



测绘遥感信息工程国家重点实验室  
State Key Laboratory Of Information Engineering In Surveying, Mapping and Remote Sensing

柳景斌

教授/博士生导师/青年千人计划学者  
导航定位与位置服务研究室主任  
湖北省自然科学基金创新群体负责人

手机: +86 13971082735 电话: +86-27-87731869  
邮箱: jingbin.liu@whu.edu.cn 地址: 中国·武汉·珞喻路129号  
网址: www.lmars.whu.edu.cn/

# 室内定位技术

主讲: 柳景斌, 测绘遥感信息工程国家重点实验室

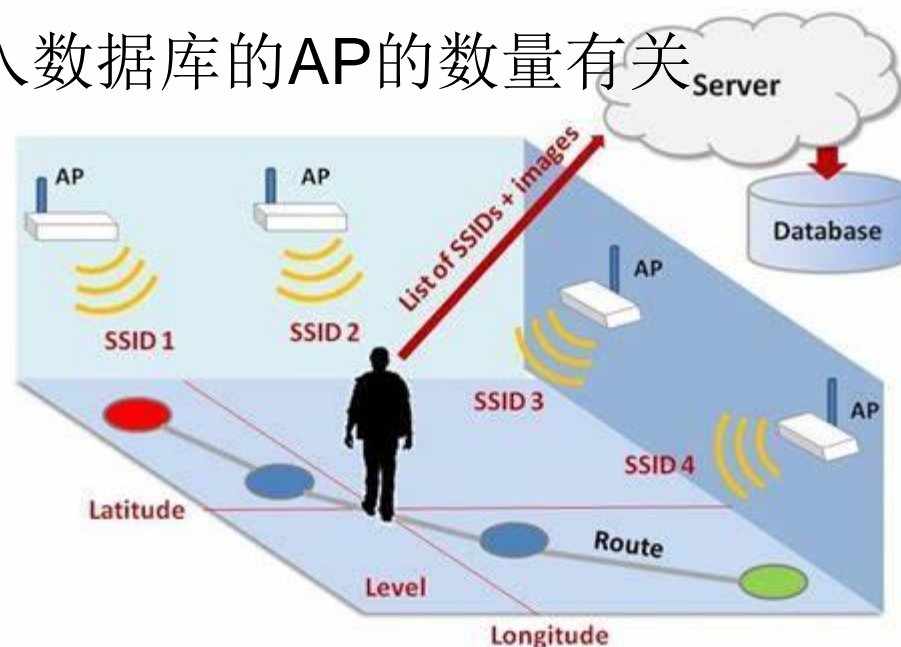
# 第3章 Wi-Fi定位系统

## 3.1 概述

# 概述

- Wi-Fi定位系统

- 受益于21世纪在城市地区快速增长的无线AP的数量
- 利用被定位目标附近的Wi-Fi热点或其他无线接入点（AP）的信号特征对其进行定位
- 主要基于RSSI和指纹方法
- 用于确定无线AP位置的典型参数是SSID（**Service Sets ID**）和MAC地址.
- 定位精度与附近位置已录入数据库的AP的数量有关

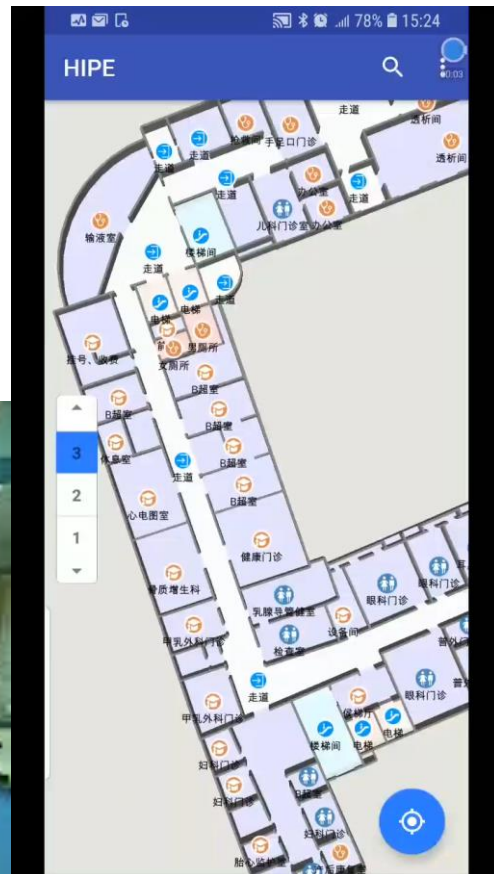


## 精准医疗及护理 (医院)

- 病人诊室导航
- 设备跟踪管理
- 护理及时呼叫 (养老院)
- 医护流程管理



**武汉市  
十一医院示范应用**



# 概述

- 主要技术方法
  - RSSI、指纹、AOA、TOF (Time of Flight)
- 应用
  - 增强现实 (AR)
  - 社交网络
  - 健康监测
  - 人员跟踪
  - 资产控制
  - 其他室内位置感知应用

## 3.2 Wi-Fi基础

# OSI模型



# OSI模型

- OSI
  - Open System Interconnection/开放式系统互联
- 制定者
  - 国际标准化组织（ISO）
- 内容：
  - 定义不同计算机互联的标准
  - 设计和描述计算机网络通信的基本框架
- 将网络通信的工作分为7层（由低至高）
  - 物理层、数据链路层、网络层、传输层、会话层、表示层和应用层



# OSI模型的工作分层①

- 物理层
  - 有关传输介质的特性标准，包括连接头、帧、帧的使用、电流、编码及光调制等。
- 数据链路层
  - 定义在单个链路上传输数据的方式。
- 网络层
  - 对端到端的包传输进行定义，定义了能够标识所有结点的逻辑地址，还定义了路由实现的方式和学习的方式。
  - 为适应最大传输单元长度小于包长度的传输介质，定义了如何将一个包分解成更小的包的分段方法。
  - 示例：IP，IPX等。

# OSI模型的工作分层②

- 传输层

- 功能包括是否选择**差错恢复协议**还是**无差错恢复协议**，及在同一主机上对不同应用的数据流的输入进行复用，还包括对收到的顺序不对的数据包的重新排序功能。示例：  
**TCP, UDP, SPX。**

