

一种基于位置指纹的无感知 WLAN 认证方案

马 飞^{1,2}, 李 娟¹

(1 北方民族大学 计算机科学与工程学院, 宁夏 银川 750021; 2 合肥工业大学 计算机与信息学院, 安徽 合肥 230009)

摘 要: 提出了一种新颖的无感知 WLAN 认证方案, 该方案利用无线信号的 RSSI 值很难被伪造的特性, 采用改进的 K-means 聚类算法降低环境因素对 RSSI 值产生的波动影响, 构造了基于 RSSI 的 Radio Map, 利用 RSSI 位置指纹匹配技术对访问 WLAN 的用户进行身份认证. 通过在 IEEE802.11g 环境下的测试结果表明, 该方案具有抗干扰能力强, 认证成功率高优点.

关键词: WLAN; 身份认证; RSSI 位置指纹; Radio Map; K-means

中图分类号: TN918.1

文献标识码: A

文章编号: 1000-7180(2014)11-0018-05

A Non-sense Authentication Scheme of WLAN Based on Location Fingerprint

MA Fei^{1,2}, LI Juan¹

(1 School of Computer Science and Engineering, Beifang University of Nationalities, Yinchuan 750021, China;

2 School of Computer and Information, Hefei University of Technology, Hefei 230009, China)

Abstract: This paper presents a new non-sense WLAN authentication scheme. By making use of the characteristics that the RSSI value is very difficult to be forged, The scheme adopts the improved K-means clustering algorithm to reduce the influence of environmental factors on wireless signal RSSI value and constructs the Radio Map based on RSSI. the scheme examines and authenticates user's access to WLAN by adopting RSSI location fingerprint matching technology. Through testing in the environment of IEEE802.11g, it shows that the scheme has the advantage of strong anti-jamming capability and high rate of successful authentication.

Key words: WLAN; authentication; RSSI location fingerprint; Radio Map; K-means

1 引言

随着 WLAN(Wireless LAN)技术的快速发展, 越来越多的用户通过访问 Wi-Fi 热点联入 WLAN 来获取感兴趣的资源. 而 WLAN 则通过有效的审核认证机制来控制用户对 WLAN 资源的合法使用. 目前常用的网络认证技术主要是采用口令密码认证, 数字证书认证等技术. IEEE802.11 委员会推出了 WEP(Wired Equivalent Privacy), WPA(Wi-Fi Protected Access), 802.1x^[1-2]等安全加密通信及安全认证协议, 各移动服务提供商也实施了移动平台环境下的 Portal、MAC 绑定、EAP-PEAP、EAP-

SIM^[3]等认证方案. 但由于 WLAN 环境的开放性特点, 攻击者很容易监听报文中的用户 ID 及密码信息, 并利用这些信息伪造合法身份登陆到 WLAN 进行非法访问, 更严重的是对网络的正常运行造成破坏. 如何降低因用户 ID 和密码被盗而带来的非法访问问题, 并能利用 WLAN 环境和用户的一些内在物理属性来进行入网的审核认证是本文重点研究与解决的问题.

2 认证访问控制方案原理与实现

2.1 方案基本原理

在无线网络环境下, RSSI (Received signal

收稿日期: 2014-03-03; 修回日期: 2014-05-22

基金项目: 北方民族大学科研项目(2013XYZ029)

strength Indication)^[4-5]指的是发送站发送的信号经传输后到达接收站点时的信号强度,该值与所处的环境、收发双方之间的距离等环境因素有直接关联,RSSI 值具有很难被伪造的特性.图 1 所示的是典型的 WLAN 结构.

