

基于 Shadowing 模型的无线入侵主机物理定位研究

付 雄¹, 彭 冰²

(1 武汉大学 法学院, 湖北 武汉 430072; 2 华中科技大学 计算机科学与技术学院, 湖北 武汉 430074)

摘 要: 为了在室内无线局域网环境中及时准确地定位非法入侵主机物理位置, 以无线信号强度衰减过程的 Shadowing 传播模型为基础, 研究了在一定的范围内如何合理地布置探测器, 如何根据接收到的入侵主机的信号强度进行物理定位的问题。提出的定位方法可以有效地对抗入侵主机随机更改信号发射功率对定位精度的影响。实际测试结果表明, 该方法定位误差平均约为 2.3 m, 可以满足室内环境下定位非法入侵主机的需求。

关键词: 无线局域网; 室内定位算法; 信号强度; Shadowing 模型

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)12-0004-06

Research on the Location of Wireless Invading Host Based on Shadowing Model

FU Xiong¹, PENG Bing²

(1 Law School, Wuhan University, Wuhan 430072, China; 2 College of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)

Abstract: In order to timely and accurately locate the physical position of illegal intrusion workstation in indoor WLAN environment, based on shadowing model, one of the most popular wireless signal strength reduction process, some position techniques in indoor WLAN are given in this paper. Our researches include how to layout sensors reasonably within a certain scope and how to calculate the position of intrusion workstation according to the signal strength received by the sensors. Although the intrusion workstation can randomly adjust its signal transmit power of, it is still effective to resist the accuracy reducing result by use of the introduced location method. The actual test result shows the location error is about 2.3 m on an average, which meets the requirement of intrusion workstation positioning in indoor environment.

Key words: WLAN; in-building location algorithm; signal strength; Shadowing model

1 引言

近年来, 无线局域网技术(Wireless Local Area Network, WLAN)作为一种新兴技术逐渐走向成熟, 作为有线网络的延伸, 无线局域网以其安装简单、应用灵活、移动性和频谱免费等特点, 应用越来越广泛。但是无线局域网的数据传输利用红外线或无线电波在空气中进行传播, 导致了通信过程中保密性受到严重的威胁。而且也正因为这样的性质, 使得无线网络中的信息无法被隔离保护, 因此无线网络面临了比有线网络更多的安全威胁^[1]。

无线局域网安全机制的完善不仅需要快速发展安全技术, 增强无线局域网本身的安全性, 同样也迫切需要发展相关的入侵追踪技术。对无线局域网中的违法活动进行入侵检测, 在成功检测到活动的非法主机后, 能够获取有关入侵主机的一系列信息, 如 MAC 地址、IP、物理方位等。由于无线网络用户可以在无线网络的覆盖区域内随意移动, 活动主机和用户的真实信息不再像有线网络一样固定不变并且详细地登记在案^[2]。虽然通过良好的入侵检测系统成功找出了入侵的记录, 并且锁定了入侵主机的标识信息等, 但是并不能由此找到进行违法活

动的不法分子. 由于无线网络所具有的一些特殊性质, 使得必须找出一种切实有效的追踪方法, 能够即时地针对活动中的入侵主机进行探测, 迅速锁定其真实的物理位置, 在其进行非法活动的当场进行抓获^[3].

2 无线局域网定位技术

目前, 无线局域网的定位技术可分为基于终端的定位技术和基于网络的定位技术^[4].

基于终端的定位技术主要是指移动终端 MS (Mobile Station) 根据基站 BS (Base Station) 和定位服务器 LS (Location Server) 提供的信息计算出自己所处的位置. 这种技术主要有以下三种: 全球卫星定位技术 GPS、辅助全球卫星定位技术 AGPS (Assisted GPS) 以及增强型观察时间差技术 E-OTD (Enhanced Observed Time Difference).

在室外环境下, 用户的密度比较低, GPS 利用多卫星信号的方位和距离实现室外无遮挡环境下全球位置的定位, 最高的定位精度可以达到 5 m, 因此全球定位系统 (GPS) 已被建议作为提供定位信息的方式. 但是在室内环境下或在高密度网络中, 给每一个移动用户增加 GPS 功能过于昂贵, 而且使用 GPS 获得高精度的定位效果必须使用差分技术, 难以实现^[5].