- 会话层

- 控制计算机间的对话，包括对多个双向消息的控制和管理。

- 表示层

- 建立应用层实体间的语境，定义数据格式及加密等。

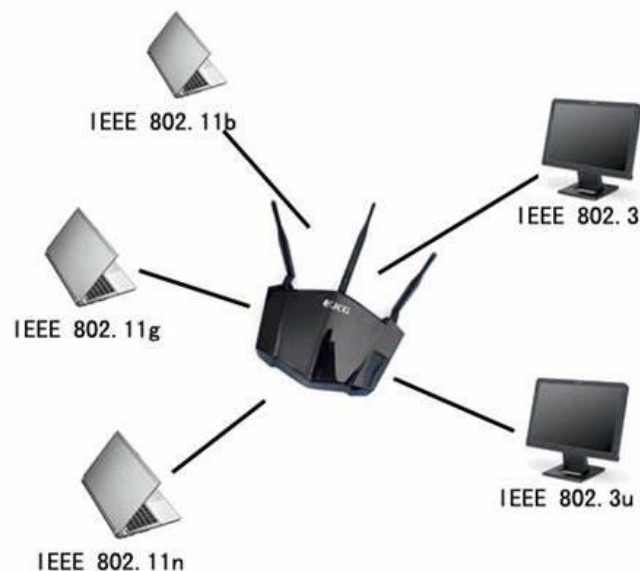
- 应用层

- 与其他计算机进行通讯的一个应用，对应应用程序的通信服务。如**Telnet、HTTP、FTP、NFS、SMTP**等。

# IEEE 802

# IEEE 802

- 一组处理局域网和城域网的IEEE标准
- 定义了局域网和城域网的物理层和MAC层中的服务和协议，对应OSI网络参考模型的最低两层，即物理层和数据链路层。



# 物理层和数据链路层

- 物理层（PHY, Physical Layer）
- 数据链路层
  - 逻辑链路控制子层
    - 用户的数据链路服务通过LLC子层为网络层提供统一的接口。
  - 介质访问控制子层（MAC, Media Access Control）
    - 通过在IP包上加了8位的目的地地址服务接入点和源地址服务接入点来保证在不同网络类型中传输。另外，有一个8或16位的控制字段用于象流控制的辅助功能。

# IEEE 802工作组①

Name	Description	Note
IEEE 802.1	Higher Layer LAN Protocols (Bridging)	active
IEEE 802.2	LLC	disbanded
IEEE 802.3	Ethernet	active
IEEE 802.4	Token bus	disbanded
IEEE 802.5	Token ring MAC layer	disbanded
IEEE 802.6	MANs (DQDB)	disbanded
IEEE 802.7	Broadband LAN using Coaxial Cable	disbanded
IEEE 802.8	Fiber Optic TAG	disbanded
IEEE 802.9	Integrated Services LAN (ISLAN or isoEthernet)	disbanded
IEEE 802.10	Interoperable LAN Security	disbanded
IEEE 802.11	Wireless LAN (WLAN) & Mesh (Wi-Fi certification)	active
IEEE 802.12	100BaseVG	disbanded

# IEEE 802工作组②

Name	Description	Note
IEEE 802.13	Unused[2]	Reserved for Fast Ethernet development[3]
IEEE 802.14	Cable modems	disbanded
IEEE 802.15	Wireless PAN	active
IEEE 802.15.1	Bluetooth certification	active
IEEE 802.15.2	IEEE 802.15 and IEEE 802.11 coexistence	Hibernating [4]
IEEE 802.15.3	High-Rate wireless PAN (e.g., UWB, etc.)	
IEEE 802.15.4	Low-Rate wireless PAN (e.g., ZigBee, WirelessHART, MiWi, etc.)	active
IEEE 802.15.5	Mesh networking for WPAN	
IEEE 802.15.6	Body area network	active
IEEE 802.15.7	Visible light communications	
IEEE 802.16	Broadband Wireless Access (WiMAX certification)	hibernating



# IEEE 802工作组③

Name	Description	Note
IEEE 802.16.1	Local Multipoint Distribution Service	
IEEE 802.16.2	Coexistence wireless access	
IEEE 802.17	Resilient packet ring	hibernating
IEEE 802.18	Radio Regulatory TAG	
IEEE 802.19	Coexistence TAG	
IEEE 802.20	Mobile Broadband Wireless Access	hibernating
IEEE 802.21	Media Independent Handoff	
IEEE 802.22	Wireless Regional Area Network	
IEEE 802.23	Emergency Services Working Group	
IEEE 802.24	Smart Grid TAG	New (November, 2012)
IEEE 802.25	Omni-Range Area Network	

# Wi-Fi

# Wi-Fi与IEEE 802.11

- Wi-Fi
  - 基于IEEE 802.11标准的无线局域网技术
  - Wi-Fi是Wi-Fi联盟的注册商标
- IEEE 802.11
  - 无线局域网通用的标准，由IEEE所定义的无线网络通信的标准。



# IEEE 802.11 PHY

IEEE 802.11 network PHY standards <span>[hide]</span>								
Protocol ↕	Release date <sup>[10]</sup> ↕	Fre- quency	Band- width	Stream data rate <sup>[11]</sup>	Allowable MIMO streams ↕	Modulation ↕	Approximate range <sup>[citation needed]</sup>	
		(GHz) ↕	(MHz) ↕	(Mbit/s) ↕			Indoor ↕	Outdoor ↕
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
802.11a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		3.7 <sup>[A]</sup>						5,000 m (16,000 ft) <sup>[A]</sup>
802.11b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
802.11g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38 m (125 ft)	140 m (460 ft)
802.11n (Wi-Fi 4)	Oct 2009	2.4/5	20	Up to 288.8 <sup>[B]</sup>	4		70 m (230 ft)	250 m (820 ft) <sup>[12]</sup>
			40	Up to 600 <sup>[B]</sup>				
802.11ac (Wi-Fi 5)	Dec 2013	5	20	Up to 346.8 <sup>[B]</sup>	8	MIMO-OFDM	35 m (115 ft) <sup>[13]</sup>	
			40	Up to 800 <sup>[B]</sup>				
			80	Up to 1733.2 <sup>[B]</sup>				
			160	Up to 3466.8 <sup>[B]</sup>				
		0.054–0.79 <sup>[C]</sup>	6–8	Up to 568.9 <sup>[14]</sup>	4			
802.11ad	Dec 2012	60	2,160	Up to 6,757 <sup>[15]</sup> (6.7 Gbit/s)	N/A	OFDM, single carrier, low-power single carrier	3.3 m (11 ft) <sup>[16]</sup>	
802.11ah	Dec 2016	0.9	1–16	Up to 347 <sup>[17]</sup>	4	MIMO-OFDM		
802.11aj	Est. Jul 2017	45/60						
802.11ax (Wi-Fi 6)	Est. Dec 2018	2.4/5		Up to 10,530 (10.53 Gbit/s)		MIMO-OFDM		
802.11ay	Est. Nov 2019	60	8000	Up to 20,000 (20 Gbit/s) <sup>[18]</sup>	4	OFDM, single carrier	10 m (33 ft)	100 m (328 ft)
802.11az	Est. Mar 2021	60						
802.11 Standard rollups								
802.11-2007	Mar 2007	2.4, 5		Up to 54		DSSS, OFDM		
802.11-2012	Mar 2012	2.4, 5		Up to 150 <sup>[B]</sup>		DSSS, OFDM		
802.11-2016	Dec 2016	2.4, 5, 60		Up to 866.7 or 6,757 <sup>[B]</sup>		DSSS, OFDM		

