一种基于RSSI的智能家居环境Evil-Twin攻击的检测方法

房鼎益[1),2)] 祁生德[1),2)] 汤战勇[1),2)] 陈晓江[1),2)] 顾元祥[2),3)]

[1)](西北大学信息科学与技术学院 西安 710127)

[2)](西北大学-爱迪德信息安全联合实验室 西安 710127)

[3)](爱迪德技术(北京)有限公司 北京 100125)

摘 要 Wi-Fi正在为各种各样的设备提供网络连接,但因其网络标识(SSID,BSSID)易被伪造,攻击者很容易伪造出普通用户无法识别的Evil-Twin AP并进行其他高级攻击.本文利用智能家居中AP位置稳定的特点,提出了基于RSSI的Evil-Twin攻击检测方法,它由单位置检测和多位置协同检测两种方案组成.该方法将Evil-Twin攻击检测问题转化为AP位置检测问题,两种方案都需要先在安全环境中构建指纹库.单位置检测时,确定当前检测到的目标AP与检测器之间的距离,并与指纹库中的安全距离进行比较,判断其安全性;多位置协同检测时,则先通过参考AP进行室内定位,确定检测设备的位置,然后反向定位确定当前检测到的目标AP与检测设备之间的距离,并与指纹库中该位置处的安全距离进行比较,判断其安全性.成功解决了基于AP硬件特征或流量特征的检测方法易被绕过的问题.该方法与已有的检测方法相比,检测设备不连入网络时依然可以成功检测,且无需加入专业的检测设备.实验结果显示,单位置检测方案将延迟时间降低至20 s,且检测正确率达到98%,使用多位置协同检测时,正确率也达到90%.

关键词 智能家居;邪恶双胞胎;无线网络;攻击位置检测;伪造AP;信号强度;物联网;传感器网络;信息物理融合系统

中图法分类号 TP311 **DOI号** 10.11897/SP.J.1016.2017.01764

An Evil-Twin AP Detection Method Based on RSSI in Smart Home

FANG Ding-Yi[1),2)] QI Sheng-De[1),2)] TANG Zhan-Yong[1),2)] Chen Xiao-Jiang[1),2)] GU Yuan-Xiang[2),3)]

[1)](*School of Information Science and Technology, Northwest University, Xi'an* 710127)

[2)](*NWU-Irdeto Network-Information Security Joint Laboratory (NISL), Xi'an* 710127)

[3)](*Irdeto Access Technology (Beijing) Co. Ltd., Beijing* 100125)

Abstract Wi-Fi is now widely used for providing internet service. Since the identifiers (SSID, BSSID) of Wi-Fi could be faked easily, attackers could deploy an Evil-Twin AP, and users could not distinguish it from the legitimate one. Based on the fact of that the location of APs are relatively stable in the scenarios of Smart Home, a RSSI-based Evil-Twin Attack detection method was proposed. It consisted of two detection strategies: single position detection and multiple position cooperative detection. This method converted the detection of Evil-Twin Attack to the detection of the locations of APs, both of the two schemes should build a fingerprint database firstly in a security Wi-Fi condition. When it comes to single position detection, the distance between the detected target AP and the detector should be firstly computed, then comparing it

收稿日期:2016-06-30;在线出版日期:2017-03-07.本课题得到国际科技合作与交流计划(2015KW-003)、国家自然科学基金(61672427,61272461,61202393)、省教育厅产业化培育项目(2013JC07)资助.**房鼎益**,男,1959年生,博士,教授,博士生导师,中国计算机学会(CCF)高级会员,主要研究领域为网络与信息安全、软件安全与保护、无线传感器网络关键技术.E-mail:dyf@nwu.edu.cn.**祁生德**,男,1990年生,硕士,主要研究方向为软件安全、物联网安全.**汤战勇**(通信作者),男,1979年生,博士,副教授,中国计算机学会(CCF)会员,主要研究方向为软件安全与保护、无线传感网安全.E-mail:zytang@nwu.edu.cn.**陈晓江**,男,1973年生,博士,教授,中国计算机学会(CCF)会员,主要研究领域为无线传感网络、软件安全与保护.**顾元祥**,男,1951年生,教授,首席架构师,主要研究领域为计算机系统安全与保护、软件安全与保护.

with the safe distance stored in the database, and checking to determine the security. As for multi-position cooperative detection, we should proceed an indoor positioning to get the position of the detector by reference APs, then confirm the distance between the detected target AP and the detector, lastly comparing it with the safe distance of the position, and checking to determine the security. This method fixed the vulnerabilities of existing methods based on hardware fingerprint or traffic feature. Compared to traditional detection methods, the proposed method could finish the detection without network or professional devices. Experimental results showed that single position detection reduced the delay time to 20s and raised the accuracy to 98%, and that multiple position detection raised the accuracy to 90%.

Keywords　smart home; evil-twin attack; wireless networks; attack position detection; fake AP; RSSI; Internet of Things; sensor networks; Cyber-Physical System

1　引　言

根据 Gartner 的报告，随着物联网的发展，到 2020 年，将会有接近 260 亿的智能设备出现，ABI Research 则估计到 2020 年，会有超过 30 亿的设备通过无线网络连接到 IoT[①]. 各种各样的智能设备使用无线网络通信并组成各类 IoT 应用，比如智能家居、智能交通等，它们将完成更多与人类生活息息相关的功能，这使得生活中的安全问题与无线网络的安全更加密不可分. 与人类生活联系最紧密的是家，智能家居环境中无法使用大量线缆，几乎所有设备都通过无线通信，ZigBee 虽然具有功耗低、成本低、网络容量大的特点，但其传输速率较低，无法满足智能家居中对数据传输实时性要求较高的设备. Wi-Fi 网络本身已经普及且组网简单、灵活性高、移动性好、传输速率快，所以被广泛应用于智能家居中. 但 Wi-Fi 作为无线网络，其传输介质开放、信号覆盖范围不可控，致使攻击者可以在信号覆盖范围内任意位置实施攻击，故其安全问题尤为突出.

Wi-Fi 网络的标识 SSID(Service Set Identifier)和 BSSID(Basic Service Set Identifier)易被伪造，攻击者可以很容易部署出普通用户无法与合法 AP(Access Point)区分开来的 Evil-Twin AP(后文中的伪 AP 和 Fake AP 都特指 Evil-Twin AP). 以前，这种攻击主要存在于机场、咖啡厅等公共环境中，但随着物联网的发展，私有 Wi-Fi 的攻击价值迅速上升，这种攻击逐渐向着智能家居等环境中的私有 Wi-Fi 发展. 一旦用户连接上这种伪 AP，攻击者即可完全掌控用户的上网环境，进一步实现隐私嗅探、数据恶意篡改等高级攻击，甚至控制智能设备的行为，比如打开或关闭智能门锁等. 这种伪 AP 可以在笔记本电脑上快速布置，甚至可以在其他更小更易隐藏的设备上完成，比如 Wi-Fi Pineapple、Raspberry Pi.

本文将针对智能家居中的伪 AP 来展开研究. 对开放 AP 实施伪 AP 攻击时只需要伪造其 SSID 和 BSSID，但对于有密码保护的 AP 则还需要设置相同的加密方式与密码. 智能家居中的 Wi-Fi 虽然经常使用 WPA 密码保护，但仍然无法阻止攻击者使用常规的暴力破解或 PIN 破解得到密码，且智能家居中各种设备本身的安全性参差不齐，一些设备本身存在的漏洞会泄漏密码，这使得智能家居 Wi-Fi 密码更易被攻击者拿到. 另外，智能家居中各种设备往往有着各自不同的较为复杂的网络设置方式，所以用户一般不会随意修改密码，这就加剧了伪 AP 攻击的危害.

现有的检测伪 AP 的方法主要有两种：基于硬件特征的检测和基于流量特征的检测，但是建立硬件特征指纹库开销大且指纹提取时间长，实时性差，流量特征检测法可被一些高隐蔽性的伪 AP 绕过. 本文根据智能家居中 AP 位置稳定的特点提出了一种新的基于 RSSI 的检测方法. RSSI 与 AP 和接收端之间的距离相关，而该距离又与 AP 和接收端的相对位置有关，所以基于 RSSI 的检测其本质是基于位置的检测. 硬件特征和流量特征均可以被模仿，但位置无法被冒充，这就奠定了 RSSI 检测法的有效性，实验结果也显示基于 RSSI 的伪 AP 的检测法可以有效应对基于硬件特征和流量特征的检测方法无法检测的情况，且检测平均延迟低于 20 s，准确率达到 96%.

① http://en.wikipedia.org/wiki/Internet_of_Things

图 1 给出了基于 RSSI 的伪 AP 检测的原理图，RAP 和 FAP 分别表示真实 AP 和伪 AP，Detector 是检测器，RSSI 和距离 D 负相关. 当真实 AP 和检测器的距离大于伪 AP 和检测器的距离，如图中 D_1 大于 D_1' 时，检测器接收到来自伪 AP 的信号强度大于真实 AP 的信号强度，由于对信号传播中多径效应的处理，检测器每次扫描总会选择同源信号中最强的信号，所以当 FAP_1 启动时，检测器会选择 FAP_1 的 $RSSI_1'$ 作为最终的 RSSI，而 FAP_1 不存在时，会选择 RAP_1 的 $RSSI_1$ 作为最终的 RSSI，若 $RSSI_1'$ 大于 $RSSI_1$，即可判定存在伪 AP. 但是当真实 AP 和检测器的距离小于伪 AP 和检测器的距离，如图中 D_2' 大于 D_2 时，无论是否存在伪 AP，检测器总会选择 RAP_2 的 $RSSI_2$ 作为最终的 RSSI，此时将无法判定是否存在伪 AP，所以需要移动检测器的位置到 $Detector_2$，使得 D_3' 大于 D_3，即可成功检测出伪 AP 的存在. 假定家居环境平均面积为 100 m^2，如此大小的空间内足够找到 $Detector_2$ 这样的位置.