基于网络的定位技术是指定位网络根据测量数据计算出移动终端 MS 所处的位置, 主要有以下几种^[6].

(1) 基于传播时间的定位技术 TOA (Time of Arriving). 所采用的基本原理是在已知传播速度的情况下, 无线电波传播的距离与它传播的时间成正比. TOA 测量要求移动终端的发射与所有基站的接收精确同步, 并且在其发射信号中要包含发射时间标记, 以便接收基站信号到达时间确定信号所传播的距离.

(2) 基于电波传播时间差的定位技术 TDOA (Time Difference of Arrival). 通过检测信号到达不同基站的时间差, 而不是到达的绝对时间来确定移动终端的位置. TDOA 降低了时间同步要求, 还可以消除或减少在所有接收机处由于信道产生的共同误差, 因此可获得比 TOA 更高的定位精度.

(3) 基于电波入射角的定位技术 AOA (Angle of Arrival). 通过基站接收机天线阵列测出移动终端发射电波的入射角, 构成从基站到移动台的径向连线, 两根连线的交点即为待定位移动台的位置.

(4) 基于接收信号强度的定位技术 RSSI (Received Signal Strength Indicator). 研究表明, 无线信号传播存在以下规律: 接收方测得的信号强度越强, 发送方距离接收方往往越近, 反之, 发送方距离接收方越远^[7]. 因此, 通过测量接收到的信号强度建立信道衰减模型, 便可以由此推算出移动台到基站的距离.

(5) 基于信号强度指纹的定位技术. 该技术并不是利用测得的信号强度直接计算与定位目标的距离, 而是通过与采样数据比较进行分析及获得位置信息.

考虑检测无线局域网中入侵主机并进行定位的实际情况, 可以假定有入侵行为的主机出现在无线网络较为发达的城市, 并进一步假定该入侵主机的位置出现在无线 AP 较为集中的地区, 否则难于实现精确定位. 此外室内无线局域网环境下, 接入点的覆盖范围往往不超过 100 m, 无线电波的传输时延可忽略不计, 且墙壁、人体等影响信号传播的障碍物很多, 无线信号存在反射和散射现象, 因此本文将采用基于信号强度测量的定位方法来估算入侵主机的物理位置.

3 入侵主机位置的理论求解

目前无线信号强度衰减过程的传播模型主要有 Free-space 模型、Two-ray ground reflection 模型、Shadowing 模型^[8]. 前两种模型将通信的范围描绘成一个理想的环绕. 由于信号多路径传播的褪色效应, 在一定的距离接收到的能量是一个随机变量. 因此本文的研究将采用更具综合性并被广泛采用的 Shadowing 模型.

3.1 Shadowing 模型

Shadowing 模型可表述为如下形式:

$$P = P_0 + 10\beta \lg(d_0/d) + X_{\text{dB}} \quad (1)$$

式中, d_0 是参考距离; P_0 是距离为 d_0 时接收到的信号强度; d 是真实距离; X_{dB} 是遮蔽因子, 它是一个均值为 0, 均方差为 σ_{dB} 的正态随机变量; P 是接收信号强度; β 是路径损耗系数, 其典型的取值如表 1 所示. P_0, P, X_{dB} 的单位均是以 1 mW 为基准功率分贝, 即 dBm.

值得注意的是, 在式 (1) 中 X_{dB} 为与传播距离无关的随机变量, 相同的传播距离, 可能被测到的损耗存在较大差异, 可以通过多次测量并进行统计平滑处理减弱这种差异. 另一方面, 通过调整无线网卡的发射功率, 可以显著影响探测器的接收信号强

度. 与文献[9]类似, 为简化定位计算过程, 本文忽略随机变量 X_{ab} , 重点考虑恶意入侵主机有意或随机地调整无线网卡发射功率, 企图误导检测系统计算出的位置与攻击主机真实的物理位置存在极大的差异.

