阶段

管理员终端设备被动扫描监听其附近 LAP 的广播帧 $\{f_1, f_2, \dots, f_i, \dots\}$, 其中, 802.11 帧包含数据帧 d_i 、控制帧 c_i 和管理帧 m_i , 仅筛选管理帧中的 Beacon 帧 fb_i 作为参考依据。由于 Beacon 帧是 AP 定期广播以示其存在的, 不需要终端与 AP 之间有数据交互就可以被扫描得到的, 从而降低了数据采集的难度, 也无需对移动终端设备再进行修改。不同类型的 802.11 帧的 MAC 头部不一样, 筛选管理帧 m_i 后, 再对其子层的 subtype 字段进行匹配, 其中, 若 subtype=0x08, 则为 Beacon 帧。

5.3 指纹处理生成阶段

本阶段的主要任务包括数据预处理和训练学习。数据预处理需从扫描到的 Beacon 帧中提取其 SSID、BSSID、BI、length 等字段, 由于这些数据是由管理员前期 LAP 部署时采集生成, 即可生成 AP 指纹索引表。另外, 诸如服务商提供的 AP 通常具有相同 SSID, 若将所有的 AP 信息分别列为一个索引, 将会增加存储开销, 因此可根据 LAP 帧的特征, 训练学习为一类 LAP 后形成指纹存储在服务器中。

5.4 检测合法 AP 阶段

本阶段的主要任务是根据指纹处理生成阶段的 AP 指纹检测待分类 AP 是否为 RAP。移动基站面向广大用户且不易被攻击, 笔者认为它是可

信的, 终端在接入 AP 前先接入移动基站获得 AP 指纹。如果扫描得到的 AP 信息被判定为 LAP, 则用户可以做后续操作 (如无线定位、接入上网等); 否则判定为 RAP, 上报给本地服务器。

根据 AP 指纹是否为服务器直接发布和应用场景的不同, 用户终端采用的 RAP 检测算法又分为集中式 LAP 检测和自主式 RAP 检测。

5.4.1 集中式 LAP 检测

集中式 LAP 检测算法是指将 AP 指纹存储在服务器中, 终端工作的时候由服务器发布 AP 指纹, 也就是说, AP 指纹的更新操作由服务器完成, 用户可直接使用, 对终端扫描到的 AP 信息进行检测, 侧重于检测属于 AP 指纹的 AP。

由 AP 指纹生成阶段可知, 若 SN 字段为 0, 则为仅广播信号的伪造 AP; 若 BI 为某个特定值 a (实验时 $a=300$), 则为手机热点; 若 BI 非常大, 则为 “Malformed packet” 错误, 丢弃处理即可; 若 length 低于某个范围, 则接入了 RAP。因此, 根据 AP 指纹, 集中式 LAP 检测算法伪代码如算法 1 所示。

算法 1 集中式 LAP 检测

输入 $\{fb_1, fb_2, \dots, fb_m\}$

输出 RAP list and LAP list

- 1) For $i=1$ to m
- 2) 提取 SSID _{i} , BSSID _{i} , SN _{i} , length _{i} , BI _{i}
- 3) If $fb_i.SN=0$ Then
- 4) AP _{i} 由 mdk3 伪造, $\rightarrow$ RAP
- 5) Else If $fb_i.BI \neq 100$
- 6) If $fb_i.BI=a$ Then
- 7) AP _{i} 是钓鱼 AP, $\rightarrow$ RAP
- 8) Else If $fb_i.BI > 1000$ Then
- 9) 判定为 Malformed Packet

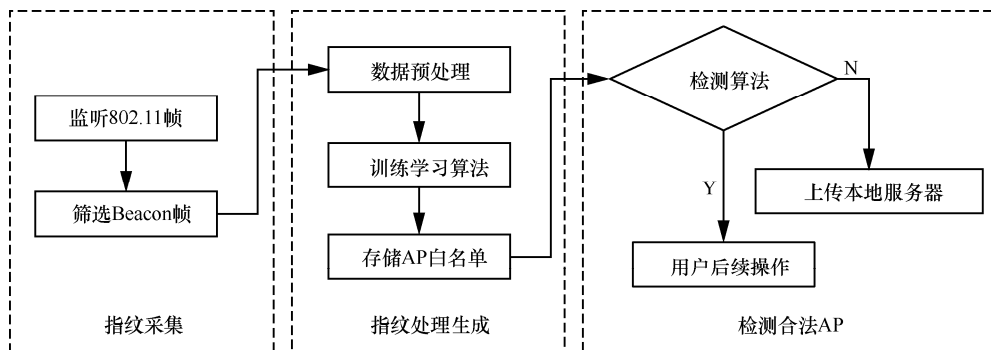


图 2 RAP 检测流程

- 10) End If
- 11) Else If $fb_i.length < threshold$ Then
- 12) AP_i 由 mdk3, $\rightarrow$ RAP
- 13) End If
- 14) 将 fb_i 分类为 LAP
- 15) End For
- 16) return RAP list and LAP list