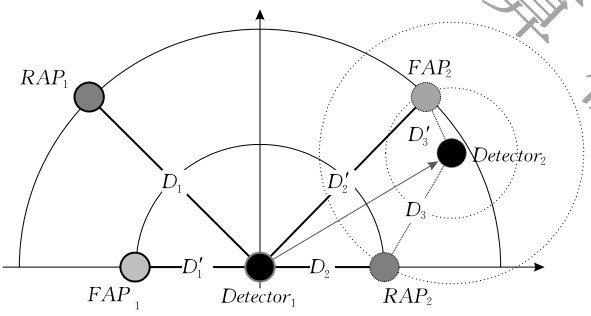


图 1 RSSI 方法原理图

本文主要贡献：(1) 提出一种新的在智能家居中检测伪 AP 的方法，该方法可以有效弥补硬件特征法和流量特征法的不足；(2) 用户无需花费太多时间做伪 AP 检测，只需在日常生活中打开手机 Wi-Fi 即可自动完成检测；(3) 在不加入其它专业检测设备时，依然可以只使用手机完成检测；(4) 通过理论分析和使用真实数据验证了基于 RSSI 的伪 AP 的检测方法的可行性和有效性；(5) 检测设备未连接伪 AP 时，依然可以成功检测，而传统检测的方法中，检测器需要和伪 AP 连接.

本文第 3 节给出伪 AP 的攻击模型；第 4 节提出基于 RSSI 的伪 AP 的检测原理；第 5 节给出单一固定位置的检测方案；第 6 节给出多位置协同检测方案；第 7 节给出对两种方案的验证实验并对结果进行评估；第 8 节对本文工作和以后的工作进行评述.

2 相关工作

目前，主要有两种检测 Evil-Twin 攻击的方法，分别是基于硬件特征的检测和基于流量特征的检测.

硬件特征检测法利用不同的网卡芯片和驱动具有不同的指纹特征这一特点建立指纹特征库，并在检测时通过匹配指纹库中的指纹数据判定是否存在伪 AP. Bratus 等人[1] 发送一些格式错误但标准协议未禁止的“刺激”帧，不同的网卡芯片或驱动对各种“刺激”帧会有不同的响应，但这种检测方法易被攻击者发现，且攻击者可以复制这种特征；Franklin 等人[2] 和 Loh 等人[3] 利用不同的无线网卡扫描网络时发出的 Probe Request 帧的周期不同来建立指纹库，但因设备加入网络时只发送少量的 Probe Request，且使用被动式扫描时该方法将会失效，所以构建指纹库的时间开销很大，检测的实时性较差；Neumann 等人[4] 则利用帧间隔到达时间来识别无线设备，但是该特征可被攻击者伪造，导致基于该特征的检测方法可被绕过. 上述硬件指纹特征检测法各有利弊，可以有效检测多种伪 AP，但攻击者仍然可以伪造硬件特征，且建立硬件特征指纹库的开销大，提取硬件指纹时间长，检测实时性较差，扩展性差.

流量特征检测法根据不存在伪 AP 和存在伪 AP 时网络流量特征的不同来检测是否存在 Evil-Twin AP，这类方法可扩展性好，但也有其缺点. Beyah 等人[5-6] 使用数据包到达时间间隔来构建流量特征库，但受流量整形影响较大，实际操作和应用性不强；Ma 等人为商用 Wi-Fi 开发出一套保护框架，该框架第 1 次结合了分布式无线终端和集中式有线终端在套接字级别的特征作为指纹数据来检测 Evil-Twin AP[7]；Wei 等人[8] 提出使用 TCP 协议中的 ACK 数据包到达时间来构建流量特征库，但其受 TCP 流量影响，限制了检测效率；Sheng 等人[9-11] 提出使用数据往返时延(Round Trip Time，RTT)来检测是否存在伪 AP；Lee 等人[12] 提出了一种 k-SVM 的方法对 RTT 进行分类以检测伪 AP，但 RTT 同时受网络类型、带宽和拥塞状况影响.

此外，Han 等人[13] 提出了车载网络中的无线伪 AP 攻击，同时给出了一种基于 RSSI 的检测方法，该方法需要所有 AP 配备 GPS 模块并报告自身的位置，用户通过所测量的 RSSI 与位置是否匹配来

判断是否存在伪 AP，该方法可以有效检测出车载网络中的伪 AP 攻击；Lee 等人[14]提出将 GPS 信号与 RSSI 结合起来检测伪 AP. 但这种方法不适合室内环境，因为 GPS 信号在室内会被严重削弱甚至被屏蔽.

3　Evil-Twin 攻击

Wi-Fi 网络采用 802.11 协议，而 802.11 并未提供强标识来识别 Wi-Fi 热点，用户能用来识别热点的信息只有 SSID 和 BSSID，甚至绝大多数用户不会用 BSSID 识别热点. 无线网络介质共享，信号覆盖范围不可控，所以这些标识信息可以轻易被攻击者拿到并伪造出具有相同标识的 AP. 对于有密码保护的 AP，首先需要得到其加密方式和密码，加密方式可以直接从 Beacon 中得到，而密码也可以通过多种方式拿到，然后为伪 AP 设置相同的加密方式和密码. 现在，家用 Wi-Fi 最安全也最常用的保护方法是 WPA，但仍无法阻止攻击者暴力破解握手包或利用无线路由的 PIN 功能得到其密码，且随着 Wi-Fi 密码共享软件的发展，攻击者可从密码共享软件的数据库中直接查到密码，除此之外，智能家居中一些设备本身存在的安全漏洞也会泄漏密码. 攻击者拿到密码后即可快速部署出用户无法识别出的 Evil-Twin AP. 我们可在笔记本电脑上快速布置出 Evil-Twin AP，甚至可以在其它更小的设备上完成，比如 Wi-Fi Pineapple、Raspberry Pi 等，具有很好的物理隐蔽性. 伪 AP 攻击，一般会使用一张无线网卡连接到真实 AP，一张无线网卡布置伪 AP，然后将两张网卡桥接，为连接到伪 AP 的设备提供网络服务，或者自身通过其他方式直接连接到 Internet 并为设备提供网络服务. 当用户连接上伪 AP 后，攻击者即可实施更多复杂的攻击，比如隐私嗅探、数据恶意篡改等[15]，当这种攻击扩展到物联网时，会出现更多复杂且高风险的攻击，甚至控制智能设备的行为，比如恶意打开智能门锁.

802.11 协议为实现 ESS 规定当多个相同标识的 AP 同时存在时，终端会选择信号最强的 AP 进行连接[16]，所以布置伪 AP 时会优先选择离攻击目标较近的位置或者使用大功率天线. 伪 AP 布置完成后可实施被动或主动钓鱼，被动钓鱼即只等待终端连接而不主动采取其他措施促使终端连接，该方法因不对真实 AP 造成过大影响而具有较好的隐蔽性，但攻击成功率不高；主动钓鱼则指攻击者布置好伪 AP 后主动使用无线阻塞攻击来切断攻击目标与真实 AP 的连接，促使攻击目标与伪 AP 连接. 若伪 AP 通过真实 AP 访问网络，那么终端的数据仍会流经真实 AP，若伪 AP 通过 3G/4G 等方式访问网络，则终端数据不经过真实 AP.

强制断开终端和 AP 的连接的的无线阻塞攻击可分为物理层攻击和 MAC 层攻击[17]，物理层攻击主要通过射频干扰实现，MAC 层攻击则通过恶意发送某些特殊帧来触发 CSMA/CA 机制的漏洞最终实现阻塞攻击. 现在有效且较隐蔽的攻击方法是 Deauthentication Flood 和 Deassociation Flood[18]. 802.11 协议的认证状态转换如图 2 所示，其解除认证为单向解除，即一旦任何一方接收到解除帧就立即断开连接.

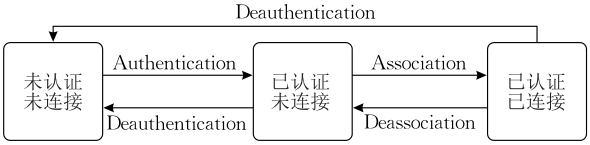


图 2　802.11 认证状态转换

又因 802.11 协议在 MAC 层只通过 MAC 地址判断发送端的合法性，因此，攻击者只需发送 MAC 地址为合法终端或真实 AP 的解除帧，即可快速断开真实 AP 与终端的连接. 如果攻击者持续频繁地发送解除帧，终端将完全无法与 AP 连接，此种攻击具有高隐蔽性和低速率性，对信道干扰时间少，不易被检测到. 另外，该攻击可以针对特定目标进行精准攻击而不影响目标外的设备.

4　基于 RSSI 的 Evil-Twin 检测原理

智能家居中 AP 位置稳定，攻击者无法伪造真实 AP 的位置，所以可以通过定位 AP 的位置来判断 AP 的合法性，于是我们提出了一种新的在智能家居中基于 RSSI 的 Evil-Twin AP 检测法. 在自由空间中，信号传播的路径损耗表示信号的衰减，定义为有效发射功率和接收功率之间的差值，其计算方法如式(1)所示

$$PL(\mathrm{dB}) = 10\log\frac{P_t}{P_r} = -10\log\left[\frac{G_tG_r\lambda^2}{(4\pi)^2d^2}\right] \quad (1)$$

其中：G_t 与 G_r 分别表示发送端和接收端的天线增益；λ 表示信号波长；d 为发送端与接收端的距离.