表 1 路径损耗系数 β 的参考值

环境		β
室外	自由空间	2
	有障碍物的城市空间	2.7 ~ 5
室内	直线传输	1.6 ~ 1.8
	有障碍物传输	4 ~ 6

对 Shadowing 模型进行的调整, 并且信号强度均以 mW 为单位, 可以得到 $P/P_0 = (d_0/d)^\beta$, 即: $Pd^\beta = k$ (常数), 由此可以建立探测器接收到的入侵主机的信号强度与二者距离之间的关系:

$$d = (k/P)^{\beta^{-1}} \quad (2)$$

3.2 定位方程组的建立

考虑到在各个方位上探测发现的概率均匀性, 在一定的范围内均匀布置三个参数一致的探测器 S_1, S_2, S_3 , 它们共同监听无线信道, 将收到的可疑数据包(包头含有接收信号强度)发送给与三者均相连的远程控制台. 由远程控制台实时计算并动态显示出入侵主机的物理位置. 由此可建立如图 1 所示的坐标图.

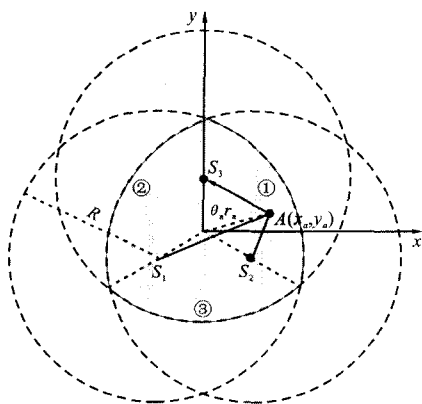


图 1 三点定位坐标图

图 1 中, R 为三个探测器的最大探测半径; l 为三个探测器距原点的距离; 最终需根据三个探测器从三个不同的方位接收到的攻击主机 A 所发出的信号强弱, 求出 A 的坐标 (x_a, y_a) 或者 (r_a, θ_a) .

显然只有当攻击主机在图 1 的灰色区域内时, 才能有效、可靠对其位置进行推算定位. 以下假定攻击主机 A 发出数据包后, 三个探测器接收到的信

号强度分别为 P_1, P_2, P_3 , 根据 S_1, S_2, S_3 的坐标和式(2)可建立以下方程组:

$$\begin{cases} \left(x + \frac{\sqrt{3}}{2}l\right)^2 + \left(y + \frac{1}{2}l\right)^2 = \overline{AS_1^2} = (k/P_1)^{2\beta^{-1}} \\ \left(x - \frac{\sqrt{3}}{2}l\right)^2 + \left(y + \frac{1}{2}l\right)^2 = \overline{AS_2^2} = (k/P_2)^{2\beta^{-1}} \\ x^2 + (y - l)^2 = \overline{AS_3^2} = (k/P_3)^{2\beta^{-1}} \end{cases} \quad (3)$$

令 $\lambda = k^{2\beta^{-1}}, \rho_1 = P_1^{-2\beta^{-1}}, \rho_2 = P_2^{-2\beta^{-1}}, \rho_3 = P_3^{-2\beta^{-1}}$, 式(3)可简化为

$$\begin{cases} \left(x + \frac{\sqrt{3}}{2}l\right)^2 + \left(y + \frac{1}{2}l\right)^2 = \lambda\rho_1 \\ \left(x - \frac{\sqrt{3}}{2}l\right)^2 + \left(y + \frac{1}{2}l\right)^2 = \lambda\rho_2 \\ x^2 + (y - l)^2 = \lambda\rho_3 \end{cases} \quad (4)$$

联立求解可得到以参量 λ 表示的入侵主机 A 的坐标:

$$x = \frac{\rho_1 - \rho_2}{2\sqrt{3}} \cdot \frac{\lambda}{l}, y = \frac{\rho_1 + \rho_2 - 2\rho_3}{6} \cdot \frac{\lambda}{l} \quad (5)$$

其中参量 λ 由下式给出:

$$[(\rho_1 - \rho_2)^2 + (\rho_2 - \rho_3)^2 + (\rho_3 - \rho_1)^2]\lambda^2 - 6(\rho_1 + \rho_2 + \rho_3)l^2\lambda + 18l^4 = 0 \quad (6)$$