- <sup>A1 A2</sup> IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- <sup>B1 B2 B3 B4 B5 B6</sup> Based on short guard interval; standard guard interval is ~10% slower. Rates vary widely based on distance, obstructions, and interference.
- <sup>C1</sup> IEEE 802.11af about using white space spectrum for WiFi based on the PHY layer of 802.11ac

- MIMO（Multiple-Input Multiple-Output）

- 在发射端和接收端分别使用多个发射天线和接收天线，使信号通过发射端与接收端的多个天线传送和接收，从而改善通信质量。
- 能充分利用空间资源，通过多个天线实现多发多收，在不增加频谱资源和天线发射功率的情况下，可以成倍的提高系统信道容量，并提高信道的可靠性。

## 多射频、多数据流，最新 MU-MIMO 技术

### 一机多射频\*\*。

普遍采用双频、三频规格，不同射频单元间使用串扰隔离技术。和普通单频及不实施射频隔离的多频产品相比，单台服务用户数获得2~3倍增长。相当于本来只有一条路，现在变成两条路、三条路，路和路之间不会相互影响。

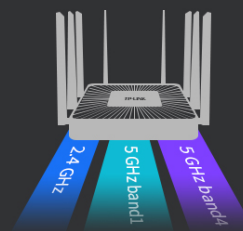
### 单一射频内多数据流\*\*。

普遍采用三数据流和四数据流规格，和单数据流产品相比，单用户平均带宽获得3~4倍增长。相当于一条路本来是单车道窄路，现在变成了三车道、四车道宽路。

### 全新MU-MIMO技术\*\*。

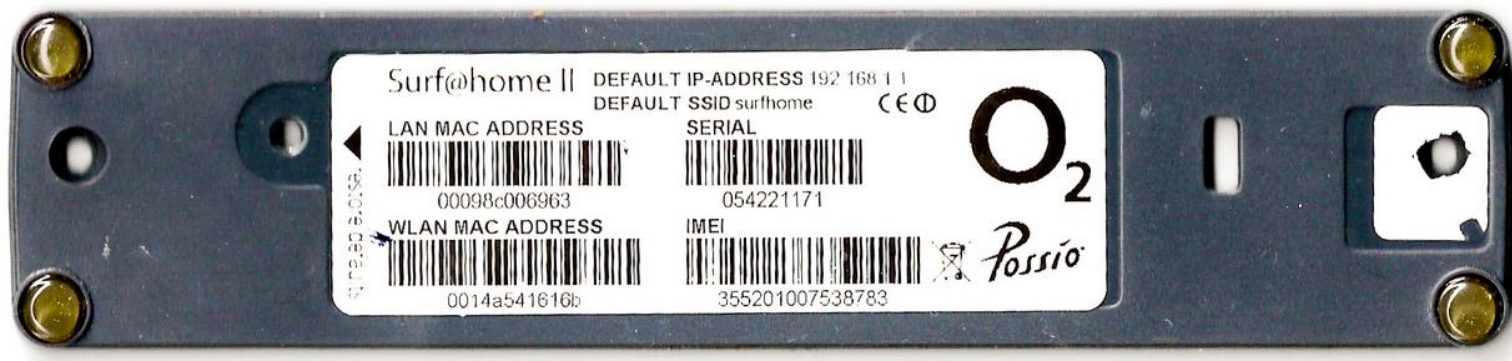
采用最新MU-MIMO技术，使在单一射频内多用户的共享方式，从——排队，顺序通过，变成齐头并进。这让多数据流射频通路的服务用户数和单用户平均带宽又获得额外的2~3倍增长。相当于明明是三车道、四车道的路，但道路入口设了一个关卡，每次只让一辆车通过，现在把关卡取消了，三辆车、四辆车可以同时上路。

最高三频规格，串扰隔离技术



# MAC地址

- Media Access Control Address，媒体访问控制地址，也被称为或物理地址（Physical Address）
- 用于在网络中唯一标示一个网卡，
- 每个网卡都需要并会有一个唯一的MAC地址

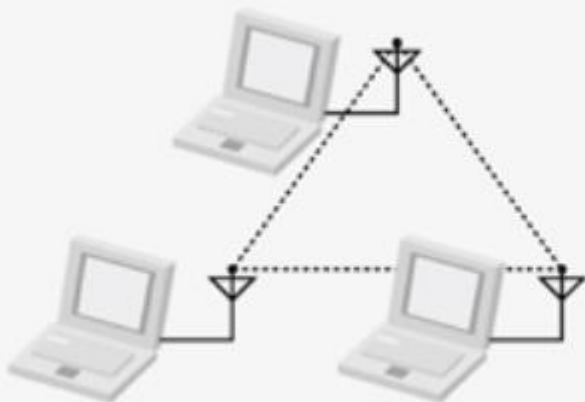


# WiFi基本服务集的构成

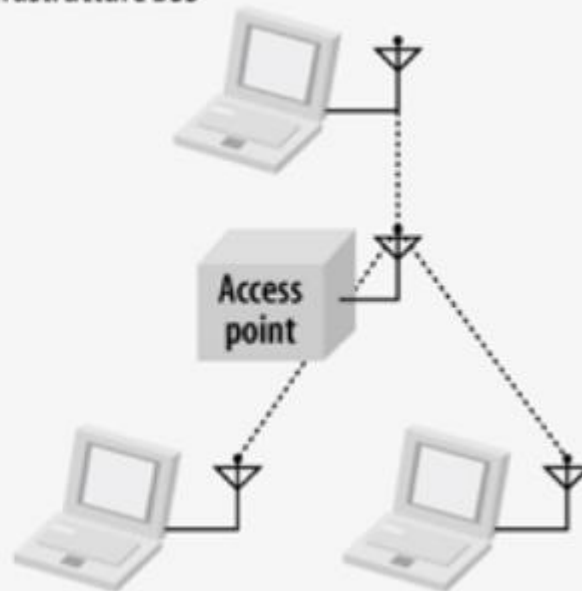
- 站点**STA**（**Station**）
  - 指具有**WIFI**通信功能的，并且连接到无线网络中的终端设备，如手机、平板电脑、笔记本电脑等。
- 接入点**AP**（**Access Point**）
  - 也可称为基站，**WIFI**热点，作用是使**STA**加入基础结构型基本服务集。
- 基本服务集**BSS**（**Basic Service Set**）
  - 两种方式
    - 有接入点的，称为基础结构型基本服务集（**infrastructure BSS**）；
    - 无接入点的，称为独立型基本服务集（**Independent BSS**，简称**IBSS**），也被称为**Ad Hoc Network**（特设网络）。
- 服务集识别码**SSID**（**Service Set Identifier**）