Wi-Fi 信道 1～信道 13 的频率为 2.412×10^9～2.472×10^9，又 $\lambda=c/f$，其中 $c\approx3\times10^8$ m/s，故 λ 的取值范围是 0.1214～0.1244. 我们做出其衰减曲线

图 3 所示:(a)中发送端和接收端都具有单位增益,信道为 1;(b)中发送端和接收端都具有单位增益,信道为 13;(c)中发送端和接收端增益积为 100,信道为 13;由(a)和(b)可知信道对衰减影响较小,由(b)和(c)可知增益对衰减影响较大,由(a)、(b)、(c)可知距离是影响衰减的主要因素,且随着距离的增加,衰减对距离越来越不敏感.

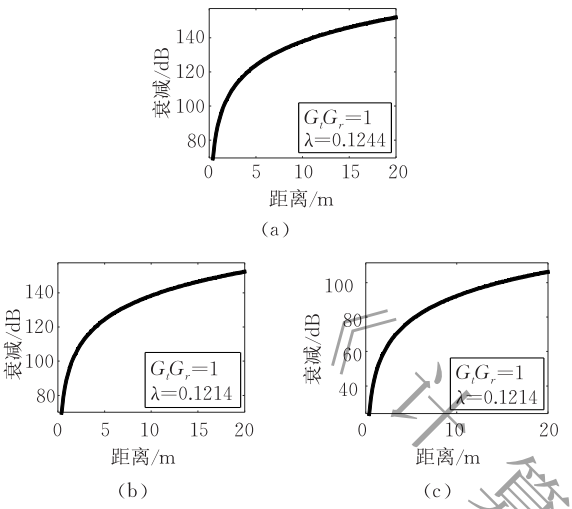


图 3 信号衰减与距离的关系

同时,我们将 PL(dB)对 d 求导,得式(2)

$$PL(\mathrm{dB})' = \frac{d(PL)}{d(d)} = \frac{20}{\ln 10} \cdot \frac{1}{d} \tag{2}$$

其中,$d>0$,因为 $PL(\mathrm{dB})'$与 d 负相关,印证了上面的结论:随着距离的增大,衰减对距离越来越不敏感.

RSSI(Received Signal Strength Indicator)是接收信号的强度指示,其值可以通过如式(3)计算

$$\mathrm{RSSI} = \text{发射功率} + \text{天线增益} - \text{路径损耗} \tag{3}$$

对于一对确定的发送端和接收端来说,发射功率和天线增益都是定值,而路径损耗是关于距离 d 的函数,所以 $RSSI$ 可以表示为 $\mathrm{RSSI}=f(d)$,则 $d=f^{-1}(\mathrm{RSSI})$. 所以,我们可以直接用 $RSSI$ 来代替距离实现定位,为此,我们提出信号空间和信号距离,信号距离 $sd(signal\ distance)$等于 RSSI 的绝对值,信号空间以信号距离的形式表现出来. 如图 4 所示,左图为物理空间,右图为信号空间,两个空间都以 AP 为参考原点,a、b、c、d 为手机的 4 个位置,在物理空间中 a、c、d 与 AP 的距离相等,小于 b 和 AP 的距离,但是在 a 和 d 处有障碍物阻挡信号传输,其中黑色障碍物的衰减因子高于灰色障碍物,所以 $sd_a>sd_d>sd_c$,$sd_b>sd_c$. 一般在无障碍物时直线到达的信号强度最好,无线设备在处理多径效应时总是优先选择强度最好的信号,所以 b 和 c 在信号空间中相对于 AP 的位置与物理空间一致;对于 d 来说,虽然存在障碍物,但障碍物衰减因子较小,使得 AP 与 d 之间穿透障碍物到达的信号比绕射到达的信号强度高,所以 d 在信号空间和物理空间相对于 AP 的方向一致,距离不同;对于 a 来说,障碍物的高衰减因子导致绕射到达的信号强度高于穿透到达的信号,所以信号空间和物理空间中 a 相对于 AP 的方向和距离均不同.

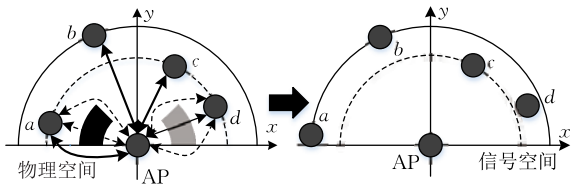


图 4 物理空间转换为信号空间

因为不同环境下信号的衰减模型不同,无法使用统一模型计算检测器与 AP 在物理空间中的距离,所以使用信号距离代替物理距离进行信号空间中的定位.

为分析同一物理位置处的信号距离,我们使用终端 MX3 收集以 TL-WR882N 搭建的 AP 的 RSSI,二者相距 5m,数据收集速率为 2次/s,收集的数据总量约为 14000 条,收集过程中周围环境不变,但有人随意走动. 其概率分布直方图如图 5 所示.

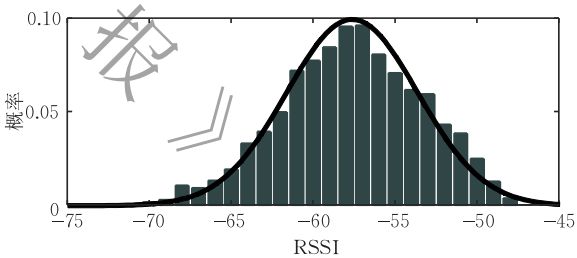


图 5 RSSI 概率分布

通过分析 RSSI 数据发现实际测量值在一个稳定值附近波动,且概率呈现近似正态分布,是一个取决于均值和方差的正态随机变量. 智能家居属私人环境,相对较封闭,干扰因素小,可以形成稳定的 RSSI 指纹,有利于基于 RSSI 的 Evil-Twin 攻击的检测.

我们在安全状态时使用信号空间中的信号距离来构建指纹库. 由于检测器认为伪 AP 与真实 AP 的信号同源,当存在伪 AP 且伪 AP 与检测器的信号距离小于真实 AP 与检测器的信号距离时,检测器将按照处理多径效应时的策略选择伪 AP 来计算自身与"源"的信号距离,并比较新的信号距离与指

纹库中的信号距离，最终判断是否存在伪 AP. 根据是否有手机在智能家居中移动做协同检测，我们提出两种检测方案：单一固定位置检测和多位置协同检测.

5　单一固定位置检测

智能家居设备在家中无人时仍需联网工作，所以检测系统需在无人条件下仍可完成伪 AP 检测. 为此，我们在固定位置安装检测器，并让该检测器 24 h 工作. 检测器在安全状态时建立目标 AP 的 RSSI 指纹库，检测时只需比较检测得到的目标 AP 的 RSSI 指纹与指纹库中记录的指纹，计算新指纹是否在安全范围内，进而判定是否存在伪 AP.

5.1　单一固定位置检测原理

现假定热点与检测器的部署如图 6 所示，其中伪 AP 与真实 AP 位置不同，其他特征如网卡硬件特征、天线增益、稳定性等完全相同；A、B、C 为检测器的三类位置，A 类位置处（Y2）真实 AP 与伪 AP 的信号强度相等，B 处（Y2 左侧）真实 AP 的信号强于伪 AP 的信号，C 处（Y2 右侧）伪 AP 的信号强于真实 AP 的信号.

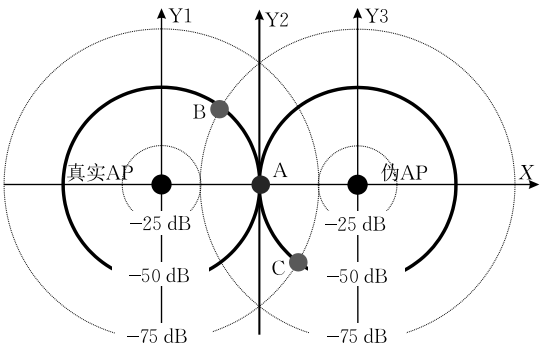


图 6　单一固定位置检测示例图

在安全状态下，即不存在伪 AP 时，A、B、C 三处检测器接收到真实 AP 的 *RSSI* 均值（单位：dBm）和方差如表 1 所示.

表 1　安全状态下 A、B、C 处的均值和方差

位置	均值	方差
A	$\mu_A=-50$	σ_A
B	$\mu_B=-50$	σ_B
C	$\mu_C=-75$	σ_C

在伪 AP 启动后，因多径效应的存在，检测器在 A、B、C 三处选择真实 AP 信号的概率分别为 P_A、P_B、P_C，且理想状态下 $0\leq P_C<P_A=0.5<P_B\leq 1$，则新的均值和方差如表 2 所示.

表 2　启动伪 AP 后 A、B、C 处的均值和方差

位置	均值	方差
A	$\mu'_A=\mu_A=-50$	$\sigma'_A=\sigma_A$
B	$-75<\mu'_B\leq-50$	$\sigma'_B>\sigma_B$
C	$-75<\mu'_C\leq-50$	$\sigma'_C>\sigma_C$

由于多径效应、外界干扰等因素，使得任意位置处的 RSSI 均在一定范围内波动. 在安全状态下，假定均值范围是 $\mu-M\leq\mu\leq\mu+M$，方差满足 $\sigma\leq\Sigma$.

计算均值和方差时，如果收集大量数据后再对总体数据计算均值和方差，会导致检测实时性差、对攻击不敏感. 比如，一次收集 2 h 数据之后再计算这批数据的均值和方差并判断是否存在伪 AP，有可能攻击者在这 2 h 之内已经完成攻击，又或者攻击者只攻击 10 min，10 min 的攻击数据对 2 h 的数据影响很小并最终导致无法检测失败. 另外，如果按照上述方法计算均值和方差，会导致前后 4 h 收集的两批数据无关，两次计算相互孤立，检测过程不连续. 所以我们使用滑动窗口的方法进行计算，如图 7 所示.