3.3 求解预备知识

物理定位的前提是: 三个探测器均接收到入侵主机 A 的信号强度. 若至少有一个探测器没能探测到 A 发送的信号, 说明 A 处于可信探测区之外, 即式(3)中至少有一个 P 值为 0, 或者式(4)中至少有一个 ρ 值为无穷大. 在这种情况下将无法求解 A 的物理位置. 此外, 可以将整个可信探测区按 θ 的取值范围分为 ①, ②, ③ 三个区间. 以下以 ③ 号可信探测区间(对应于 $\frac{7\pi}{6} \leq \theta \leq \frac{11\pi}{6}$) 为例进行分析, 由三个探测器分布的均匀性可知, 其他两个区间的分析与 ③ 号区间类似.

在以 S_1 为圆心的方程 $\left(x + \frac{\sqrt{3}}{2}l\right)^2 + \left(y + \frac{1}{2}l\right)^2 = R^2$ 中, 令 $x = 0$, 可以求解出大于 0 的 y 坐标(由对称性, 此即为可信区间距原点的最大距离)从而可以得到在 ③ 号可信探测区内:

$$\begin{aligned} -(R - l) &\leq y \leq 0, \\ 0 &\leq r \leq l \left[-0.5 + \sqrt{\left(\frac{R}{l}\right)^2 - 0.75} \right] \end{aligned} \quad (7)$$

以下简记: $\rho_1 + \rho_2 + \rho_3 = a, \rho_1^2 + \rho_2^2 + \rho_3^2 = b^2, w = r/l$, 则

$$(\rho_1 - \rho_2)^2 + (\rho_2 - \rho_3)^2 + (\rho_3 - \rho_1)^2 = 3b^2 - a^2 \geq 0 \quad (8)$$

此外由式(4)可得

$$\frac{b^2}{a^2} = \frac{(x^2 + y^2 + l^2)^2 + 2l^2(x^2 + y^2)}{3(x^2 + y^2 + l^2)^2} = \frac{1}{3} \left[1 + \frac{2l^2 r^2}{(r^2 + l^2)^2} \right] \quad (9)$$

$$\frac{\rho_3}{a} = \frac{x^2 + (y-l)^2}{3(x^2 + y^2 + l^2)} = \frac{1}{3} \left[1 - \frac{2lr \sin \theta}{r^2 + l^2} \right] \quad (10)$$

根据式(7)可得出以下结果:

(1) 若 $0 < \frac{l}{R} < \frac{1}{\sqrt{3}}$, 在③号可信探测区内可能 $r > l$, 其中:

① 如果 $0 < \frac{l}{R} < \frac{1}{\sqrt{3}}$ 且 $0 \leq r \leq l$, 则 $0 \leq w \leq 1$;

② 如果 $0 < \frac{l}{R} < \frac{1}{\sqrt{3}}$ 且 $l < r \leq l \left[-0.5 + \sqrt{\left(\frac{R}{l}\right)^2 - 0.75} \right]$, 则 $1 < w \leq -0.5 + \sqrt{\left(\frac{R}{l}\right)^2 - 0.75}$;

(2) 若 $\frac{1}{\sqrt{3}} < \frac{l}{R} < 1$ 时, 在③号可信探测区内恒有 $0 \leq r \leq l$, 从而 $0 \leq w \leq 1$;

(3) 若 $\frac{l}{R} \geq 1$ 时, 整个可信探测区的面积为 0, 无法进行物理定位。

3.4 入侵主机物理位置求解

由上节中的简记符号可将关于 λ 的式(6)简化为

$$(3b^2 - a^2)\lambda^2 - 6al^2\lambda + 18l^4 = 0 \quad (11)$$

易知: $\Delta_\lambda = 36a^2l^4 - 72(3b^2 - a^2)l^4 = 108(a^2 - 2b^2)l^4$, 如果入侵主机 A 在③号可信探测区间内, 式(10)必有正实数解, 因此要求: $a^2 - 2b^2 \geq 0$, 联立式(8)可得有解的限定条件:

$$\frac{1}{3} \leq \frac{b^2}{a^2} \leq \frac{1}{2} \quad (12)$$

将式(9)代入式(12)中化简, 可以验证, 对于任意正实数 r , 式(12)均成立; 因此式(11)必然有两个实数解, 分别为

$$\lambda_1 = 3l^2 \frac{a - \sqrt{3(a^2 - 2b^2)}}{3b^2 - a^2} \quad (13)$$

$$\lambda_2 = 3l^2 \frac{a + \sqrt{3(a^2 - 2b^2)}}{3b^2 - a^2}$$

容易验证, 以上的两个解均为非负数, 然而当

攻击机 A 处于可信探测区中时, 只有一个确切的物理位置. 因此两个解中一个为正确解, 另一个解需要舍去。

显然, 如果选择合适的 l , 必然会使得式(11)的两个解代入式(5)后求得的两个点的坐标, 一个点在可信探测区之内, 另一个点在可信探测区之外. 位于可信探测区之外点所对应的 λ 正是式(13)需要舍去的解. 也就是说由 λ_1 确定的点距 S_3 的距离必须不大于 R (位于③号可信探测区间内), 而由 λ_2 确定的点距 S_3 的距离必须大于 R (位于③号可信探测区外), 因此:

$$\lambda_1 \rho_3 \leq R^2, \lambda_2 \rho_3 > R^2 \quad (14)$$

将式(13)代入式(14)中, 并由式(9), 式(10)可得

$$\begin{cases} \frac{l}{R} \leq \sqrt{\frac{2w^2}{[(w^2+1)-|w^2-1|](w^2-2w\sin\theta+1)}} \\ \frac{l}{R} > \sqrt{\frac{2w^2}{[(w^2+1)+|w^2-1|](w^2-2w\sin\theta+1)}} \end{cases} \quad (15)$$

由第 3.3 节中的分析可知:

(1) 若 $0 \leq w \leq 1$, 则式(15)简化为

$$\begin{cases} l/R \leq (w^2 - 2w\sin\theta + 1)^{-1/2} \\ l/R > w(w^2 - 2w\sin\theta + 1)^{-1/2} \end{cases} \quad (16)$$

(2) 若 $1 < w \leq -0.5 + \sqrt{\left(\frac{R}{l}\right)^2 - 0.75}$, 则式

(15) 简化为

$$\begin{cases} l/R \leq w(w^2 - 2w\sin\theta + 1)^{-1/2} \\ l/R > w(w^2 - 2w\sin\theta + 1)^{-1/2} \end{cases} \quad (17)$$

综合上述两种情况, 可得到 l/R 取值范围如 2 所示, 图中阴影部分区域即为在最保守的情况下, l/R 的合理区域。

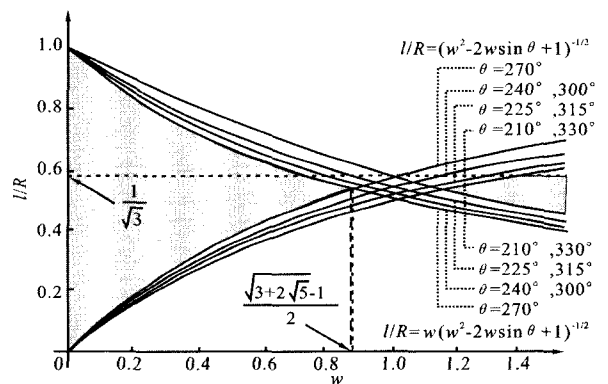


图 2 l/R 的取值范围

为了任意选取 $\theta \in \left[\frac{7\pi}{6}, \frac{11\pi}{6}\right]$, 由式(13)的两个解所确定的两个攻击点只有一个在③号可信探