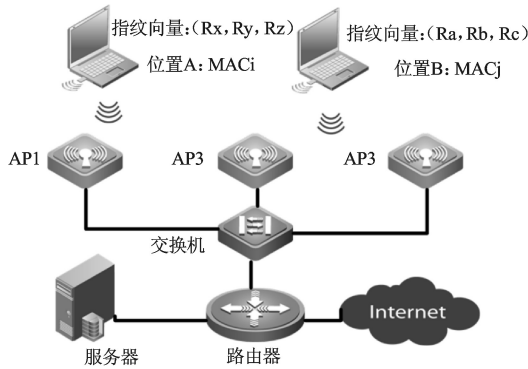


图 1 WLAN 结构图

在图 1 中,位置点 A 与 B 处各放置了一台物理地址分别为 MACi 和 MACj 的无线 STA(Station).三台 AP(Access Point)分别标识为 AP1、AP2、AP3. Rx、Ry 和 Rz 分别为 AP1、AP2 和 AP3 采集到的 MACi 站点在位置 A 所发送信号到达各 AP 点后的 RSSI 值,这三个值构成 MACi 站点在位置点 A 的位置指纹向量,记为 $MACi(Rx, Ry, Rz)$. 同样 $MACj(Ra, Rb, Rc)$ 为 MACj 站点在位置 B 处的位置指纹向量. 工作 AP 的数量至少为 3,这样才能形成有效的具有唯一性的 RSSI 位置指纹向量. 每个 RSSI 位置指纹向量都与发出信号的 STA 的物理位置及 MAC 地址有唯一关联关系. 在图 1 中,位置点 A 与 B 相隔一定的距离,而 RSSI 与距离及环境因素直接相关,所以 A 点与 B 点的 RSSI 位置指纹向量必然不相同. 在 WLAN 布置完毕,所有 STA 和 AP 的位置固定后,每个 STA 在其所处位置的 RSSI 位置指纹向量是唯一的,不会与其他位置点 STA 的 RSSI 位置指纹向量相同,本文实现的认证方案就是充分利用了 RSSI 位置指纹向量与物理位置及 MAC 地址直接关联且唯一对应的特性,把该特性应用到 WLAN 的认证机制中.

下面考虑三种认证情况

CASE1:合法 STA 在合法位置访问网络

当 MACj 站点在 B 点,MACi 站点在 A 点访问 WLAN,对这种合法 STA 在合法位置提出的联网请求,认证方案是认可的,允许联网. 方案会记录每个合法 STA 在其合法位置的 RSSI 位置指纹向量,当 STA 提出联网请求时,认证机制通过位置指纹判

匹配,就可判断出其身份与位置的合法性.

CASE2:合法 STA 在非法位置访问网络

若 MACj 站点由位置点 B 处移动到位置点 A 处发送信号,则其 RSSI 位置指纹向量由 $MACj(Ra, Rb, Rc)$ 变为 $MACj(Rx, Ry, Rz)$,而 WLAN 认证机制认可的在 A 点处的位置指纹向量为: $MACi(Rx, Ry, Rz)$,这两个位置指纹向量显然因关联的 MAC 地址不同而有差异,则 WLAN 认证机制将会拒绝 MACj 站点在 A 处与 WLAN 进行联网.

CASE3:非法 STA 伪造合法 MAC 地址访问网络

假设 MACj 站点为攻击者,MACi 为合法用户,MACj 为了绕开系统的 ACL(Access Control List)访问控制机构,其修改自己的物理地址变为 MACi,希望在 B 位置处以合法用户 MACi 的身份访问 WLAN,可以看到,尽管攻击者伪造了 MAC 地址,但其很难伪造 MACi 在 A 处的 RSSI 位置指纹向量,所以这种低层 MAC 地址欺骗也很容易通过位置指纹匹配技术检测到,WLAN 认证机制拒绝其访问网络.

认证方案能够正确实施要基于两个前提:

- (1)各无线 STA 的位置基本固定;
- (2)工作 AP 数量大于等于 3.

前一个条件容易满足,因为对一般的公司而言,每个员工的台式电脑基本固定,并且出于安全考虑,公司也不希望这些电脑随便移动位置. 而后一个条件也会因为现在的公司为了保证上网质量基本都采用了冗余 AP 架构方案^[6]而得到满足.

