文章编号:1671-4598(2018)02-0150-04 DOI:10.16526/j.cnki.11—4762/tp.2018.02.037 中图分类号:TN99 文献标识码:B

基于传播模型和位置指纹的三维室内无源定位方法

唐力强,罗 冰,张一嘉
(中国电子科技集团公司 第三十六研究所,浙江 嘉兴 314033)

摘要:为了提高对室内窃听窃视设备的可疑信号侦察和无源定位能力,深入研究了非合作室内无源定位技术,通过分析各种室内定位算法后,提出了基于传播模型和位置指纹的三维室内无源定位方法,该方法通过位置指纹定位平面位置,通过传播模型定位高度,两者结合可获得室内三维位置,通过信噪比和幅度多重位置指纹建库与匹配算法研究,采用数据插值进一步提高了定位精度;结合该算法模型,提出了系统的组成与设计,该系统由传感节点、无线网络和信息处理机三部分组成,基于该系统完成了实际定位试验,在传感节点间隔5米的情况下,定位精度可达到3米;该方法对反窃听窃视装备应用和信息安全建设具有重大的现实意义。

关键词:室内无源定位;传播模型;位置指纹

Three Dimensional Indoor Passive Location Method Based on Propagation Model and Location Fingerprint

Tang Liqiang, Luo Bing, Zhang Yijia
(36th Institute, China Electronics Technology Group Corporation, Jiaxing 314033, China)

Abstract: In order to improve the suspicious signal reconnaissance and passive location of indoor equipment capacity eavesdropping burglary, the passive localization technique in non cooperative indoor environment is deeply studied, after analyzing various indoor location algorithms, three-dimensional indoor passive localization method based on propagation model and location fingerprinting is proposed. The method uses position fingerprints to locate the plane positions and to propagate the localization height of the model. the three dimensional indoor passive location can be obtained after the combination of the two position, through the research of database building and matching algorithms for signal to noise ratio and amplitude multi position fingerprinting, data interpolation is used to further improve the localization accuracy. Combined with the algorithm model, The composition and design of the system are proposed, the system is composed of three parts: sensor node, wireless network and information processor, and the actual positioning experiment is completed based on the system. When the sensor node is spaced 5 meters apart, the positioning accuracy can reach 3 meters. This method has great practical significance for the anti eavesdropping burglary equipment application and the construction of information security.

Keywords: indoor passive location; propagation model; location fingerprinting

0 引言

随着新技术的不断发展,加上政界、商界、反恐领域、科技领域和军事领域利益最大化需求,窃取机密资料的手法也在日益精密,窃听窃视无疑是其中重要的组成部分。目前反窃听窃视设备较多,其中比较常用的设备大部分为国外产品,在使用方面存在较多不足,包括发现可疑信号能力弱、不具备信号源定位能力等。因此,深入研究非合作室内无源定位技术,对信息安全建设具有重大的现实意义。

1 室内定位方法概述

室内定位方法大致可以按照3种最基本的定位思路进行归类,第一类是通过测量信号距离和角度来进行几何计算得到辐射源位置,其中TOA通过测量时差计算距离差绘制双曲线方程获得辐射源位置,信号传播模型则通过电波传播理论建模,由测量幅度值映射为距离从而获得辐射源位置,AOA通过定向天线或者阵列天线测量信号方向,多站交叉获得辐射源位置[1];第二类是通过物理量感知发现辐射源“靠近”传感器,用传感器的位置来估计辐射源位置,具有代表性的为最近节点法;第三类是利用对已知位置的各种测量值作为该位置的“指纹”特征,利用辐射源特征与已知位置特征匹配获得辐射源位置,可利用幅度、信噪比等参数作为特征进行特征匹配,称为位置指纹法[2]。

表1 室内定位技术比较

比较项目	TOA	信号传播模型	AOA	最近节点	位置指纹
定位准确度	高	低	高	低	较高
成本	高	低	高	低	低
样本数据	不要	需要	不要	不要	需要
算法效率	低	高	高	高	较高
受环境干扰	强	强	强	弱	弱
可行性	低	高	高	高	高
弱点	宽带信号	室内传播模型复杂	定向或阵列天线	多径影响	需要建模