# 两种基本服务集BSS（Basic Service Set）

*Independent BSS*



*Infrastructure BSS*





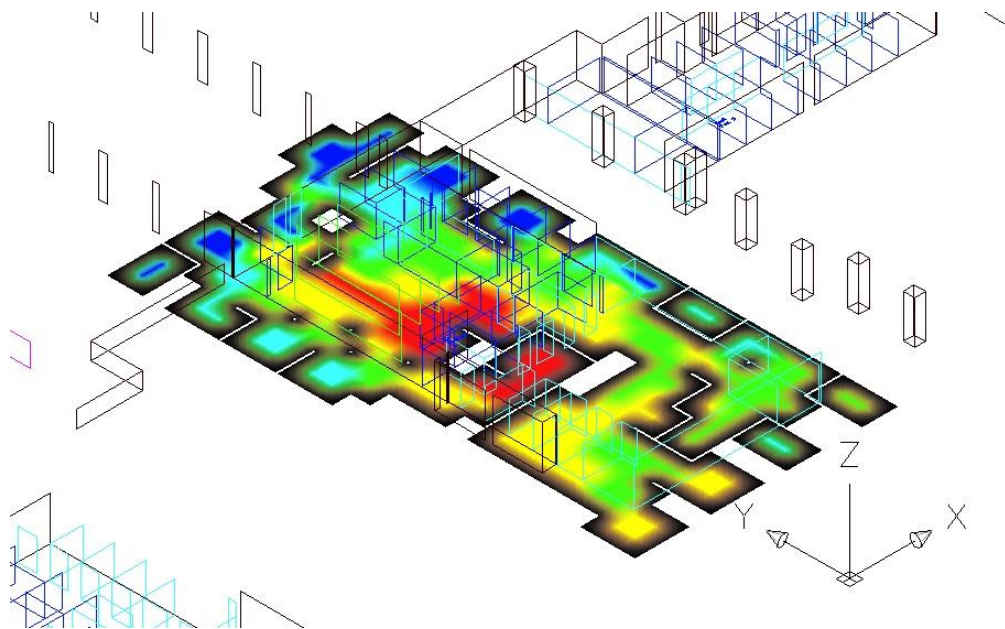
## 2.3 Wi-Fi定位技术方法

# 基于RSSI和交会的方法

- 观测量
  - 由RSSI转换的距离
- 方法
  - 距离交会
- 精度
  - 2~4m ( $1\sigma$ )

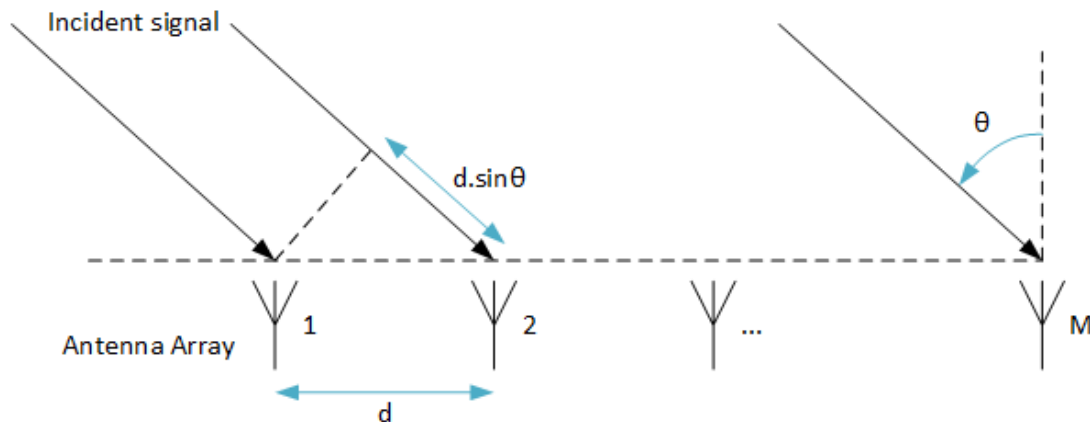
# 基于指纹的方法

- 观测量
  - RSSI向量（多AP）
- 方法
  - 指纹匹配
- 精度
  - 0.6m ( $1\sigma$ )
- 局限
  - 指纹库需要经常更新



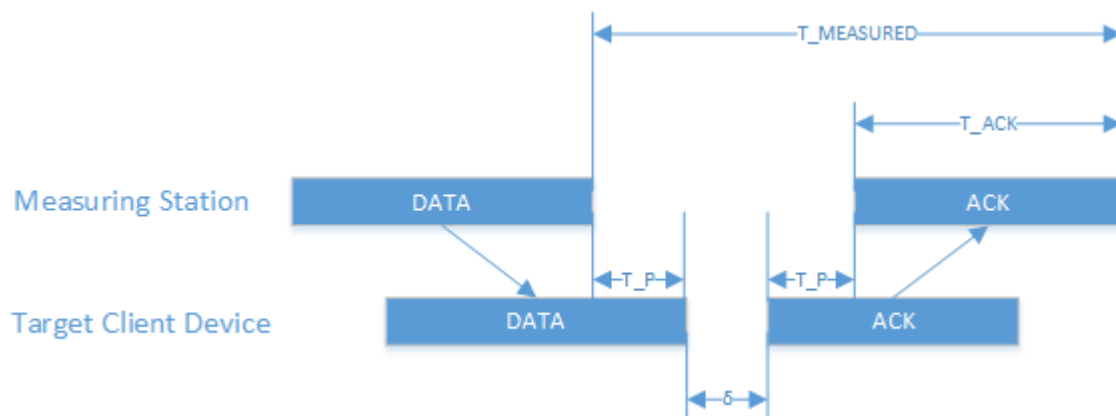
# 基于AOA的方法

- 观测量
  - AOA（利用MIMO Wi-Fi界面，采用诸如MUSIC算法）
- 方法
  - 方向交会
- 精度
  - 较高
- 局限
  - 需要特定硬件支持