以上是本文所采用的位置指纹认证方案的基本思想,这个方案要求每个具有合法 MAC 地址的 STA 必须在 WLAN 认证机制认可的合法位置对 WLAN 进行访问,否则拒绝其入网.

认证方案的优点:WLAN 认证管理机制可以不必设置高层的认证过程,直接采用每个 STA 所处位置的 RSSI 指纹向量和 MAC 地址作为认证信息,而这两种信息可由 STA 的硬件及无线信号直接提供,所以只要用户具有合法的 MAC 地址并在合法的位置访问网络,就不必再手动输入 ID 及对应的密码,可以“无感知”的直接入网,简化了用户的操作,并避免了用户因遗忘或被盗 ID 与密码信息带来的管理及安全方面的问题.

2.2 位置指纹数据库

在认证访问控制方案中,建立整个 WLAN 环境下的 Radio Map(位置指纹数据库)^[7-9]是非常重要的环节,本文的试验环境设置如图 2 所示.

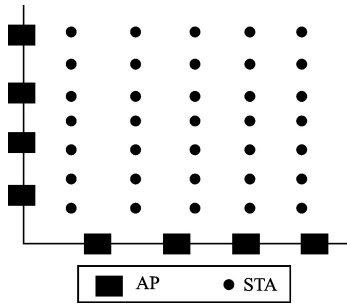


图2 试验环境平面图

图1中,设置了8个AP点(用实心方块表示),35个无线STA(用实心小圆表示).由于RSSI的米级别的定位精度,决定了这些位置点间隔的距离不能太近,所以在本文试验中,各位置点间隔都 ≥ 2 米.采集RSSI值的系统结构如图1所示,预先布置的AP点将采集所有位置点处的STA发出信号的RSSI值,并交付于Server,经处理后形成每个位置点的RSSI位置指纹向量,这些向量最终构成了Radio Map,其结构如表1所示.

表1 RSSI位置指纹数据库结构

MAC ID	RSSI位置指纹向量	位置点ID
MAC _i	$\langle R_{i1}, R_{i2}, \dots, R_{im} \rangle$	PID _j

其中,MAC_i为位于位置点PID_j的STA的MAC地址, $\langle R_{i1}, R_{i2}, \dots, R_{im} \rangle$ 为该STA在PID_j位置点的RSSI位置指纹向量,PID_j为该站点所处位置的ID标识.其中 $i, j \in n$, n 为位置点个数, m 为AP点个数.

信号因受环境因素的影响,各AP采集到的由同一测试位置点处的STA发出的信号RSSI数值会产生波动,这种信号的数值波动满足高斯混和分布.目前形成Radio Map的方法主要是计算RSSI的均值,然后构成RSSI均值向量作为相应位置点的RSSI位置指纹向量.通过观察,尽管存在这种波动,但还是会让同一位置点处的STA发出的信号RSSI值形成一个“簇”.找到这个簇的中心,则这个簇中心所代表的RSSI向量就可以作为该位置点的位置指纹向量,并且由于位置点数量已经确定,则可以采用聚类算法对所有采集到RSSI值进行聚类,最终形成的每个簇的中心就可作为相应位置点的位置指纹向量,这样做的优点是可以不必过多考虑STA与各AP点的方向、角度、信号传播时间、障碍物等因素对RSSI值产生的影响,所以本文采用了一种改进的K-means聚类算法^[10-11]来形成Radio Map.