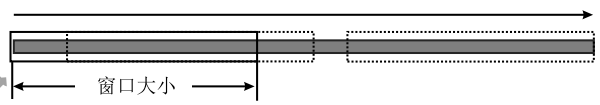


图 7　滑动窗口原理图

窗口越大，检测的延迟性越高，且漏检率越高；相反，窗口越小，检测的延迟性越低，且误检率越高. 在实际检测中，窗口大小可作为可调节参数，根据实际需求进行调节.

检测器刚启动时，收集的数据量小于窗口大小，不进行计算；当数据量等于窗口大小时进行第一次计算；之后检测器每扫描一次，窗口向右滑动一次并计算和判断一次，直到检测器停止工作.

图 6 中，C 类位置处，伪 AP 的信号强于真实 AP 的信号，终端处理多径效应时会优先选择伪 AP 的信号来计算信号强度，所以 $\mu'>\mu$，当 $\mu'>\mu+M$ 时，即可认为出现了伪 AP. 由于均值计算采用滑动窗口算法，所以均值为一系列数据，取 $\mu+M$ 为特征收集阶段的均值最大值 μ_{max}，即当 $\mu'>\mu_{max}$ 时则认为出现了伪 AP；A 类位置处，伪 AP 的信号强度等于真实 AP 的信号强度，所以 $\mu'=\mu$，无法识别出伪 AP；B 类位置处，真实 AP 的信号强度高于伪 AP 的信号强度，但检测器认为真实 AP 的信号和伪 AP 的信号是同源信号，同样因为无线设备处理多径效应的策略导致检测器优先选择真实 AP 的信号来计算该源的信号强度，所以 $\mu'=\mu$，依然无法检测

出伪 AP.

5.2 检测器部署位置选择

由 5.1 节中对三类地址的分析可知:检测器和真实 AP 的距离不可过近,过近会导致检测器无法检测到伪 AP,漏检率极高,另一方面,由第 4 节可知距离越小,RSSI 对距离变化越敏感,当过于敏感时,检测器和 AP 的位置发生小范围合理挪动时会造成较高的误检率.所以,部署检测器时应尽量布置在 C 类位置处,即让检测器距离真实 AP 较远,信号较弱,且离最可能出现攻击的地方较近的位置.

5.3 优缺点分析

该方法获取 RSSI 指纹简单,检测过程中可以无人参与,且可以通过调节窗口大小实现不同的安全性要求.但它的缺点也很明显,在 A 类和 B 类位置处检测器无法检测到伪 AP,检测的成功率与检测器的位置直接相关.

为弥补上述缺陷,我们进一步提出了多位置协同检测法.

6 多位置协同检测

多位置协同检测依赖于手机的移动性,通过人在日常生活中带着手机移动并在不同的位置停留,最终将其转化为多个固定位置的检测.在多个位置做检测时,需要确保检测阶段所比较的 RSSI 指纹和指纹收集阶段所记录的某条 RSSI 指纹来自于同一个位置,所以我们首先需要确定手机的位置.最为人所熟知且精度较高的定位方法是 GPS,但 GPS 信号在室内会被严重削弱甚至被屏蔽.现在的 Wi-Fi 网络非常普及,在一个位置往往可以检测到多个(大于等于 3 个)Wi-Fi 热点,满足 Wi-Fi 信号室内定位的条件,故而可以使用 Wi-Fi 室内定位来确定手机位置.因为室内环境复杂,信号衰减模型很难得到,且用于定位的参考 AP 的位置未知,所以我们选择位置指纹法.一般所说的室内定位的目的是为用户提供物理空间的地址,所以需要将指纹信息和物理空间的地图映射,而此处我们不需要物理空间的地图,所以不需要将指纹信息和物理空间映射.这里的"定位"并不是真正的物理空间的定位,而是信号空间的定位,"位置"也不会映射到物理地图,没有物理空间坐标,它的坐标只是多个 AP 的 RSSI 构成的一个多元组.因为在信号空间的定位不需要用到信号衰减模型,这就减小了定位误差.多位置协同检测的原理主要是通过定位手机的位置,将其转化为多个单一固定位置的检测,如图 8 所示.

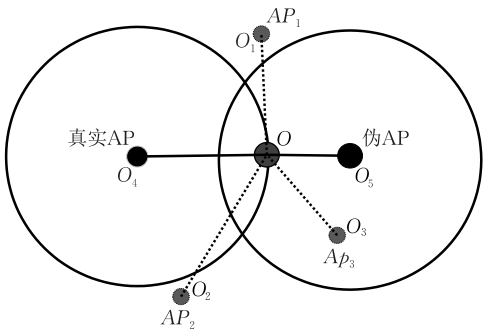


图 8 多位置协同检测原理图

图中 AP_1,AP_2 和 AP_3 是 3 个参考 AP,点 O 是手机的位置,sd_1,sd_2,sd_3 分别是 AP_1,AP_2,AP_3 和手机位置 O 的信号距离,$sd_i=|OO_i|$, $i=1,2,3,4,5$. AP_1,AP_2 和 AP_3 可以定位出手机在此信号空间中的位置,得到手机的位置后即可将该位置处的检测转化为一次单一固定位置检测,多个位置处的检测则转化为多次单一固定位置检测.参考 AP 可以是周围一切非目标 AP 的 AP,可以是邻居家的 AP,也可以是自己家的其他 AP.参考 AP 至少需要 3 个,因为在平面上不共线的 3 个圆最多只有 1 个公共交点,所以可以区分出每一点,如果只有两个参考 AP,理论上有两个点区分不了.

多位置协同检测包括两个阶段:指纹收集阶段和检测阶段.指纹收集阶段,需要先在安全状态下,收集多个位置处的参考 AP 和目标 AP 的 RSSI 信息,并构建指纹库;检测阶段,使用参考 AP 对手机进行定位,并与指纹库中的指纹数据进行匹配,转化为单一固定位置检测,方案框架如图 9 所示.

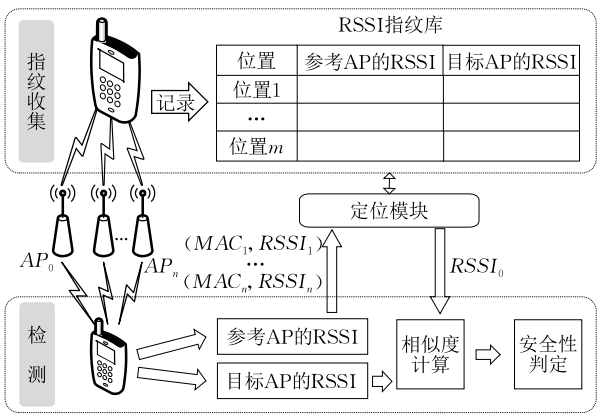


图 9 多位置协同检测框架图

上图中 AP_0 为目标 AP,$AP_2 \sim AP_n$ 为待选参考 AP,整个处理过程可分为以下 5 步.

(1) RSSI 获取;

(2) 有效数据选取;

(3)指纹库的建立；

(4)手机位置确定；

(5)合法性判别.

6.1　RSSI 的获取

多位置协同检测利用的是手机的移动性来实现，所以使用手机来获取 RSSI 值. 检测程序导入相应的管理包(Android：android. net. wifi. * ；IOS：SystemConfiguration/CaptiveNetwork. h)并调用相关的接口，就可让手机在日常活动中获取到足够的 RSSI 数据.

6.2　有效数据选取

有效数据选取包括两部分：有效 RSSI 的选取和有效参考 AP 的选取，这也是本方案最大的两个难题.

6.2.1　有效 RSSI 值的选取

因为手机被人带着移动，所以需要从一个 AP 的大量 RSSI 中选取出位置相对稳定的 RSSI 作为一个位置处的 RSSI 信息，即有效的 RSSI，也就是手机长时间不动或者小范围移动时的稳定 RSSI. 移动过程中停留时间过小，数据还不稳定，所以这些数据对于定位和检测均无效，需要将它们去掉. 如图 10 中所示，两个方框内的数据即为在两个位置相对稳定处采集的数据，框外的数据为移动过程中的数据. 第 1 个框中的数据是手机离 AP 距离为 1 m，且中间无人为干扰；框外的数据为人带着手机以大约 1.5 m/s 的正常步速离开房间并一直移动，然后回到原来的位置，整个过程持续了 100 s，并在 5 s 之后到达一个新的位置；第 2 个框中的数据为手机与 AP 之间距离 4m，且中间有两人在不时的晃动干扰.

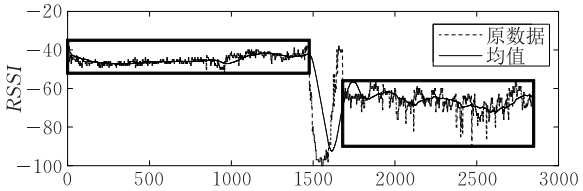


图 10　RSSI 序列图

判断手机是否移动不能用手机的陀螺仪等，因为这里的位置都是信号空间中的位置，且在一定物理空间范围内的移动不一定导致信号空间内的移动. 从大量数据中分离出有效的数据，最简单的方法是使用原始数据进行分离，当 RSSI 超出范围$[a,b]$时则认为位置发生了变化，但是确定该范围需要确定两个参数 a 和 b，且这两个参数都会随着距离的变化而变化，除此之外，该算法易受干扰因素的影响，波动较为剧烈，如图 10 中，原始数据不稳定，尤其是第 2 个框中的数据波动很大，增加了分割的难度. 为解决同一位置处数据波动过大对分割的影响，可以使用均值弱化波动，计算均值时仍使用滑动窗口的算法，当均值超出范围$[c,d]$时则认为位置发生了变化，但是均值算法仍然需要确定两个参数，且参数随着距离的变化而变化，并且在 RSSI 序列中确定位置稳定的开始点延迟性较大，如图 10 中，以窗口大小为 120 计算均值，可以明显看到均值的波动延迟于原始数据. 所以我们提出了方差增量算法.