测区内,又要使得③号可信探测区间的最大探测半径尽可能的大,可以通过求解下式:

$$\frac{1}{\sqrt{w^2 + 2w + 1}} = \frac{w}{\sqrt{w^2 + w + 1}} \quad (18)$$

求得可信区间最大探测半径与 l 的比值为

$$w_{\max} = \frac{r}{l} = \frac{\sqrt{3 + 2\sqrt{5}} - 1}{2} \quad (19)$$

然后反代至式(18)的左边(或右边)可求得最佳的 l 值与 R 之比为

$$\frac{l}{R} = \frac{2}{\sqrt{3 + 2\sqrt{5}} + 1} \quad (20)$$

显然 l 越大,可信探测区域的范围就越小;反之 l 越小,三个探测器靠得越近,虽然可信探测区域的范围有所增大,但不仅定位的精度不够高,而且更容易受入侵主机有意添加的干扰.因此在探测器的最大探测半径 R 给定后,选择 l 时除了要考虑满足 λ 的解只有一个在可信区间内,还要综合考虑可信探测区域的大小和定位精度的要求而定.

根据上述分析结果选择合适的 l 布置探测器.最终选择式(13)中较优的 λ 的解,代入式(5)中即可求出入侵主机的物理位置.虽然本文忽略了遮蔽因子 X_{db} ,但可以根据大量接收到的关于入侵主机的数据报文信息而求出的各个位置进行统计处理,即便入侵主机实施信号干扰也最终能推测出入侵主机的位置.

4 实验测试与结果分析

选取一幢 H 型大楼左半部分的第一层为实验场地,部署 802.11b 无线局域网,测试面积约为 $1\,600\text{ m}^2$ ($40\text{ m} \times 40\text{ m}$),为在尽可能大的面积上保证每个移动用户可能出现的位置都有探测器能检测到信号,按照对称的方式放置了 3 个装有 Netgear 511T 网卡(芯片组为 Atheros AR5005GS)的笔记本作为探测器.以一台 PC 机作为控制台进行定位计算,探测器与控制台之间的通信通过 X5 型类双绞线进行.以一台内置无线上网功能的笔记本作为入侵主机,该机可在待测范围内任意移动,并开 30 个 ping 控制台的进程.对入侵主机每 5 秒钟进行一次无线网卡发包功率的随机调整.在待测区间以 5 m 步距测量路径损耗系数然后平均化,最终确定 $\beta=5.17$.

获取测试数据时,为尽量减小信号干扰带来的影响,采用概率统计法计算信号强度,平均每收到 500 个报文进行一次均值计算.以 10 次均值计算出

的物理位置再平均后作为某一次测试最终推算的入侵主机位置.测试结果如图 3、图 4 所示.