2 基于传播模型和位置指纹的三维室内无源定位

在室内无线环境里,信号强度、信噪比都是比较容易测得

收稿日期:2017-06-07; 修回日期:2017-07-19。

作者简介:唐力强(1977-),男,硕士,高级工程师,主要从事通信侦察和测向定位系统总体论证、总体设计和装备研制方向的研究。

的电磁特征。LEASE 定位系统通过部署若干信号发射器，定期向外发射固定信号强度信息。在利用信号场景的定位技术中，信号强度的样本数据集也被称为位置指纹或者无线电地图。本文在对室内信号传播建模的基础上，创新性的提出了一种二维位置指纹定位方法，该方法实现了对室内未知辐射源实施非合作的无源定位，下面将详细说明理论依据和定位方法。

2.1　室内信号传播建模

不同的无线电波模型适用于不同环境，这些传播模型都可以归结为[3]：

$$A = k_1 + k_2 \log f - k_3 \log h_1 - k_4 \log h_r + 10n\log d + x \quad (1)$$

式中，A 为路径损耗，k_1，k_2，k_3，k_4 为传播模型参数，f 为载波频率，h_l，h_r 分别为信号源高度和观测台天线高度，n 为路径衰减因子，x（dB）为阴影衰落。当影响电波传播环境固定不变时，上述参数在环境较为单一的情况下均为不变因子，路径损耗 A 与距离 d 呈确定的对数关系。为了验证上述理论在室内环境下的传播特性，本文对频率分别为 800 MHz、2.4 GHz以及 4 GHz 的单音信号辐射源进行了信号传播建模实验，在室内的固定位置放置信号辐射源，在不同的距离测量侦收到的信号强度并进行记录，实验结果如图 1 所示。

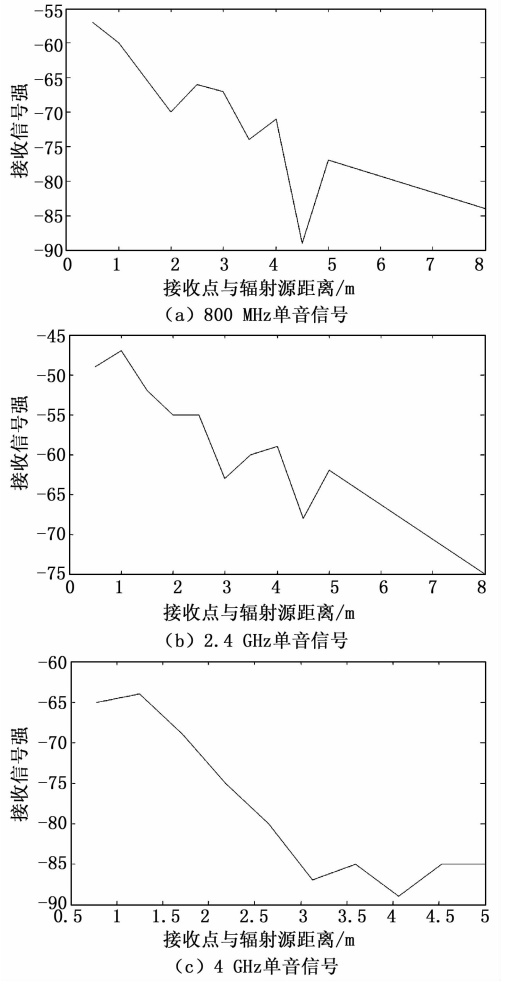

图 1　信号在室内传播建模实验

根据实验结果，当辐射源距离接收点在 3 米以内时，由于距离近时接收点主要接收辐射源的直达波，因此距离和幅度关系接近理论方程，接收信号幅度和辐射源距离呈理想的对数关系，输入距离值，即可得到与之对应的接收信号场强。当辐射源距离接收点大于 3 米时，由于多径效应影响，辐射源的反射、衍射和绕射波对信号接收影响较大，因此接收信号幅度和辐射源距离对数关系减弱，甚至无规律可循。