方差增量算法同样借助于滑动窗口的方法，当数据量小于窗口大小时，数据量过小，不进行计算；当数据量大于等于滑动窗口大小时，第 i 个窗口表示为 W_i

$$W_i=\{r_{i-ws+1},r_{i-ws+2},\cdots,r_{i-1},r_i\},\ i\geq ws,\ r_i\in R$$

其中 R 是整个 RSSI 序列，r_i 是数据集中第 i 个 RSSI，ws 是窗口大小.

方差是各个数据分别与其平均数之差的平方的和的平均数，它可以用来度量窗口内的 RSSI 数据和其均值之间的偏离程度. W_i 的方差 σ_i 就表示 W_i 内数据的波动程度，波动越大，方差越大，人在移动过程中 RSSI 会剧烈波动，方差会快速变大，如图 11 所示，窗口大小为 120，中间两个波峰对应人的移动过程，即对应图 10 中方框外的部分.

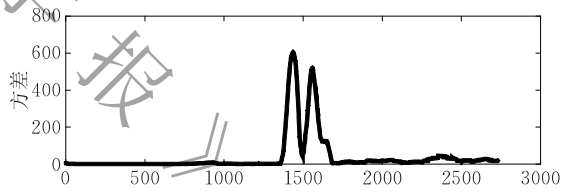


图 11　RSSI 序列方差图

但是，当信号本身不稳定时，方差也很大，所以方差大并不能说明人在移动. 如果由于信号本身不稳定造成方差很大，则整个方差序列会稳定在一个较大值；但若是手机的移动造成方差很大，则手机移动前方差会在一定范围内先稳定，移动时方差迅速增大，所以，可使用方差曲线的斜率来判断当前是否在移动. 这里的方差曲线实质是一系列离散的点，无法对其求导，所以采用类似斜率的方法，求出方差增量$k(i)$如式(3)所示

$$k(i)=\frac{d_{\sigma_i}}{d_i}=\frac{\sigma_i-\sigma_{i-1}}{i-(i-1)}=\sigma_i-\sigma_{i-1}\qquad(3)$$

其中：σ_i 为 W_i 的方差；σ_{i-1} 为 W_{i-1} 的方差. 将图 11 中的方差序列代入式(3)即可得到方差增量序列，如图 12 所示.

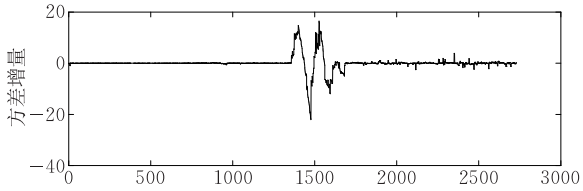


图 12 RSSI 序列方差增量图

当方差增量 $k(i)$在 0 附近波动时，说明原方差稳定在一定范围，即手机没有移动或者小范围移动. 为此，给定阈值 K，当 $|k(i)|\leq K$ 时，则认为手机位置稳定，否则认为手机位置发生了变化. 至此，我们成功将确定手机是否移动的参数由两个降为一个，且该参数受距离影响很小，在不同的位置可以使用同一个 K. K 越大，检测程序对位置变化越不敏感，对于位置变化的漏检率越高；相反，当 K 越小，检测程序对位置变化越敏感，对于位置变化的误检率越高. 在实际检测中，可将 K 值设定为可调参数，在多个位置处，分别计算该位置处的 $k(i)$；并取 $k(i)$的最大值作为给用户的推荐值 SK，当用户将 K 值设置为 SK 后，可以带着手机进行位置稳定与否的测试，并根据测试结果对 K 值进行微调.

位置稳定的 RSSI 序列具有以下特点：

开始点：$[|k(i)|\leq K]-ws(+1)$

结束点：$[|k(i)|>K]-ws/2$

方括号表示第 1 个满足条件的 i，由于 $k(i)=\sigma_i-\sigma_{i-1}$，$\sigma_i$是第 $i(ws\leq i\leq n)$个窗口的方差，且 $W_i=\{r_{i-ws+1}, r_{i-ws+2}, \cdots, r_{i-1}, r_i\}$，所以当 $|k(i)|\leq K$ 时，σ_{i-1}已经是稳定数据，即第 $i-ws$ 个 RSSI 已经稳定(当 $i-ws=0$ 时，从第 $i-ws+1$ 开始). 而只要当 $|k(i)|>K$ 时，说明第 i 个 RSSI 就不再稳定，但是计算方差时用到了均值，而均值具有延迟性，所以为了确保稳定 RSSI 序列的正确性，得到的结束点再向前减去半个窗口大小. 由于选取有效 RSSI 序列时以大于等于窗口大小的数据片段为有效序列，所以去掉长度小于窗口大小的片段.

6.2.2 有效参考 AP 的选取

要提高多位置协同检测的准确性，就需要提高定位的准确性. 由于室内环境中无线信号传输的复杂性，导致 AP 信号不稳定. 现在的网络环境中，一个位置往往可以检测到多个 AP，要提高定位的准确性，就需要从多个 AP 中选取出信号稳定且和目标 AP 相关性好的 AP 作为参考 AP，此处的相关性是指当手机与目标 AP 之间的信号距离发生变化时手机与参考 AP 的信号距离也发生变化，当与目标 AP 的信号距离不变时其与参考 AP 的信号距离也不变，所以目标 AP 与参考 AP 之间的方差增量曲线的波动应该呈现一致性.

由于收集 RSSI 值时可能出现某次未能扫描到某个 AP 的 RSSI，或者是因为手机对不同 AP 的 RSSI 变化的敏感性不同造成方差增量曲线在时间轴上不一致. 如图 13 所示，两条曲线分别为两个 AP 的方差增量序列，NISL 为目标 AP，WSN 为一个待选参考 AP，这两个 AP 在位置稳定的时候方差增量均较平稳，在移动过程中他们的方差增量序列均出现较大幅度的波动，虽然他们的波动幅度相差较大，且在时间轴上他们的波动未能完全同步，但整体的相似度最高，所以不能完全按照横坐标来一对一计算两条曲线的距离.

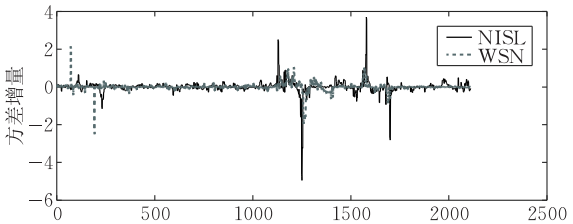


图 13 目标 AP 与参考 AP 的方差增量图

为此，我们采用动态时间规整[19] (Dynamic Time Warping，DTW)算法来计算距离并确定参考 AP 的有效性. DTW 是把时间规整和距离测度计算结合起来的一种非线性规整技术，使用某种指定属性的非线性规整函数对时间轴上的波动近似建模，通过歪曲其中一个模式的时间轴使之跟另一个模式达到最大程度的重叠，从而消除两个时空模式之间的时间差别. 如图 14 所示，图 14(a)不使用动态时

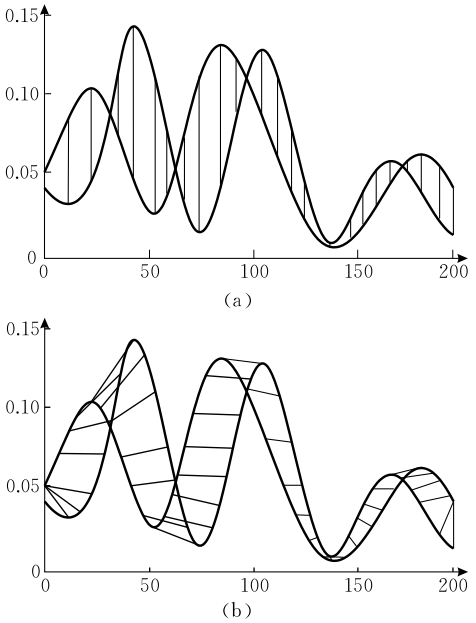


图 14 动态时间规整(DTW)

间规整计算距离，图 14(b)使用动态时间规整计算距离，图 14(b)可以使得计算距离时达到最小失真.

在选取有效参考 AP 时，对于每个 AP，储存它的大量方差增量值，并通过 DTW 算法计算每个备选参考 AP 与目标 AP 的方差增量序列之间的距离. 得到所有备选参考 AP 与目标 AP 的距离后，根据距离对备选参考 AP 排序，距离越小，有效性越好. 由三角定位可知，要定位平面上一点至少需要 3 个参考 AP，所以从备选参考 AP 中至少选择最有效的 3 个 AP 作为参考 AP. 为了防止某个参考 AP 失效，比如突然下线或者位置移动，所以我们从备选列表中选 4 个参考 AP.

6.3　RSSI 指纹库建立

得到参考 AP 并切分出有效 RSSI 序列后就可以用来生成 RSSI 指纹库(RSSI-MAP)，从图 9 所示的多位置协同检测的框架图中可以看到，我们需要在训练阶段建立 RSSI 指纹库，并在检测过程中将得到的 RSSI 数据与指纹库中的数据进行匹配，为此我们设计了如表 3 的 RSSI-MAP 结构.