2.3 改进的K-means聚类算法

在选择形成Radio Map的聚类算法时,并没有直接采用传统的K-means算法,因为原算法在开始阶段的初始簇中心是随机产生的,从而导致了算法的不稳定性,而本文让在每个位置点的STA单独发送信号,其它位置点的STA静默,各AP采集到的RSSI值构成的RSSI向量就可以作为簇的初始中心,这样做的目的是让算法尽快收敛.其余的工作步骤和传统K-means算法一致,具体算法步骤如下:

(1)给定大小为K的RSSI向量集,选择已经计算好的每个位置点的初始RSSI向量作为初始聚类中心 $Z_j(I)$, $I=1, j=1, 2, 3, \dots, M$,其中M为位置点个数;

(2)计算RSSI向量集中的每个向量与聚类中心的欧氏距离,即计算:

$$D(x_i, Z_j(I)) = \sqrt{(x_{i1} - x_{j1})^2 + (x_{i2} - x_{j2})^2 + \dots + (x_{in} - x_{jn})^2} \quad (1)$$

式中, $x_i = (x_{i1}, x_{i2}, \dots, x_{in})$, $Z_j(I) = (x_{j1}, x_{j2}, \dots, x_{jn})$ 都为N维RSSI向量,N为工作AP的个数. $i=1, 2, \dots, K$, $j=1, 2, 3, \dots, M$.如果满足:

$$D(x_i, Z_k(I)) = \min\{D(x_i, Z_j(I)), j=1, 2, 3, \dots, M\} \quad (2)$$

则 $x_i \in w_k$;

(3)计算误差平方和准则函数 J_c :

$$J_c(I) = \sum_{j=1}^M \sum_{n=1}^{K_j} \|x_n(j) - Z_j(I)\|^2 \quad (3)$$

(4)判断:若 $|J_c(I) - J_c(I-1)| < \xi$ 则算法结束;否则 $I = I + 1$,计算M个聚类中心:

$$Z_j(I) = \frac{1}{n} \sum_{i=1}^{n_j} x_i^{(j)}, j=1, 2, 3, \dots, M \quad (4)$$

返回(2)

2.4 位置指纹认证过程

符号定义如下所示.

(1)SMAC_{ij}:位于位置点j(PID_j)处具有物理地MAC_i的STA;

(2)RMAC_{ij}:物理地址为MAC_i的STA在位置(PID_j)处的RSSI位置指纹向量;

假设SMAC_{im}在位置点m(PID_m)处发出联网请求,而j(PID_j)为该STA应该所处的合法位置点.若PID_m与PID_j相同,则代表该STA在其合法位置发出联网请求,如果二者不相同,代表其在非法位置发出联网请求.则整个认证过程就是判断SMAC_{im}是在合法位置提出联网请求,还是在非法

位置提出联网请求.具体的认证过程如下所示.

Step1:各 AP 点采集由 SMACim 在位置点 m 发出的信号到达 AP 点的 RSSI 值,并连同其物理地址 MACi 一起交由 Server 运行改进的 K-means 聚类算法进行数据处理,找到其簇的 Centroid 中心,该中心所对应的向量就是 SMACim 在其发送位置 m 的指纹向量,记为 RMACim;

Step2:Server 用 SMACim 的物理地址 MACi 作为关键字去检索 Radio Map,若没有找到匹配项,则以非法访问直接报警(被 ACL 拒绝),否则转到 Step3;

Step3:Server 计算 RMACim 与 Radio Map 中存放的每一条 RSSI 位置指纹向量(记为 RMACxy)间的 Euclidean 距离,即计算公式(5):

$$\| \text{RMACim} - \text{RMACxy} \| = \sqrt{\sum_{n=1}^N (R_{na} - R_{nb})^2} \quad (5)$$

式中, N 为 RSSI 位置指纹向量的维数,也即进行采样的 AP 点的个数. “Rna”与“Rnb”分别为 RMACim 与 RMACxy 中的相应的分量.经过计算后找到离 RMACim 最近的 RSSI 位置指纹向量,记为 RMACxy’.

Step4:在 Radio Map 中,若 RMACxy’所属记录的 MAC ID 项的值与 MACi 相等,也就意味着 PIDm 与 PIDj 值相同,表明 SMACim 确实在其合法位置 j(PIDj)提出的联网请求,则认证成功,允许 SMACim 联网,否则拒绝其联网.