2.2　位置指纹室内非合作无源定位

位置指纹定位方法主要分为六个步骤，分别为：布点、构建位置指纹库、扫描全频段内的信号位置指纹、基于位置指纹的定位算法、基于传播模型的三维空间定位算法[5]。

1）布点：根据室内信号传播建模的结论，按 3～6 米间隔布置节点，可根据房间大小在室内布置 4/8/16/32 个传感节点，如要对信号进行 3 维立体定位，也可在墙面上布置传感节点，形成立方体的分布。

2）构建位置指纹库：传感节点定期向外发射不同频段的信标，其他传感节点同时接收该信标，记录本节点接收信标的能量值和信噪比值，作为当前频段的位置指纹传输至服务器的位置指纹数据库中。例如，位置 6 的传感节点发射信标时，位置 1～5 和 7～16 号节点接收信标，测量信标能量和信噪比，并以发射信号的能量和信噪比值归一化后记录至数据库中。记录格式如表 2 所示，其中 $V=[1, Vf2, Vf3\cdots Vfn]$ 代表信号能量值，$S=[Sf1, 1, Sf3\cdots Sfn]$ 代表信号信噪比值，第一个下标表示标定信号频率序号，第二个下标表示信标接收传感节点的位置序号。在位置指纹建库的基础上，还可以利用信号室内传播模型，采用内插的方法增加位置指纹数据库的密度。

表 2　位置指纹数据表示

频段	信标节点 1	信标节点 2	……	信标节点 n
100 MHz	$[1, V_{12}, V_{13}, \cdots, V_{1n}]$ $[1, S_{12}, S_{13}, \cdots, S_{1n}]$	$[V_{11,1}, V_{13}, \cdots, V_{1n}]$ $[S_{11,1}, S_{13}, \cdots, S_{1n}]$	……	$[V_{11}, V_{12}, \cdots, V_{1n-1,1}]$ $[S_{11}, S_{12}, \cdots, S_{1n-1,1}]$
200 MHz	$[1, V_{22}, V_{23}, \cdots, V_{2n}]$ $[1, S_{22}, S_{23}, \cdots, S_{2n}]$	$[V_{21,1}, V_{23}, \cdots, V_{2n}]$ $[S_{21,1}, S_{23}, \cdots, S_{2n}]$	……	$[V_{21}, V_{22}, \cdots, V_{2n-1,1}]$ $[S_{21}, S_{22}, \cdots, S_{2n-1,1}]$
……	……	……	……	……
6 000 MHz	$[1, V_{602}, V_{603}, \cdots, V_{60n}]$ $[1, S_{602}, S_{603}, \cdots, S_{60n}]$	$[V_{601,1}, V_{603}, \cdots, V_{60n}]$ $[S_{601,1}, S_{603}, \cdots, S_{60n}]$	……	$[V_{601}, V_{602}, \cdots, V_{60n-1,1}]$ $[S_{601}, S_{602}, \cdots, S_{60n-1,1}]$

3）扫描信号位置指纹：室内传感节点在不同的位置扫描测量相应频段内信号的频率 f、幅度 V 和信噪比 S，记为 $v=[v_{f1}, v_{f2}, v_{f3}, \cdots, v_{fn}]$ 和 $s=[s_{f1}, s_{f2}, s_{f3}, \cdots, s_{fn}]$，其中 f 为信号频率。建立信号位置指纹数据库后，通过软件算法可快速、精确和低成本地获得相应频段内任意信号频率、幅度和信噪比。

4）基于位置指纹的定位算法：匹配位置指纹包含两部分内容，频率选择和节点匹配。通过信号频率 f 在位置指纹数据库中寻找最接近的频段的标定数据，例如，当测量信号频率为 1 727 MHz 时，可选择 1 700 MHz 标定的位置指纹数据进行匹配。信号的幅度测量值为 $v=[v_{f1}, v_{f2}, v_{f3}, \cdots, v_{fn}]$ 和