表 3　RSSI-MAP 结构

位置	参考 AP	目标 AP
1	$R_1=(r_{1,1},r_{2,1},\cdots,r_{L,1})$	$R'_1=r_{0,1}$
2	$R_2=(r_{1,2},r_{2,2},\cdots,r_{L,2})$	$R'_2=r_{0,2}$
…	…	…
J	$R_J=(r_{1,J},r_{2,J},\cdots,r_{L,J})$	$R'_J=r_{0,J}$

其中，$R_J=(r_{1,J},r_{2,J},\cdots,r_{L,J})$表示 RSSI-MAP 中位置 J 处来自 L 个参考 AP 的 RSSI 的指纹信息，$R'_J=r_{0,J}$表示位置 J 处来自目标 AP 的 RSSI 指纹信息. 每个 AP 的指纹信息 r 用如下结构描述：$r(\overline{rssi},var,len)$，该三元组中的项分别表示 RSSI 序列的均值、方差、长度，其中参考 AP 的均值为整个 RSSI 序列的均值，而目标 AP 的均值为在位置 J 处的最大均值. 由第 4 节可知在同一位置同一 AP 的 RSSI 成近似正态分布，所以使用均值和方差即可描述 AP 的在某个位置处的 RSSI 指纹，RSSI 序列长度用来做后续的指纹库的动态更新.

6.4　手机位置确定

要通过比较目标 AP 的 RSSI 序列是否满足指纹库中目标 AP 的 RSSI 指纹，并判定其合法性，需先确保比较的 RSSI 数据来自同一个位置，所以需要确定手机的位置.

用 $R_T=(r_{1,T},r_{2,T},\cdots,r_{L,T})$表示在位置 T 处检测得到的参考 AP 的 RSSI 指纹信息，并用 $R'_T=r'_{0,T}$ 表示位置 T 处检测得到的目标 AP 的 RSSI 指纹信息. 位置匹配用最近邻算法[20]，R_T 和 R_J 之间的距离表示为 $Dist(R_T,R_J)$，其计算方法如式(4)所示

$$Dist(R_T,R_J)=\sqrt{\sum_{i=1}^{L}(\overline{rssi_{i,T}}-\overline{rssi_{i,J}})^2} \tag{4}$$

式中：$\overline{rssi_{i,T}}$为检测时参考 AP 的 RSSI 均值，$\overline{rssi_{i,J}}$为指纹库中参考 AP 的 RSSI 序列均值，上述均值不使用窗口算法，即计算完整序列的均值. 位置 j 为 T 与 RSSI-MAP 中所有位置距离最近的位置. 当存在 3 个以上参考 AP 时即可实现完全定位，即指纹和位置一一映射. 式(4)中 $Dist(R_T,R_J)$和参考 AP 的数量 L 有关，为降低不同位置参考 AP 数量不同对 $Dist_T$造成的影响，故使用该距离除以 L，即

$$Dist_T=\min\left[\frac{Dist(R_T,R_J)}{L}\right] \tag{5}$$

当 $L\geq 3$ 时，取前 3 个参考 AP 的指纹代入式(4)与式(5)计算距离并定位. 当多个位置与 T 的 $Dist(R_T,R_J)$相等时，加入第 4 个参考 AP 并计算新的 $Dist_T$.

当 $L=2$ 时，不能实现 RSSI 指纹和位置的一一映射，但是理论上也只有 2 个位置无法正确区分，此时继续用 $L\geq 3$ 时的方法定位，若出现多个距离相同的位置，则选择距离目标 AP 更近的那个位置.

当 $L=1$ 时，为提高定位精确度，在计算位置 T 和位置 J 之间的 RSSI 相似度时引入方差. 当两个位置距离 AP 的信号距离相等，即均值相同时，只用均值无法区分这两个位置，但这两个位置和 AP 之间的障碍物对信号的干扰不一定相同，所以方差也不一定相同. 由前文可知，同一位置处来自同一 AP 的 RSSI 呈近似正态分布，即 $r(\overline{rssi},var,len)$所代表的 RSSI 序列近似满足如式(6)的概率分布

$$P(rssi)=\frac{1}{\sqrt{2\pi}\cdot\sigma}\cdot e^{\frac{(rssi-\mu)^2}{2\cdot\sigma^2}} \tag{6}$$

其中，$\sigma=var$，$\mu=\overline{rssi}$.

在信息论中，KL 散度[21-22] (Kullback-Leibler divergence)可用来描述两个概率分布 P 和 Q 的差异，$D_{KL}(P\|Q)$表示当用理论分布 Q 来拟合真实分布 P 时，产生的信息损耗. 所以在这里可使用 KL 散度计算位置 T 和 J 的 RSSI 概率分布之间的距离. 对一个离散随机变量的两个概率分布 P 和 Q 来说，KL 散度定义如式(7)所示

$$D_{KL}(P\|Q)=\sum P(i)\cdot\ln\frac{P(i)}{Q(i)} \tag{7}$$

将式(6)代入式(7)可得到式(8)所示的距离公式

$$Dist(R_T,R_J)=D_{KL}(R_T\|R_J)=\sum_{rssi=-100}^{0}\frac{P(rssi)}{2}\cdot\left[\frac{(rssi-u_1)^2}{\sigma_1^2}-\frac{(rssi-u_2)^2}{\sigma_2^2}\right] \quad (8)$$

其中，$\sigma_1=var_{L,T}$，$\mu_1=\overline{rssi_{L,T}}$，$\sigma_2=var_{L,J}$，$\mu_2=\overline{rssi_{L,J}}$，$P(rssi)=\frac{1}{\sqrt{2\pi}\cdot\sigma_1}\cdot e^{\frac{(rssi-\mu_1)^2}{2\cdot\sigma_1^2}}$.

使用上述距离计算公式求得距离后，同样使用最近邻算法在 RSSI-MAP 中找到对应的位置 J.

6.5 合法性判别

在得到位置 J 后，查询 RSSI-MAP 并从中获取位置 J 处目标 AP 的 RSSI 的最大均值 $\max(\overline{rssi})$，实际检测的目标 AP 的均值为 $\overline{rssi}$，两者的差值 $Diff_T=\overline{rssi}-\max(\overline{rssi})$. RSSI-MAP 中参考位置的最小距离为 M，设置为检测器从位置 A 移动到位置 B 使得目标 AP 的最大均值差值大于等于 1(可分辨)时，A 与 B 之间的 $Dist$. 检测时，若 $Dist_T\leq M$ 且 $Diff_T\leq 0$，则判定当前状态安全，无伪 AP 存在；若 $Dist_T\leq M$ 且 $Diff_T>0$，则判定出现伪 AP；若 $Dist_T>M$，则更新指纹库，更新算法详见 6.6 节. 这里的 $Dist_T$ 是欧式距离，即使是通过 K-L 散度计算得到的最近位置，在进行合法性判断时仍需重新以欧式距离计算 $Dist_T$.

6.6 指纹库的动态更新

RSSI 指纹库的动态更新包括两个部分：一是新指纹的添加；二是现有指纹的更新.

新指纹添加是因为 RSSI 指纹库在训练阶段由于各种原因导致指纹库中的指纹数据不能完全覆盖分割粒度为 M 的所有空间子区域，所以需要在后期不断地完善指纹库.

现有指纹的更新是因为环境变化造成的，主要包括参考 AP 存活状态变化、备选参考 AP 与目标 AP 的相关性发生变化、参考 AP 位置发生变化等，此时我们需要在检测阶段，动态更新指纹库中已经存在的指纹信息

$$[R_J(r_{1,J},r_{2,J},\cdots,r_{L,J}),R'_J(r_{0,J})].$$

在 6.2.2 节中计算 $Dist_T$ 时，若存在 4 个有效参考 AP 为 AP_1,AP_2,AP_3,AP_4，它们的有效性 $E_1>E_2>E_3>E_4$，则 $Dist_T=Dist_T(AP_1,AP_2,AP_3)$，对应的位置为 J.

当 $Dist_T>M$ 时，重新计算

$$\begin{cases}Dist_{T3}=Dist_T(AP_1,AP_2,AP_4)\\Dist_{T2}=Dist_T(AP_1,AP_3,AP_4)\\Dist_{T1}=Dist_T(AP_2,AP_3,AP_4)\end{cases}.$$

若 $Dist_{Ti}\leq M$，则使用 $r_{i,T}$ 代替 RSSI-MAP 中的 $r_{i,J}$ 以实现现有指纹的更新，若 $Dist_{Ti}$ 全部大于 M，则将 (R_T,R'_T) 加入 RSSI-MAP 中实现新指纹的添加.

当 $Dist_T\leq M$ 时，若参考 AP 的指纹 $r_{i,t}.len\geq r_{i,j}.len$，则使用 $r_{i,T}$ 代替 RSSI-MAP 中的 $r_{i,J}$ 以实现现有指纹的更新.

7 实验及评估

为了验证基于 RSSI 的 Evil-Twin AP 检测法的可行性与有效性，我们在 Android 系统上分别实现了单一位置监测系统和多位置协同监测系统并进行相关的实验.

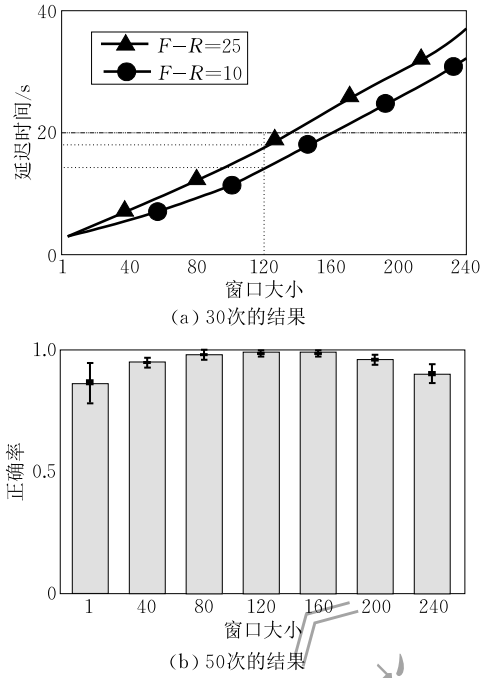
7.1 单一位置检测实验及评估

7.1.1 滑动窗口大小对检测的影响

由于均值等于窗口内的 RSSI 数据总和除以滑动窗口大小，所以窗口越大，检测的延迟性越高，且漏检率越高；相反，窗口越小，检测的延迟性越低，但误检率越高. 同时，伪 AP 与真实 AP 的 RSSI 均值差越大，伪 AP 对计算均值时窗口内数据总和的影响也越大，延迟时间越小. 在实际检测中，窗口大小可作为可调节参数，对安全性要求越高时，可将窗口调节至越小，反之则将其调大.