5.4.2 自主式 RAP 检测

自主式 RAP 检测是指终端利用机器学习算法根据服务器提供的 LAP 列表信息训练 AP 指纹, 并完成终端的 RAP 检测。因此, 自主式 RAP 检测需要将算法嵌入终端设备中。该方法可对未知 AP 信息进行分类预测, 判断其真伪。本文选用的 802.11 帧参数字段具有稳定性, 即具有相对固定值或相同的变化规律, 仅需要将训练和预测结果分为 LAP 和 RAP 这两类; 并且, 由于 802.11 帧在传输过程中存在异常情况, 如接收到 Malformed Packet, 而 SVM 在松弛情况下允许存在离群值, 即满足异常点存在的条件。因此, 选用 SVM 分类算法来检测 RAP, 其伪代码如算法 2 所示。由于数据集较小, 机器学习算法执行前需考虑十折交叉验证, 降低采集数据过拟合现象。

算法 2 自主式 RAP 检测

输入 $\{fb_1, fb_2, \dots, fb_m\}$

输出 RAP list and LAP list

- 1) For $i=1$ to m
- 2) 提取 SSID _{i} , SN _{i} , length _{i} , BI _{i}
- 3) Cross-Vlilation()
- 4) Train and Class
- 5) 利用 SVM 检测分类 AP
- 6) If AP_i is RAP Then
- 7) 忽略该帧
- 8) Else
- 9) 将 AP_i 添入 LAP list, continue
- 10) End If
- 11) End For
- 12) return RAP list and LAP list

6 实验和分析

6.1 实验设置

根据攻击模型, 本文部署了 2 种 RAP 攻击,

即用户不接入的 RAP_A 和用户接入的 RAP_B。使用具有无线功能的 Lenovo B460e 笔记本和 Meizu note2 智能手机开启无线热点, 充当 RAP_B; 用一台装有 Ubuntu 15.04 系统的笔记本广播虚假 AP 信号, 充当 RAP_A。攻击采用 Aircrack-ng 和 MDK3 这 2 种工具, 利用 Aircrack-ng 套件中的 airmon-ng 工具和 airodump-ng 工具监控和嗅探无线数据分组; 利用 MDK3 的 Beacon Flood Mode 功能伪造 AP, 利用其 Deauthentication/Disassociation Amok Mode 功能切断用户与本地 AP 之间的连接。客户端采用 Airmagnet WiFi Analyzer Pro 捕获 802.11 帧数据。

实验中, 使用 Python 的机器学习库 Scikit-Learn 中的 Cross-Vlilation 做交叉验证。利用 anaconda 中集成的机器学习库 sklearn, 实现对包含特征和目标的训练集进行监督学习, 并通过 train_test_split() 功能从样本中随机按比例选取训练数据和测试数据。

6.2 实验分析

本文用 Airmagnet WiFi Analyzer Pro 筛选捕获 Beacon 帧数据完成指纹采集过程。实验收集到帧数据中, 大多数 RAP 的 length 小于 150 byte, 部分 RAP 约为 200 byte, 近似于 LAP 难以判断。因此, 单从一个参数 length 检测 RAP 仅能判断部分 RAP 攻击, 如实验中用 MDK3 伪造的 RAP。故本文用 SVM 算法对 3 种字段的 AP 进行分类检测, 结果如图 3 所示。可以清楚地发现, RAP 被分类在相对聚集的区域, 即图中*标识的地方。