信噪比测量值为 $s=[s_{f1}, s_{f2}, s_{f3}, \cdots, s_{fn}]$，其中最简单直接的最近邻法进行匹配定位，通过计算最短欧几里得距离，求取各个传感节点所对应的信号幅度和信噪比的方差 $\Delta vs_1 \cdots \Delta vs_i \cdots \Delta vs_n$，如式（2）所示。

$$\Delta vs_i = \sqrt{(v_{f1}-V_{f1})^2+(v_{f2}-V_{f2})^2+\cdots+(v_{fn}+V_{fn})^2}+\alpha\sqrt{(s_{f1}-S_{f1})^2+(s_{f2}-S_{f2})^2+\cdots+(s_{fn}+S_{fn})^2} \quad (2)$$

其中：v 和 s 向量为测量值，V 和 S 为标定值，α 为幅度和信噪比权重，可根据具体应用场景控制幅度方差和信噪比方差对 Δvs_i 的影响度，取所有方差的最小值 $\Delta vs_{\min}$，其所对应的节点位置即为信号的匹配位置。也可以根据实际情况选择其他定位算法，例如朴素贝叶斯法等。

5）基于传播模型的三维空间定位算法：普通的室内环境是一个三维空间，在完成基于位置指纹定位算法后，可获得二维平面空间的位置，但无法获取辐射源在室内的高度，如图 2 所示。在本文 3.1 室内信号传播建模章节中得到的结论，当辐射源距离传感节点在 3～4 米以内时可通过接收信号场强反推获得辐射源距离。一般普通房间的单层层高为 3 米左右，恰好满足此结论的应用条件，因此可以基于传播模型通过最近两个传感节点的信号场强幅度反推辐射源距离进行交叉定位。

根据 2.1 节中传播模型公式（1），假设两个不同位置的接收天线都能够收到同一信号源发射的信号，且两传输路径有相同的传播模型参数，设两个接收天线到辐射源的路径损耗分别为 A_1，A_2，则两路径接收信号损耗差值为：

$$A_1-A_2=10n\log\frac{d_1}{d_2}+(X_1-X_2) \quad (3)$$

式中，d_1，d_2 为信号源到接收天线 1，2 的距离，定义 $X'=X_1-X_2$，则：

$$k_{12}=d_1/d_2=10^{\frac{A_1-A_2}{10n}+X''} \quad (4)$$

式中，反映阴影衰落的随机变量 $X''=X'/10n$ 是零均值的高斯随机分布。假设信号源位置坐标为 (x, y)，两个接收天线位置坐标分别为 (x_1, y_1)，(x_2, y_2)，则由式（4）可以得到：

$$k_{12}=\frac{\sqrt{(x-x_1)^2+(y-y_1)^2}}{\sqrt{(x-x_2)^2+(y-y_2)^2}} \quad (5)$$

对式（4）整理得：

$$(x-\frac{k_{12}^1x_2-x_1}{k_{12}^2})^2+(y-\frac{k_{12}^2y_2-y_1}{k_{12}^2-1})^2=\frac{k_{12}^2}{(k_{12}^2-1)^2}D_{12}^2 \quad (6)$$

式中，D_{12} 为两接收天线之间的距离。于是两个位置的接收天线之间的接收信号场强差就可以确定一个方程，求解所有的方程构成的方程组，就可以得到辐射源的位置在高度平面上的距离，结合平面位置即可得到室内空间的三维坐标。

综上所述，通过基于位置指纹的定位算法确定辐射源室内平面位置，通过基于传播模型定位方法确定辐射源室内的高度，两种方法的结合可获得辐射源室内三维空间位置。

3 系统设计和组成

3.1 系统组成

本系统由传感节点、无线网络和信息处理机三部分组成，其布置如图 2 所示。

1）传感节点：以 Xilinx 公司推出的 SoC Zynq－7045 作为主芯片，搭载 2 片 ADI 公司的 AD9361 射频芯片，支持 80 MHz～6 GHz 的 4 收 4 发，若接 4 个天线则可支持 4 个传感节点检测，使用锂电池供电。天线按照 70 MHz～3 GHz 和 3～6 GHz 两段设计，两根天线分别接两路收发。