为验证窗口大小对延迟的影响，我们设置如下实验：伪 AP 与真实 AP 的 RSSI 均值差分别为 25 和 10，即 $F-R=25$ 和 $F-R=10$；窗口大小依次为 1,40,80,120,160,200,240；每次检测的安全阈值为检测器收集 30 分钟 RSSI 得到的最大均值，使用均值差和窗口大小共组合出 14 组实验，每组实验进行 30 次，并取平均值，最终得到如图 15(a)的结果. 可以看到，窗口越大，延迟越高；伪 AP 与真实 AP 的 RSSI 均值差越大，延迟越小，当窗口大小为 120 时，平均延迟小于 20 s.

为验证窗口大小对正确率的影响，我们在 $F-R=10$ 的情况下，设置窗口大小依次为 1,40,80,120,160,200,240；在检测程序运行 10 min 后，打开伪 AP 并让其运行 3 min 后关闭 3 min，由于均值从异常状态恢复到正常需要一定的延迟时间，所以每 3 min 内度过延迟时间后再出现错检或漏检，则认为检测错误；如此反复 50 次，最终得到如图 15(b)的结果，窗口大小等于 80,120,160 时正确率超过 98%. 窗口过小时，因较高的误检率而导致正确率较低；当窗口过大时，因漏检率较高而导致正确率较低.



(a) 30次的结果

(b) 50次的结果

图 15　窗口大小对延迟和正确率的影响

当窗口过小时易受噪声数据的干扰，误差较大；当窗口过大时延迟较高，且计算量大. 根据 Figuera 等人[23]的理论分析是实际实验，将实验中数据收集速率为每秒两次，当窗口大小为 120 时，收集 120 条数据只需 1 min，从窗口内无伪 AP 数据到窗口内数据全部来自伪 AP 时，检测延迟达到最高，即 1 min，而在 1 min 之内攻击者很难完成一次完整的攻击；且窗口为 120 时，准确率超过 98%.

7.1.2　阈值大小对检测的影响

为验证阈值对检测结果的影响，我们设置如下实验：窗口大小为 120，$F-R=25$ 和 $F-R=10$ 时，分别以真实 AP 在 1 h 内的均值最大值 R_{max} 以及 $R_{max}-2$，$R_{max}+2$，$R_{max}+4$，$R_{max}+8$ 作为阈值进行伪 AP 检测，共组合出 10 组实验. 每组实验中，在检测程序运行 10 min 后，打开伪 AP 并让其运行 3 min 后关闭 3 min，如此反复 50 次，得到如图 16 所示的结果. 实验结果显示，安全阈值取 R_{max} 时，$F-R=25$ 和 10 的正确率均达到 96%，在 $R_{max}+2$ 时，$F-R=25$ 的正确率达到 100%，$F-R=10$ 的正确率达到 99%.

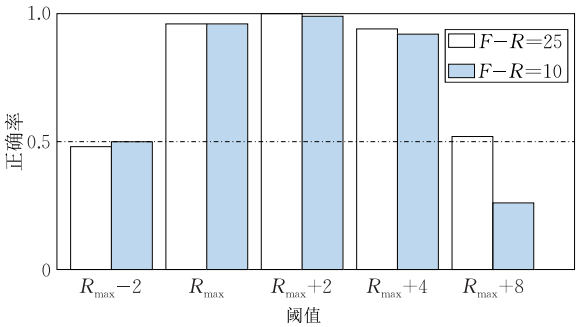
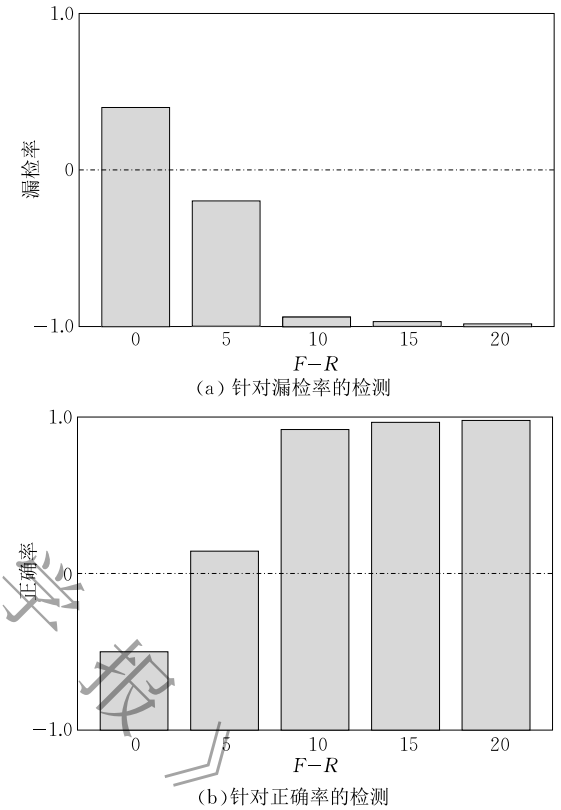


图 16　安全阈值对检测正确率的影响

7.1.3　距离对检测的影响

为验证距离对检测结果的影响，我们分别在 $F-R=0,5,10,15,20$ 处，以 R_{max} 为阈值进行检测，共 5 组实验. 每组实验中，在检测程序运行 10 min 后，打开伪 AP 并让其运行 3 min 后关闭 3 min，如此反复 50 次，得到如图 17 所示的结果，当 $F-R\geq10$ 时，正确率均超过 96%，漏检率小于 3%.



(a) 针对漏检率的检测

(b)针对正确率的检测

图 17　距离对检测结果的影响

7.2　多位置协同检测实验及评估

7.2.1　方差增量法有效性验证

为验证方差增量法切分有效 RSSI 的有效性，我们以 6.2.1 节中的数据为例，窗口大小设置为 120，K 取推荐值 $SK=4$，然后按照 6.2.1 节中的方差增量法分割 RSSI 序列，得到如表 4 所示的片段. 然后去掉长度小于 120 的片段，得到 S_1 和 S_10 两个有效 RSSI 序列片段，总长度为 2598，原始数据序列中有效片段的长度为 2605，算法切分正确率为 99.7%.

7.2.2　DTW 算法选取有效 AP 的有效性验证

为验证 DTW 算法可以有效选取有效 AP，我们打开检测软件让其采集可以扫描到的所有 AP 的 RSSI，分别在 3 个不同位置各停留 15 min，并在不同位置转换时以约 1.5 m/s 的速度移动，共扫描到 28 个

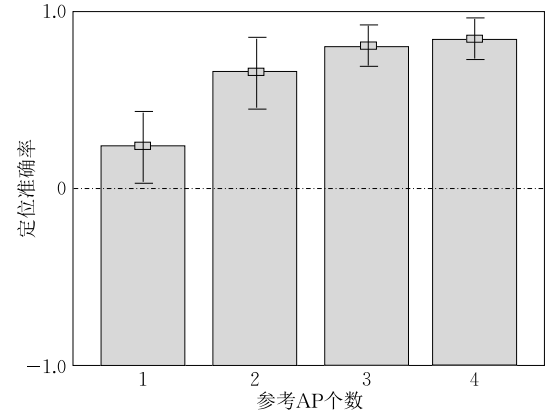
表 4 初次分 RSSI 片段

标志	范围	长度	范围	均值
S_1	**1～1422**	**1422**	**[−52, −35]**	**−45.15**
S_2	1366～1431	66	[−44, −39]	−42.50
S_3	1424～1502	79	[−84, −38]	−50.04
S_4	1489～1560	72	[−100, −64]	−91.17
S_5	1507～1569	63	[−100, −87]	−95.95
S_6	1552～1620	69	[−100, −72]	−90.91
S_7	1609～1718	110	[−76, −38]	−56.54
S_8	1660～1726	67	[−75, −40]	−56.68
S_9	1669～1731	63	[−75, −40]	−59.95
S_10	**1861～2848**	**1168**	**[−90, −56]**	**−66.37**

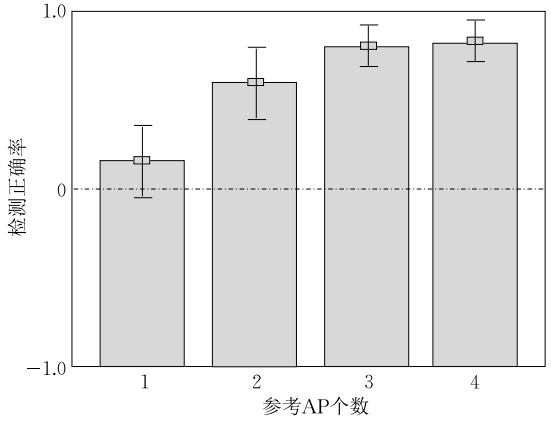
AP，包括一个目标 AP 和 27 个待选参考 AP. 然后分别使用 DTW 算法计算这 27 个 AP 的方差增量序列和目标 AP 的方差增量序列的距离，最终成功找出了 4 个最相关且最稳定的参考 AP.