# 基于ToF的方法

- 观测量
  - 信号传播时间，可得出距离
- 方法
  - 距离交会
- 精度
  - 2~3m
- 局限
  - 需要特定硬件支持



## 3.4 Wi-Fi定位系统的实现

# Wi-Fi定位系统工作的两个阶段

- 离线建指纹库阶段

- 位置与指纹对应关系的建立通常在离线阶段进行。
- 在每一个网格点上，通过一段时间的数据采样（5到15秒钟，大约每秒采集一次）得到来自各个AP的平均RSS，采集的时候移动设备可能有不同的朝向和角度。

- 在线定位阶段

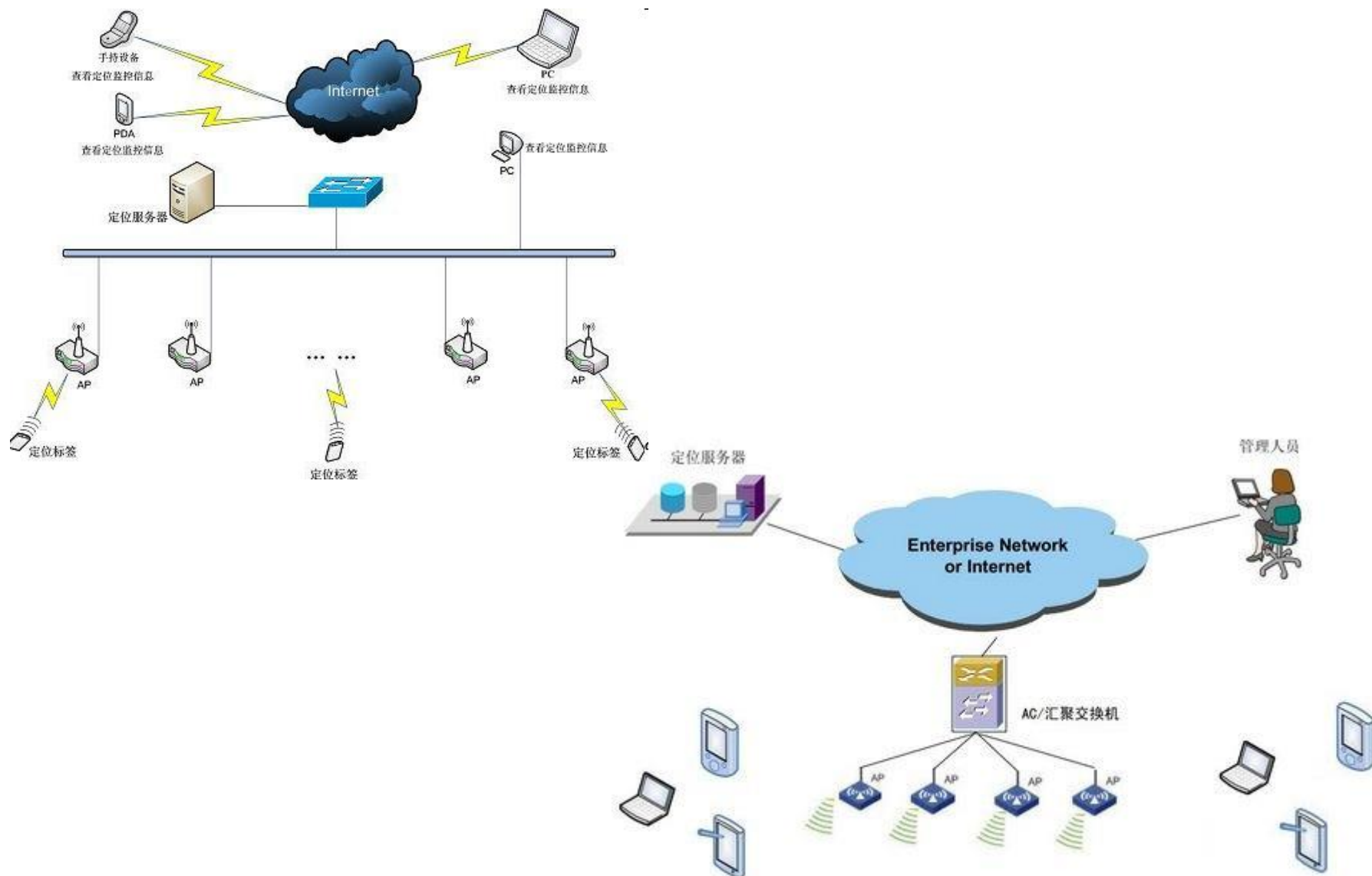
- 在在线阶段，一个移动设备处于这个地理区域之中，但是不知道它的具体位置，它甚至不太可能正好处于网格点上。
- 假设这个移动设备测量到了来自各个AP的RSS
- 要确定移动设备的位置，就是要找到在指纹库中找到与该位置最匹配的指纹。一旦找到了最佳的匹配，那么移动设备的位置就被估计为这个最佳匹配的指纹所对应的位置。

# Wi-Fi定位系统的工作模式

- 单机模式
  - 指纹库存于定位终端，指纹匹配在定位终端进行
  - 无需网络连接
  - 终端计算量大，指纹库无法及时更新
- Web服务模式
  - 定位服务器位于云端
  - 指纹库位于定位服务器
  - 指纹匹配在云端进行
  - 定位终端无需进行复杂计算
  - 需要网络连接



# Web服务模式下的Wi-Fi定位系统



# 指纹库建立与更新

- 广域
  - 初始指纹库的建立：需要专门采集
  - 指纹库更新：众包模式
- 局域
  - 初始指纹库的建立：需要专门采集
  - 指纹库更新：专门采集+众包模式