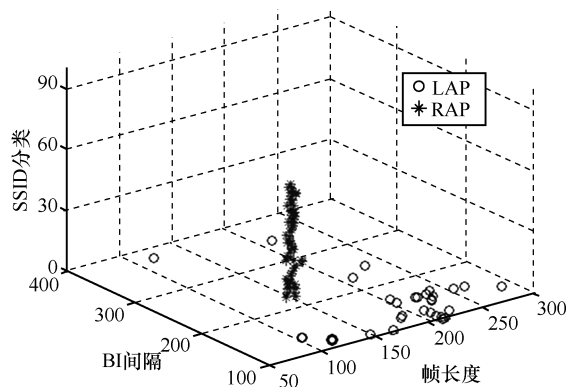


图3 三维字段的 AP 分类情况

实验时, 扫描 AP 信息按 SSID 划分共 17 种 LAP 和 57 种 RAP, 对采集到的 Beacon 帧提取特

征字段,并按 1:3 比例随机选取部分 AP 信息列入表 1 中。由于合法 AP 的 SN 是随时间增长的且 BI 为 100 个时间单位,而 Timestamp 与 BSS 主定时器有关,因此表中仅含有的 SSID、length 和 number 这 3 个易于标识 AP 的信息。

表 1 初始数据样本

SSID	number	length
AP ₁	1 291	211.70
AP ₂	70	144
AP ₃	2 026	180
AP ₄	2 090	217
AP ₅	89	172
AP ₆	67	266.66
AP ₇	20	198
AP ₈	359	65
AP ₉	438	70
AP ₁₀	37	80

对于表 1, RAP 伪造本地 LAP 的 SSID, 则其 length 存在冲突, 如表 1 的 AP₁ 和 AP₆; RAP 伪造其他地方的 LAP, 则其 length 低于一般值, 如表 1 的 AP₈、AP₉ 和 AP₁₀, 但不适用于手机热点。

人工分类后获取到包含输入和目标的训练集, 作为机器学习训练的输入, 从而获取到对应的模型和 AP 白名单, 于是终端可以对未知输入进行分类预测。利用 sklearn 库, 实现对包含特征和目标的训练集进行监督学习, 采用 SVM 学习一个模型, 用于 AP 分类和预测, 根据扫描 Beacon 帧时间进行 RAP 的检测, 其准确率如表 2 所示。

考虑到不同时间的攻击 RAP 数量不同, 实验又随机从 4 个连续的时间间隔中获取 Beacon 帧的特征字段, 其中不超过 1 000 个连续的 Beacon 帧, 所对应的时间间隔基本小于 5 s, 故不列出时间, 使用 SVM 对其检测 RAP 的准确率, 如图 4 所示。

表 3

本文 2 种检测算法对比

对比项	服务器参与部分	准确率	不足
集中式 LAP 检测	发布 AP 指纹	100% (仅检测出属于 AP 指纹)	更新取决于服务器的 AP 指纹; 服务器 AP 指纹一错全错
自主式 RAP 检测	确定算法和参数	98%以上 (扫描时间为 5 s 左右)	检测 RAP 前需训练学习

表 2 连续时间段对 RAP 检测准确率

扫描时间/s	帧数量	准确率
60	9 267	0.998 65
50	7 861	0.992 60
40	6 199	0.989 41
30	7 309	0.985 15
20	4 974	0.983 53
10	2 678	0.980 85
5	642	0.981 51

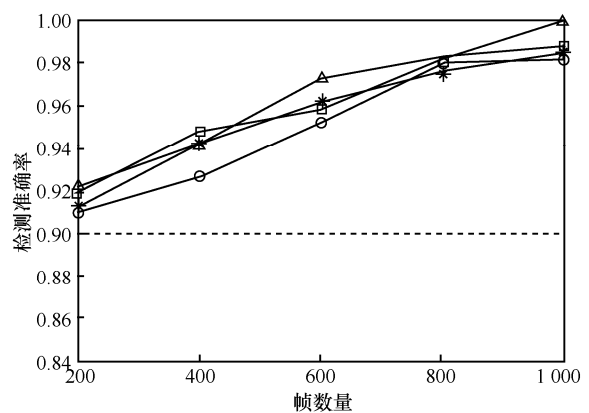


图 4 准确率与 Beacon 帧数量关系

6.3 方案对比

1) 对比本文方案

集中式 LAP 检测算法需要服务器提供 AP 指纹, 终端根据指纹白名单筛选 RAP, 客户端仅做检测操作, 减少了工作量, 也在一定程度上保证了 LAP 列表的稳定唯一性。自主式 RAP 检测算法需将该算法嵌入至终端, 从而 SVM 方可训练学习分类。但训练时需掌握 LAP 的信息, 为了降低采集数据过拟合现象, 还需有 RAP 信息完成学习。具体方案对比如表 3 所示。