3 认证方案测试与结果分析

按图 2 所示为对 IEEE 802.11g 网络进行设备布署.共安装了 8 台 AP,为了保证试验对测试点间的间距要求并依据不同的测试目的,每次选取 35 个位置点中的 10 个作为一组测试点,共随机选取了 25 组.开启的工作 AP 数量也随着不同的测试有所增减.每个测试位置点处的 STA 发送帧,各 AP 点持续对各 STA 所发信号的 RSSI 值采样 3 分钟.

3.1 认证方案测试

(1)测试 1

测试目的:STA 不同间隔对认证成功率的

影响;
环境参数:位置点间隔 3 m、5 m 和 7 m,测试点人员较少时(下班时段),工作 AP 点个数为 4.

(2)测试 2

测试目的:人员密集度对认证成功率的影响;

环境参数:位置点间隔 4 m,工作 AP 点个数

为 4;

测试时间段:人员较多时段(上班时段)与人员较少时段(下班时段).

(3)测试 3

测试目的:工作 AP 数量对认证成功率的影响;

环境参数:各位置点间隔 4 m,下班时段.

3.2 测试结果分析

测试 1 研究了 STA 不同间隔对认证成功率的影响,从表 2 试验结果中可以看到,认证成功率随着位置点间的间隔增大而上升,原因在于间隔越大各位置点间的 RSSI 指纹向量间的区别度越大,在进行认证判定时的成功率也越高,同时误判率也在下降.

表 2 位置点间不同间隔对认证的影响

位置间隔/m	认证成功率/%	认证错误率/%
3	94.45	4.24
5	97.38	2.01
7	98.67	1.12

测试 2 主要是为了研究人员活动因素对认证准确度的影响,从测试结果表 3 中可以看到,在人员较多的上班时段认证成功率要低于人员较小的下班时段,误判率也较高,原因在于试验中的 Radio Map 是在下班时段进行数据训练建立而成,而 IEEE802.11g 网络的工作频率为 2.4 GHz,与水的共振频率相同,而人体的主要成份是水,所以当环境中大量人员进行活动时会对信号的传播带来影响或干扰,而这种干扰会影响到 RSSI 值的采样及认证的准确度.

表 3 人员密集度对认证的影响 %

时段	认证成功率	认证错误率
上班时段	94.28	3.93
下班时段	96.74	2.67

测试 3 主要是为了研究工作 AP 点的数量对认证准确度的影响,从表 4 测试结果看出,随着工作 AP 数量的增大,认证的准确性在增加,但增加的幅度不大,比较平缓.说明在形成 RSSI 指纹向量时,工作 AP 的个数只要满足大于等于 3 时就已经可以形成有效的 RSSI 向量来进行认证了.故在不必过多考虑网络性能的情况下,认证需要的工作 AP 数量等于 3 即可.

表 4 工作 AP 的数量对认证的影响

工作 AP 数量/台	认证成功率/%	认证错误率/%
4	96.45	2.84
6	98.38	1.17
8	98.67	1.04

由于移动站和固定站的 RSSI 模式完全不同,本文实现的认证方法的应用环境是固定站模式.在该模式下,在离线 RSSI 采集阶段可获得稳定的 Radio Map.但由于 RSSI 易受外界环境变化的影响,所以要定期更新 Radio Map 以保证高的认证准确度.

4 结束语

本文设计和实现了一种新颖的无感知 WLAN 认证方案,该方案利用无线信号的 RSSI 值很难被伪造的特性,采用改进的 K-means 聚类算法降低环境因素对 RSSI 带来的波动影响,构造了基于 RSSI 的 Radio Map,然后通过 RSSI 位置指纹区配对用户访问 WLAN 进行审核认证.测试结果表明,该方法具有抗干扰能力强,认证成功率高优点.