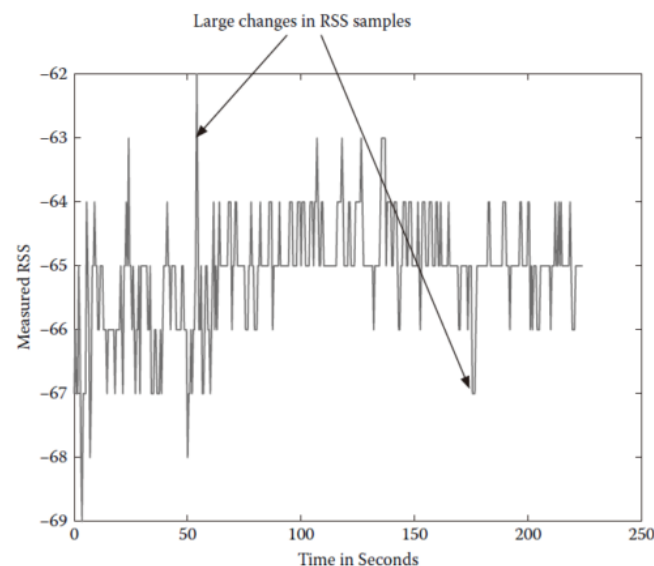
# 瞬时Wi-Fi信号RSSI不稳定问题的处理

- 问题

- 无线电的传播易受环境影响，RSS随时间变化，而且有时变化得很显著。

- 应对

- 取多次采样，然后进行中值滤波或均值滤波等。



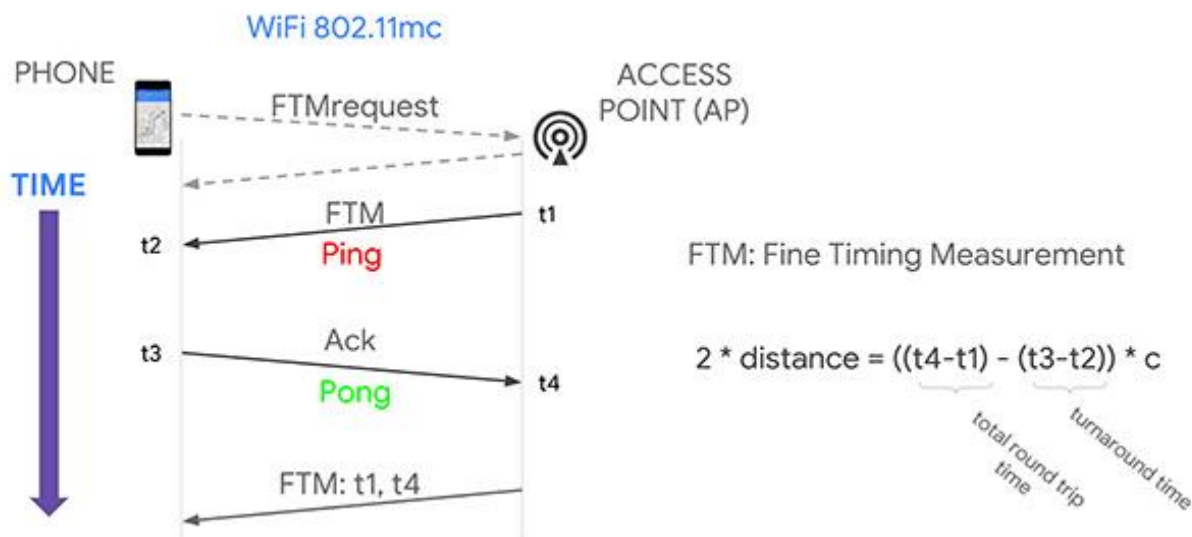
# WiFi指纹匹配定位原理

- WiFi指纹匹配定位中的主要问题
  - 信号强度跳变（噪声）
  - 基站位置变化带来的问题
  - 训练效率**vs**定位精度的问题
  - 不同类型的终端系统误差
  - 如何发现“最优”解（匹配算法）
  - 如何结合行人运动特点提高定位精度？

## 3.5 可与Wi-Fi定位协同的定位技术

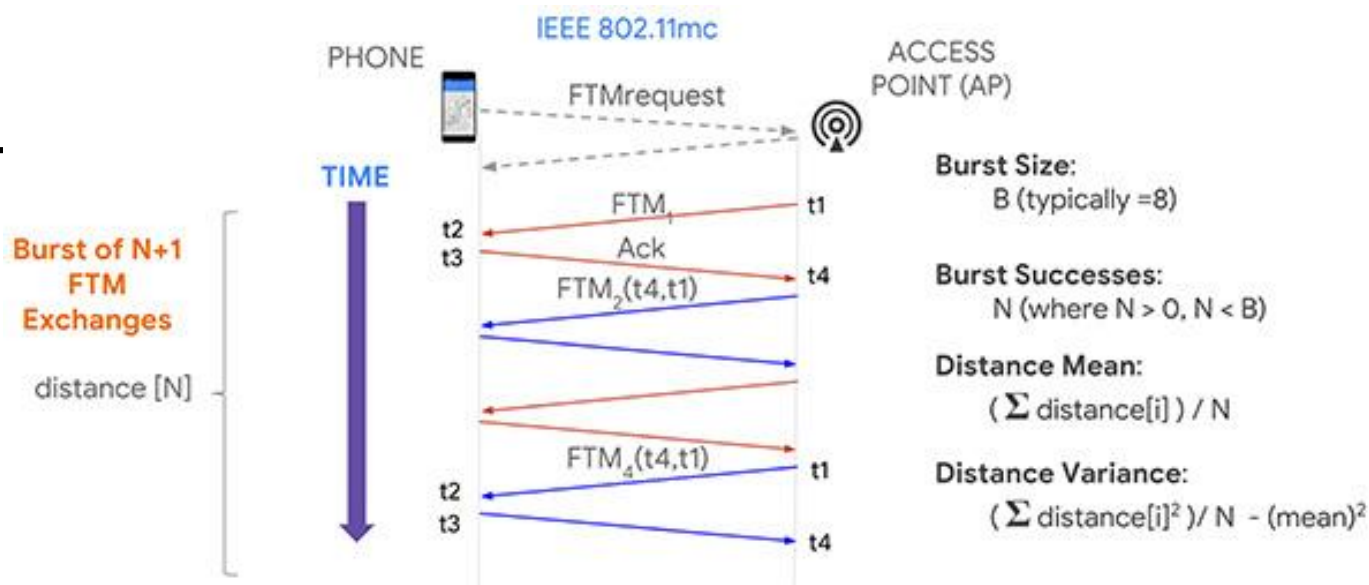


- 通过测量WiFi信号往返时间差(Round Trip Time)测量手机到WiFi基站 (Access Point) 的距离;
- 适用协议和软件平台: 802.11mc和Android 9系统;
- 手机端和Access Point端内部时钟都是不同步的, 所以单向的测量无法消除时钟不同步的影响;
- 时间戳t2,t3存储在手机端, 时间戳t1,t4存储在AP端, Ping-Pong结束后, AP端再发携带t1,t4的数据包到手机端计算距离。