2）无线 AP：采用 802.11 ad 无线通信协议，支持 60 GHz 的高速传输，既可实现高速数据通信又与侦测频段相隔离，不影响传感节点的信号检测。

3）信息处理机：采用高性能工作站连接无线 AP，接收来自各个传感节点的信号和数据，通过软件进行频谱辐射源数据建库、信号识别处理、室内外判断、室内定位等算法处理。也可采用高性能笔记本电脑，通过软件处理完成上述算法计算。

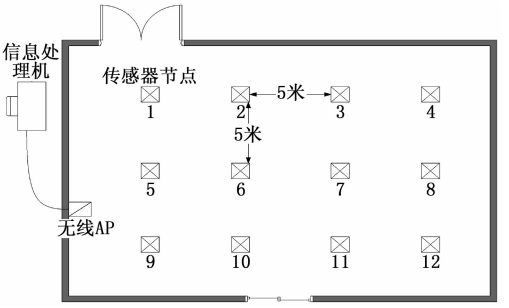

图 2 室内传感节点布置图

3.2 系统设计

信息处理机和传感节点根据各自的任务分工对信号进行处理和分析，第一部分为信号识别算法，识别是否是商用信号，并对 wifi、3 G、4 G 等类型进行识别和分类，若非商用信号则识别其信号特征，包括调制样式、带宽、频率等，并存储记录。第二部分算法为室内外定位算法，将获得的所有传感节点幅度值与标定完的辐射地图进行匹配，结合信号类型识别结果，综合判断信号是否在室内。第三部分算法为室内定位算法，当判定信号在室内时，通过辐射源指纹识别算法，匹配计算辐射源位置，设备告警并给出室内大致位置。

首先根据房间大小在室内布置若干个传感节点；然后传感节点切换至建库模式，每个传感节点自动发射各个频段的信号，其他节点接收该信号进行标定，将标定值通过无线 AP 传输至信息处理机，信息处理机建立数据库并绘制辐射地图，可设置间隔一定时间执行一次；所有传感节点切换至检测模式进行全频段扫描，当发现可疑辐射源信号，所有传感节点对辐射源信号特征值进行测量，并将其传输至信息处理机进行识别与定位。

4 系统实验

4.1 基于传播模型的 GSM 信号室内外判别实验

1）试验概述：按图 3 布置天线阵，被测手机分别在房间的天线阵内的 4 个区域和房间外进行通话，通话时采集记录 4 个天线的信号，通过数据采集和分析对 GSM 手机进行室内外的判断。

2）试验步骤：

a）将设备按照试验框图进行连接；

b）通道一致性校正；

c）天线放置于办公室 4 角；

d）将手机分别放置在采样点，开机打电话产生信号；

e）将 1 727 MHz 射频变频至 70 MHz 频率 20 MHz 带宽的中频信号

f）采集设备分别记录 4 个天线的信号原始数据；

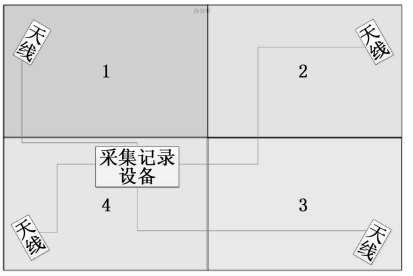

图 3　测试区域

g）信号处理算法进行幅度计算。

3）数据分析：室外实验时，衰减 30 dB 后已检测不到信号，在未衰减 30 dB 情况下，可测到手机信号值如表 3 所示。

表 3　实测室外值

	天线 1	天线 2	天线 3	天线 4
幅度	286.382	298.440	292.328	305.322
归一化	1	1.0 421	1.0 208	1.0 661

室内实验结果如表 4 所示，表中为最小值归一化后的幅度比值。

表 4　实测室内各个区域值

位置	天线 1	天线 2	天线 3	天线 4
1	1.2 840	1.2 301	1	1.1 409
2	1.0 823	1.2 033	1	1.0 603
3	1	1.0 650	1.1 334	1.0 299
4	1.0 297	1.1 041	1	1.1 721

4）结果分析：在一定衰减值下，室外信号无法被定向天线侦测到，信号幅度高低可作为室内外信号的判据之一。当降低衰减值时，各个天线可接收室外信号，归一化后接近于 1（如表 4 所示），因此接近于 1 的幅度比值也可作为判据之一。在 1、2、3、44 个区域均可根据幅度比值进行匹配，并给出大致区域。采用非标定的比幅方法，不但可区别室内外信号，还可对室内信号进行粗定位，虽精度不高，但是稳定可靠。