参考文献:

- [1] IEEE Standards Board 802 part 11. Wireless LAN medium access control and physical layer specifications [S]. IEEE Standard 802.11, 1999.
- [2] IEEE Standard 802.11X: Port-based network access control for local and metropolitan area networks [S]. IEEE Standard 802.11X, 2004.
- [3] 中国移动 WLAN 用户接入流程技术规范 [S]. 北京:中国移动通信有限公司, 2008.
- [4] Koski L, Perala T, Piche R. Indoor positioning using WLAN coverage area estimates[C]// International Conference on Indoor Positioning and Indoor Navigation, Switzerland, 2010.
- [5] Kamol, Kaemarungsi, Krishnamurthy. Properties of

indoor received signal strength for WLAN location fingerprinting ubiquitous [C] // First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous'04). USA: Boston, 2004.

- [6] 文柳. WLAN 无线接入网络规划 [D]. 北京:北京邮电大学, 2010.
- [7] Azin Arya, Philippe Godlewski. An analysis of radio fingerprints behavior in the context of RSSI-based location fingerprinting systems [C] // Proceedings of the 5th ACM international workshop on mobility management and wireless access. Canada: Toronto, ACM, 2007:1-8.
- [8] Kamol Kaemarungsi, Prashant Krishnamurthy. Analysis of WLAN's received signal strength indication for indoor location fingerprinting [J]. Pervasive and Mobile Computing, 2012, 8(2):292-316.
- [9] 冯柳平, 刘祥南, 刘明业. IEEE 802.11 访问控制与 MAC 地址欺骗 [J]. 微电子学与计算机, 2006, 23(1): 25-27.
- [10] 周爱武, 于亚飞. K-Means 聚类算法的研究 [J]. 计算机技术与发展, 2011(2):48-61.
- [11] 许虎寅, 王治和. 一种改进的基于密度的聚类算法 [J]. 微电子学与计算机, 2012, 29(2):44-47.

作者简介:

马飞 男, (1976-), 博士, 副教授. 研究方向为网络安全, 云计算、社交网络分析、隐私保护.

李娟 女, (1975-), 硕士, 副教授. 研究方向为网络安全、云计算.

(上接第 17 页)

参考文献:

- [1] Wang Hongwei, Zhan Yanglin, Liang Liping. A coverage-driven auto-verification platform [J]. Electronic test, 2013(5):82-84.
- [2] Zhong Wenfeng. System verilog and function verification [M]. Beijing: China Machine Press, 2010.
- [3] 田劲, 王小力. 基于 UVM 验证方法学的 AES 模块级验证 [J]. 微电子学与计算机, 2012, 29(8):86-90.
- [4] 谢峥, 王腾, 雍姗姗, 等. 一种基于 UVM 面向 RISC CPU 的可重用功能验证平台 [J]. 北京大学学报:自然科学版, 2014, 50(2):221-227.
- [5] Namdo Kim, YoungNam Yun, YoungRae Cho, et al. How to automate millions lines of top-level UVM test-bench and handle huge register classes [J]. IEEE, 2012:405-407.
- [6] Zheng Xie, Wang Xin'an, Lian Zhibin, et al. A novel intelligent verification platform based on a structured

analysis model [J]. Science China Information Sciences, 2013, 56(6):1-14.

- [7] Wang Shizhong, Tian Ze, Wu Xiaocheng, et al. Function verification of time synchronization circuit based on UVM [EB/OL]. (2013-04-18). [2014-01-10]. <http://www.cnki.net/kcms/detail/61.1450.TP.20130418.1701.005.html>.
- [8] Cappelli F, Lavagno A, Canegallo R, et al. A reconfigurable processor architecture and software development environment for embedded systems [C] // IPDPS'03. France, Nice, 2003.

作者简介:

徐金甫 男, (1965-), 博士, 副教授. 研究方向为专用集成电路设计与验证.

李森森 男, (1988-), 硕士. 研究方向为专用集成电路设计与验证.