7.2.3 定位算法验证

我们在 100 m² 的空间内，约每 4 m² 采集一次数据，共 25 组数据. 在检测阶段，在每个位置停留 5 min，不同位置之间以 1.5 m/s 的速度变换，并分别以 7.2.2 节中找到的 4 个参考 AP 中的前 4 个、前 3 个、前 2 个作为参考 AP，用欧式距离进行定位；并用第 1 个参考 AP 验证使用 KL 散度计算距离并定位，得到如图 18(a)所示结果. 只有 1 个参考 AP 时，定位准确率仅为 62%；有 2 个参考 AP 时，定位准确率为 83%；当参考 AP 多于 3 个时，定位准确率高于 90%.



(a) 第一组结果



(b) 第二组结果

图 18 参考 AP 对检测结果的影响

7.2.4 多位置协同检测有效性验证

我们在笔记本电脑上使用 hostapd 实现伪 AP，并在 Android 上实现该检测系统. 特征收集阶段，在 100 m² 的空间内，约每 4 m² 采集一次数据，每次采集时长为 30 min，共 25 组数据，窗口大小设置为 120，所有位置处的安全阈值都取该处的 RSSI 均值最大值. 检测阶段，在每个位置停留 5 min，不同位置之间以 1.5 m/s 的速度变换，窗口大小为 120，实验共进行 200 次，100 次开启伪 AP，100 次关闭伪 AP. 开启伪 AP 时，若有任一位置检测出伪 AP，则检测成功，若所有位置都未检测出伪 AP，则检测失败；关闭伪 AP 时，若有任一位置检测出伪 AP，则检测失败，若所有位置都未检测出伪 AP，则检测成功. 最终得到如图 18(b)所示结果，当只有一个参考 AP 时，检测正确率仅为 58%，当有两个参考 AP 时，正确率达到 80%，当参考 AP 多于 3 个时，检测正确率超过 90%.

8 结 论

本文提出智能家居中基于 RSSI 的伪 AP 检测方法，其本质是检测 AP 的位置是否合法. 因为 AP 的硬件特征和流量特征可被伪造，但位置无法被伪造，所以该方法可以有效应对硬件特征和流量特征检测法被绕过的情况，最后通过实验证明该方法可以很好的降低检测延迟和提高检测准确率.

该方法根据检测位置固定与否分为单一固定位置检测和多位置协同检测两种方案，单一固定位置检测方案实现简单，计算量小，但是检测器的部署位置会直接影响检测结果，部署位置不恰当时漏检率较高. 多位置协同检测需要手机参与检测，方案实现较复杂，但可以有效解决单一固定位置漏检的问题. 它通过 Wi-Fi 室内定位的方法将多位置问题转化为多个单一固定位置检测问题. 在实现有效 RSSI 选取时提出了方差增量法，将两个不具有普适性的参数转化为一个普适性较好的参数，并成功分割出有效 RSSI 序列；在选取有效参考 AP 时，借助 DTW 算法成功选择出与目标 AP 相关性好且信号稳定的参考 AP.

参 考 文 献

[1] Bratus S, Cornelius C, Kotz D, et al. Active behavioral

fingerprinting of wireless devices//Proceedings of the 1st ACM Conference on Wireless Network Security. Virginia, USA, 2008: 56-61

[2] Franklin J, McCoy D, Tabriz P, et al. Passive data link layer 802.11 wireless device driver fingerprinting//Proceedings of the 15th Conference on Usenix Security Symposium. Vancouver, Canada, 2006: 167-178

[3] Desmond L C C, Yuan C C, Pheng T C, et al. Identifying unique devices through wireless fingerprinting//Proceedings of the 1st ACM Conference on Wireless Network Security. Virginia, USA, 2008: 46-55

[4] Neumann C, Heen O, Onno S. An empirical study of passive 802.11 device fingerprinting//Proceedings of the Distributed Computing Systems Workshops (ICDCSW). Macau, China, 2012: 593-602

[5] Beyah R, Kangude S, Yu G, et al. Rogue access point detection using temporal traffic characteristics//Proceedings of the Global Telecommunications Conference. Dallas, USA, 2004, 4: 2271-2275

[6] Song Y, Yang C, Gu G. Who is peeping at your passwords at Starbucks?To catch an evil twin access point//Proceedings of 2010 IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Chicago, USA, 2010: 323-332

[7] Ma L, Teymorian A Y, Cheng X. A hybrid rogue access point protection framework for commodity Wi-Fi networks//Proceedings of the 27th IEEE International Conference on Computer Communications. Phoenix, Arizona, 2008: 1220-1228

[8] Wei W, Suh K, Wang B, et al. Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs//Proceedings of the 7th Special Interest Group on Data Communication Conference on Internet Measurement. San Diego, USA, 2007: 365-378

[9] Han H, Sheng B, Tan C C, et al. A timing-based scheme for rogue AP detection. IEEE Transactions on Parallel and Distributed Systems, 2011, 22(11): 1912-1925

[10] Mano C D, Blaich A, Liao Q, et al. RIPPS: Rogue identifying packet payload slicer detecting unauthorized wireless hosts through network traffic conditioning. ACM Transactions on Information and System Security, 2008, 11(2): 2

[11] Qu G, Nefcy M M. RAPiD: An indirect rogue access points detection system//Proceedings of the 29th Performance Computing and Communications Conference (IPCCC). New Mexico, USA, 2010: 9-16

[12] Lee J W, Lee S Y, Moon J S. Detecting rogue AP using k-SVM method. Journal of the Korea Institute of Information Security and Cryptology, 2014, 24(1): 87-95

[13] Han H, Xu F, Tan C C, et al. Defending against vehicular rogue APs//Proceedings of the IEEE International Conference on Computer Communications. Shanghai, China, 2011: 1665-1673

[14] Lim K, Shao J, Lee J, et al. Scheme of rogue AP detection in managed WLAN based on AP's location. Journal of Measurement Science and Instrumentation, 2012, 3(4): 370-373

[15] Cai M, Wu Z, Zhang J. Research and prevention of rogue AP based MitM in wireless network//Proceedings of the 9th International Conference on P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC). Guangdong, China, 2014: 538-542

[16] LAN/MAN Committee of the IEEE Computer Society. IEEE Standard for Information exchange between system-LANs and MANs-Specific requirements-Part11: WLAN MAC and PHY Specifications. IEEE Std, 2007, 802: 11p

[17] Chen Wei, Gu Yang, Li Chen-Yang, et al. Wireless rogue access point attack and detection research. Journal of Wuhan University (Natural Science Edition), 2014, 60(1): 13-23 (in Chinese)
(陈伟，顾杨，李晨阳等. 无线钓鱼接入点攻击与检测技术研究综述. 武汉大学学报(理学版), 2014, 60(1): 13-23)

[18] Bellardo J, Savage S. 802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions//Proceedings of the USENIX Security Symposium. Washington, USA, 2003: 15-28

[19] Wang J, Katabi D. Dude, where's my card?: RFID positioning that works with multipath and non-line of sight. ACM Interest Group on Data Communication Review, 2013, 43(4): 51-62

[20] Fang Y, Deng Z, Xue C, et al. Application of an improved K nearest neighbor algorithm in WiFi indoor positioning//Proceedings of the China Satellite Navigation Conference (CSNC) 2015. Xi'an, China, 2015: 517-524

[21] Kullback S, Leibler R A. On information and sufficiency. The Annals of Mathematical Statistics, 1951, 22(1): 79-86

[22] Baez J C, Fritz T. A Bayesian characterization of relative entropy. Theory and Applications of Categories, 2014, 29(16): 422-456

[23] Figuera C, Rojo-Álvarez J L, Mora-Jiménez I, et al. Time-space sampling and mobile device calibration for wifi indoor location systems. IEEE Transactions on Mobile Computing, 2011, 10(7): 913-926

FANG Ding-Yi, born in 1959, Ph.D., professor, Ph.D. supervisor. His research interests include cyber and information security, software security and protection, key technology of WSN.

QI Sheng-De, born in 1990, M.S. His main research interests include software security and IoT security.

TANG Zhan-Yong, born in 1979, Ph.D., associate professor. His main research interests include software security and protection, wireless sensor network security.

CHEN Xiao-Jiang, born in 1973, Ph.D., professor. His main research interests include wireless sensor network,

software security and protection.

GU Yuan-Xiang, born in 1951, professor, chief architect. His main research interests include computer system security and protection, software security and protection.

Background

This paper is related to the wireless network security. In recent years, Evil-Twin attack has been paid more attention in wireless network. Thus, the Evil-Twin AP detection becomes a focus of wireless network security. Existing Evil-Twin AP detection techniques are mainly based on the fingerprint of NIC (Network Interface Card) and the traffic features. Attackers can forge those features to escape from Evil-Twin AP detection, but they cannot forge the location of the real AP. Therefore, we propose a novel detection method based on RSSI in smart home. Someone has used the RSSI to detect the vehicular rogue AP with GPS, but the GPS is disabled for indoor location. Thus, we combine the Wi-Fi indoor location and RSSI similarity computing to perform the Evil-Twin AP detection in smart home. It aims to complement existing techniques based on the hardware fingerprint and traffic features. With this method, we need not to spend too much time on detecting, and we perform the detection without network and other new professional devices.

In this work, there are two practical challenges we need to solve, the first is how to identify the effective data from a mass of RSSI. To address this problem, we propose a novel method named variance increment. The second is how to select the effective reference AP for location, we introduce DTW to solve it.

This work is supported by the International S&T Cooperation and Communication Plan (2015KW-003), the National Natural Science Foundation of China (61672427, 61272461, 61202393), the Industrialization cultivation project of Shaanxi Provincial Education Department (2013JC07).