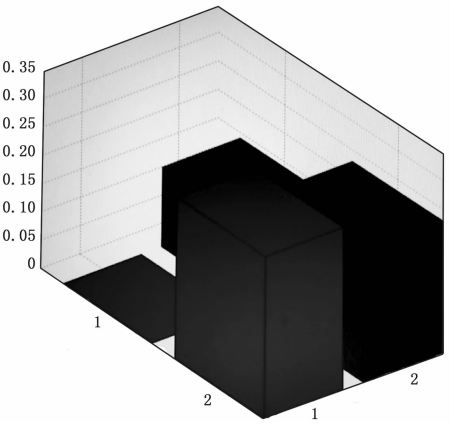

图 4　幅度归一化直方图

综上所述，要判断是否在室内外，可通过设定信号幅度绝对阈值和幅度相对阈值进行判断和筛选。

4.2　基于位置指纹的 Wifi 信号定位实验

本文实验使用了 12 个传感节点、1 个无线 AP 和 1 台信息处理机。在长方形房间内每隔 5 米布置一个传感节点（如图 2 所示），对 2.4 GHz 信号进行建库和定位。首先由各个传感节点发射频率为 2.4 GHz 幅度为－10 dbm 的单音信号进行标定和建库，其中建库数据如表 3 所示，数据表格中横轴 S1－S12 为不同位置传感节点发射标定信号，纵轴为在不同位置传感节点的去直流分量后的接收幅度值。

从表中可以看到不同位置的辐射源，在 12 个点的接收幅度值均有较大差别，利用信号强度均方差可较清晰的区分相邻辐射源的特征。通过对表中的建库幅度值采用最近邻法进行匹配定位，实际测试结果均能较好地获得 2.4 GHz 频段内的各种辐射源的位置，定位精度可达到 3 米。在此基础上还可利用近距离传播模型进行插值建模，在插值的基础上增加位置指纹模型库的密度，可进一步提高定位精度。

5　结论

本文在通过分析各种室内定位算法的基础上，提出了基于传播模型和位置指纹的三维室内无源定位方法，该方法通过位置指纹定位平面位置，通过传播模型定位高度，两者结合可获

表 5　2.4 GHz 信号建库数据表

(dbm)	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12
R1		21.8	8.3	－14.1	0.1	－1.1	－14.1	－7.19	－10.8	－3.7	－3.3	－2.1
R2	15.2		15.5	－2.3	－2.2	－6.7	－8.1	－8.4	－20.8	－9.7	－21.3	－6.9
R3	1.2	20.2		14.7	－11.7	－9.1	－4.4	－9.4	－20.8	－8.7	－6.3	－4.4
R4	11.2	12.2	12.2		－6.8	－8.9	－3.2	－2.02	－6.8	－4.7	－6.3	－6.7
R5	－5.9	－16.8	2.4	0.07		7.3	1.6	5.3	－0.8	－3.7	4.7	－12.1
R6	9.0	－14.7	－6.4	－7.9	9.1		12.3	7.8	0.2	0.3	－5.3	－18.1
R7	1.9	－17.3	－4.9	－6.7	0.2	6.9		13.8	－0.8	－11.7	－5.3	－0.9
R8	－8.2	－23.7	－10.9	6.1	5.2	0.6	16.7		－2.8	－1.7	－2.3	－5.8
R9	－7.0	1.7	－8.2	－9.0	－0.5	－2.6	0.6	－4.8		12.3	5.7	－2.4
R10	0.03	－1.7	－10.9	1.6	2.7	2.9	0.14	1.9	15.2		13.7	12.7
R11	－25.5	－2.1	－6.8	－4.6	－2.3	0.9	－10.9	－11.3	11.2	12.3		14.2
R12	－15.5	－4.1	－9.9	－3.4	－9.9	－6.6	－5.8	－0.74	10.2	－1.7	1.2	

（下转第 157 页）