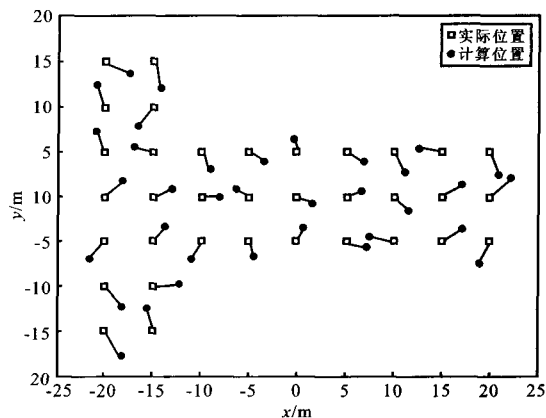


图 3 测试点实际位置与计算位置布局

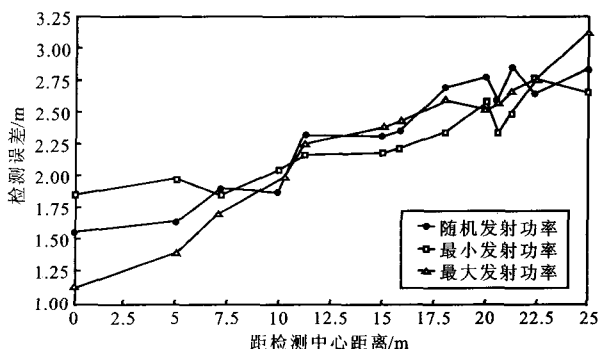


图 4 测试点计算位置误差

实验结果表明,无论入侵主机的信号发射功率处于最大值还是最小值以及随机任意选取发射功率值,本文提出的定位入侵主机位置的算法其误差范围约为 $1.5 \sim 3\text{ m}$ (实测三种情况下综合平均误差约为 2.29 m),能够较精确地定位入侵主机所属的房间.此外,由图 4 可见,在以检测中心为圆心,半径 15 m 左右的范围,定位误差较少,随着入侵主机偏离中心距离的增大,定位误差有一定程度的扩大.这主要是因为三个探测器安置在三个房间的角落,当入侵主机距其中某个探测器较远而距另两个探测器较近(处于同一房间)时,信号的反射和散射效应使得路径损耗系数 β 与实测所取的平均 β 值偏离较大造成.因此,本文的算法尤其适用于入侵主机在三个 Sensor 中间位置的场合.

5 结束语

考虑到入侵主机为了抵抗入侵检测系统的定位计算而随机调整无线网卡发射功率,本文以 Shadowing 模型为基础,详细研究了探测器的最佳布置和入侵主机物理位置的计算问题.实验结果表明在

三个探测器共同作用的可信探测区,本文的算法精度较好地满足了对入侵主机的房间级定位需求,为无线局域网的安全防护提供了可借鉴的思路。

参考文献:

- [1] Rappaport T S. Wireless communications: principles and practice[M]. New Jersey: Prentice Hall Publications, 2002.
- [2] Youssef M, Agrawala A, Shankar A U. WLAN location determination via clustering and probability distributions[C]// IEEE International Conference on Pervasive Computing and Communications, PerCom 2003. Fort Worth, Texas: IEEE, 2003.
- [3] Roos T, Myllymaki P, Tirri H, et al. A probabilistic approach to WLAN user location estimation[J]. International Journal of Wireless Information Networks, 2002, 9(3): 155—164.
- [4] Chen G, Kotz D. A survey of context-aware mobile computing research [R]. Hanover: College Dartmouth, 2000.
- [5] Moeglein M, Krasner N. An introduction to SnapTrack server-aided GPS technology[C]// Proceedings of the International Technical Meeting of the Satellite Division of the Insitute of Navigation, ION GPS 98. Nash-

ville: the Insitute of Navigation, 1998: 333—342.

- [6] Tekinay S, Chao E, Richton B. Performance benchmarking for wireless location systems[J]. IEEE Communications Magazine, 1998, 36(4): 72—76
- [7] Kaemarungsi K, Krishnamurthy P. Properties of indoor received signal strength for WLAN location fingerprinting[C]// Proceedings of the 1st Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, MobiQuitous'04. Boston, Mass: IEEE, 2004: 14—23.
- [8] Bahl P, Padmanabhan V N. RADAR: An in-building RF-based user location and tracking system[C]// Proceeding of the IEEE Infocom 2000. Los Alamitos, California: IEEE Computer Society, 2000, 2: 775—784.
- [9] Patwari N, O'Dea R J, Wang Y W. Relative location in wireless networks[C]// Vehicular Technology Conference, VTC 2001. Washington D C: IEEE, 2001, 2: 1149—1153.

作者简介:

付 雄 男,(1968—),工学博士,博士后.研究方向为信息安全和计算机犯罪。

彭 冰 男,(1972—),副教授.研究方向为无线局域网安全检测、网络攻击原理与防御技术。

(上接第3页)

- [6] Chen Jyhhorng, Fu Lichen, Lin Minghung. Petrinet and GA based approach to modeling, scheduling, and performance evaluation for wafer fabrication[C]// Proceedings of the 2000 IEEE International Conference on Robotics and Automation (ICRA'00). San Francisco: IEEE, 2000: 3403—3408.
- [7] 侯俊,齐震.基于 Petri 网的作业网络模型的正确性研究[J].微电子学与计算机,2006,23(7): 215—217.

- [8] 岳昊.三划分问题可多项式归约为唯一可达向量 Petri 网可达性问题[J].微电子学与计算机,2008,25(10): 144—146.

作者简介:

刘歌群 男,(1974—),博士,博士后,研究方向为系统科学、控制工程。