2) 相关工作对比表

笔者从方案实施检测方、参数设置、准确率等方面, 对比本文方案与其他文献相关工作, 具体如表 4 所示。

表 4 本文方案相关工作对比

方案	检测端	参数	检测 RAP 类型	其他和不足	准确率
文献[7]	服务器	—	中间人攻击	采用 HNN 算法, 但所需数据集较大	—
文献[8]	服务器	Clock skew	中间人攻击	需预先建立数据库, 再进行比较	90%
文献[4]	服务器	BF size	Phishing AP	TSV 对检测率影响较大	100%
文献[6]	终端	RTT	“2 跳”的	传输速度受网络类型、带宽和拥塞状况影响	100%
文献[10]	终端	RSSI	“2 跳”的	信号强度受干扰大	95%
本文	终端	3 个	广播/接入 AP	实时更新白名单受限服务器	>98%

7 结束语

RAP 普遍存在如中间人攻击和网络嗅探等攻击, 在很大程度上泄露了用户的位置信息、上网行为和社交关系等隐私信息。因此, 本文提出了一种基于指纹的 RAP 检测算法, 利用 Beacon 帧参数的不可伪造性和稳定性判断 AP 的合法性。首先, 根据 Beacon 帧特征参数训练学习 LAP 指纹, 构成 LAP 指纹白名单, AP 的特性参数不易受影响和篡改, 保证了离线指纹的可靠性。然后, 用户以 AP 指纹为基础, 利用服务器发布的检测算法进行 RAP 校验。在自主式方法中, 终端利用机器学习方法在线检测 RAP, 降低了因定量设置阈值检测伪 RAP 造成的误判率。本文所提方法在传输数据是加密的情况下, 仍适用于检测多种攻击方式 RAP。

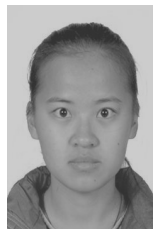
参考文献:

- [1] WANG C, TAI T. Achieving time-based fairness for VoIP applications in IEEE 802.11 WLAN using a cross-layer approach[C]//IEEE International Symposium on Personal Indoor and Mobile Radio Communications. 2010:1475-1480.
- [2] SANDEEP B V. Rogue access point detection using multi parameter dynamic feature analysis for wireless LAN[D]. Bharati Vidyapeeth University, 2016.
- [3] HAN H, SHENG B, TAN C, et al. A timing-based scheme for rogue AP detection[J]. IEEE Transactions on Parallel & Distributed Systems, 2011, 22(11):1912-1925.
- [4] ALOTAIBI B, ELLEITHY K. An empirical fingerprint framework to detect rogue access points[C]//Systems, Applications and Technology Conference. 2015:1-7.
- [5] KIM I, SEO J, SHON T, et al. A novel approach to detection of mobile rogue access points[J]. Security & Communication Networks, 2015, 7(10):1510-1516.
- [6] DAHIYA M, GILL S. Detection of rogue access point in WLAN using hopfield neural network[J]. International Journal of Electrical & Computer Engineering, 2017, 7(2):1060-1070.
- [7] JADHAV S, VANJALE S B, MANE P B. Illegal access point de-

tection using clock skews method in wireless LAN[C]//The International Conference on Computing for Sustainable Global Development. 2014:724-729.

- [8] ZHENG X, WANG C, CHEN Y, et al. Accurate rogue access point localization leveraging fine-grained channel information[C]//Communications and Network Security. 2014:211-219.
- [9] KIM T, PARK H, JUNG H, et al. Online detection of fake access points using received signal strengths[C]//Vehicular Technology Conference. 2012:1-5.
- [10] 李晴, 叶阿勇, 许力. 公众环境下无线接入的安全问题研究[J]. 信息安全, 2016 (4):69-75.
- LI Q, YE A, XU L. Research on security issues of wireless access in public environment[J]. Netinfo Security, 2016 (4):69-75.
- [11] CHENG N, WANG X, CHENG W, et al. Characterizing privacy leakage of public WiFi networks for users on travel[C]//IEEE INFOCOM. 2013:2769-2777.

[作者简介]



李晴 (1992-), 女, 福建莆田人, 福建师范大学硕士生, 主要研究方向为网络与信息安全。



叶阿勇 (1977-), 男, 福建漳州人, 福建师范大学教授, 主要研究方向为无线网络技术、隐私与安全、信息服务。

姚志强 (1967-), 男, 福建莆田人, 福建师范大学教授, 主要研究方向为软件服务工程方法、多媒体信息网络与安全。

陈爱民 (1965-), 男, 福建莆田人, 福建师范大学副教授, 主要研究方向为数据库与图像处理及其应用。