- 室内环境复杂多变，RF干扰，测量误差，物体和人员的移动都会对测量精度造成影响
- 重复测量提高精度





实验场地：测试距离44m。以1.2m为间隔，共测试37个点。

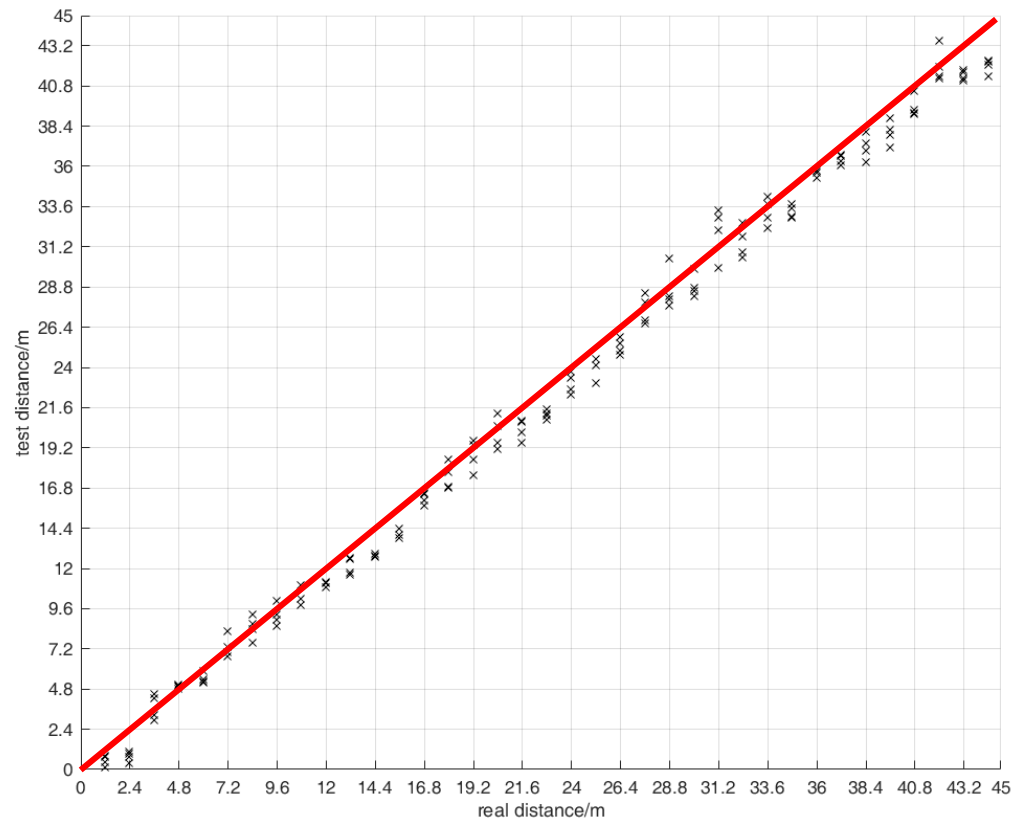
实验设备：~~WILD RTT基站，谷歌pixel 3L(Android 9)~~

固有误差：需要考虑进测试时手拿手机状态下，手臂的长度



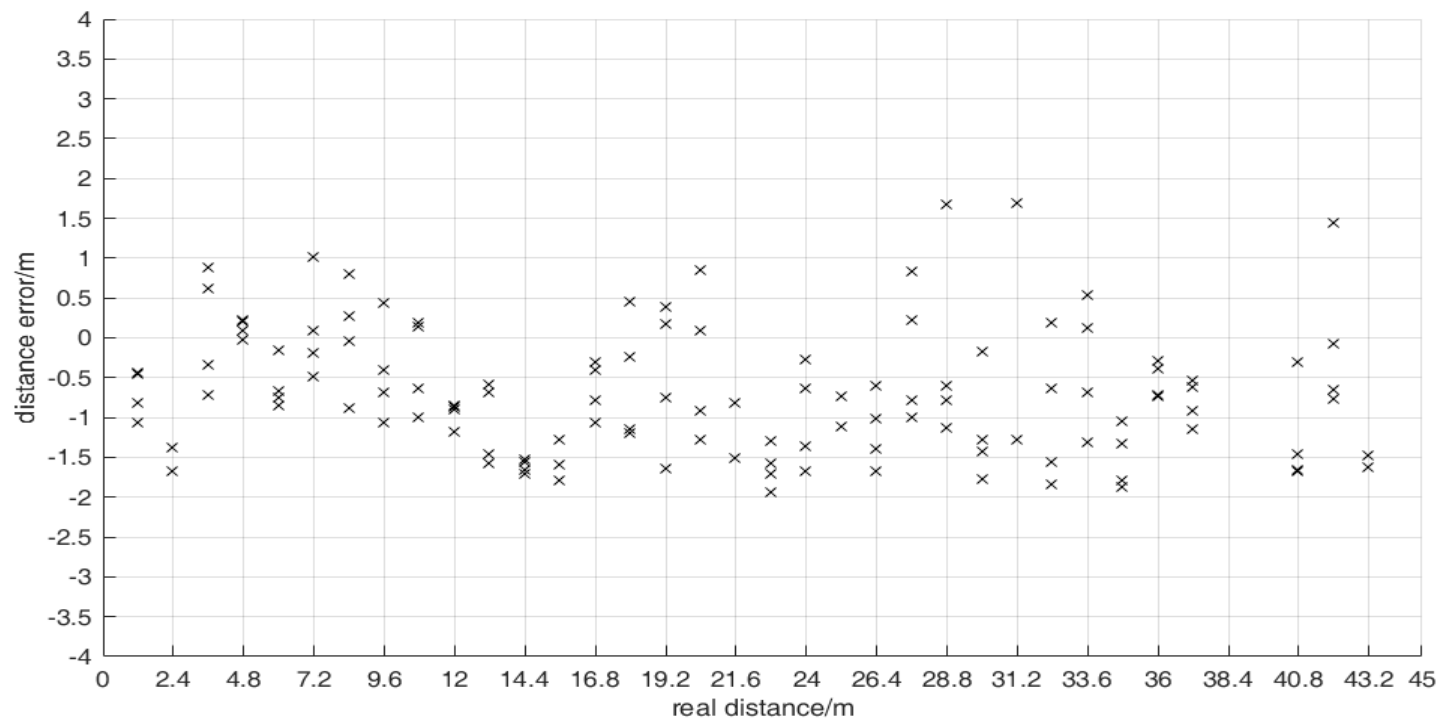


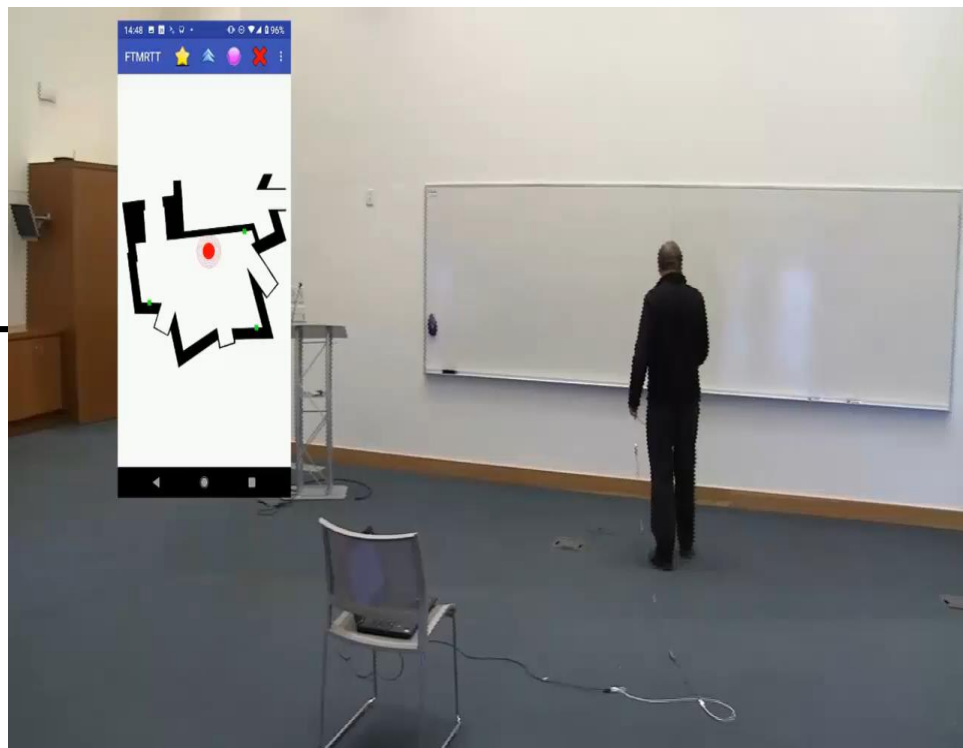
测试距离达44m，  
以1.2m为间隔





考虑手臂长度导致的系统误差，整体结果偏负，故实际测试距离误差在1.5m内。





# BLE定位

- BLE
  - Bluetooth Low Energy/低功耗蓝牙
- BLE的特点
  - 信道少（3个），传统蓝牙有32个，避免相互干扰
  - 开启时间短（毫秒级），功耗低，“完成”一次连接（即扫描其它设备、建立链路、发送数据、认证和结束）只需3ms，传统蓝牙技术需要数百毫秒。
  - 具有深度睡眠模式，该模式下发送数据量少，发送间隔0.5~4s
- BLE基本观测信息
  - 与WiFi RSSI相同



BLE观测信息

# BLE标签

- BLE标签
  - BLE Beacon
  - 对周围播发其标识信息的低功耗蓝牙设备

- iBeacon概况

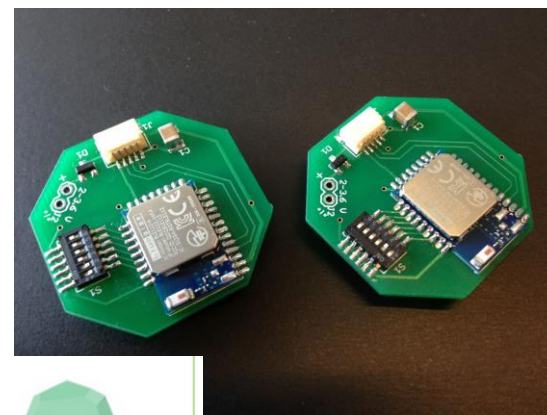
- 苹果公司提出的“一种可以让附近手持电子设备检测到的一种新的低功耗、低成本信号传送器”的一套可用于室内定位系统的协议。
- 2013年9月发布

- 工作方式

- 配备有低功耗蓝牙（BLE）通信功能的设备使用BLE技术向周围发送自己特有的ID，接收到该ID的应用软件会根据该ID采取一些行动。比如：
  - 在店铺里设置iBeacon通信模块，直接或者由服务器向用户发送折扣券及进店积分。
  - 在家电发生故障或停止工作时向应用软件发送信息。

# iBeacon

- iBeacon标签



The Hitchhikers Guide  
to iBeacon Hardware.

A Comprehensive Report by Aislelabs



Accent Systems



April Brother



BlueSense



Estimote



Gimbal Series 10



Gliworm



Kontakt.io



KSTechnologies



Minew



Roximity



Radius Networks



RECO Beacon



RedBear



Sensorberg



SensorTag



Tod

- iBeacon的“通告帧”（Advertising）
  - 定期发送的帧，只要是支持BLE的设备就可以接收到
  - 内容为iBeacon数据
- iBeacon数据由4种信息构成：分别是UUID（通用唯一标识符）、Major、Minor、Measured Power。
  - **UUID**：为ISO/IEC11578:1996标准的128位标识符。
  - **Major**和**Minor**：均为16位的标识符，内容由发布者自行设定。例如，连锁店可在Major中写入区域资讯，可在Minor中写入店铺ID等。在家电中，可用Major表示产品型号，用Minor表示错误代码。
  - **Measured Power**：iBeacon标签与接收器之间相距1m时的RSSI。接收器根据该值及实测RSSI来推算标签与接收器间的距离。



# iBeacon

- iBeacon数据

iBeacon配置

×

设备：jia ibeacon

UUID：FDA50693-A4E2-4FB1-AFCF-C6EB0764782

8-4-4-12格式

Major ID：100500.65535

Minor ID：605700.65535

公共周期：1000ms (100..5000ms,100ms的整数倍)

发射功率：中

设备名称：jia ibeacon16个字符

设备MAC地址：b4:99:4c:3a:18:67

固件版本：Lierda V01.03

在位时间：0分

保存

放弃

20:32

子恒

无服务

详细信息

设备电量

100

>

UUID

FDA50693-A4...

>

MAJOR

10034

>

MINOR

58888

>

校验距离

-59 dBm

>

广播功率

7

>

广播周期

5

>

设备序列号

2059

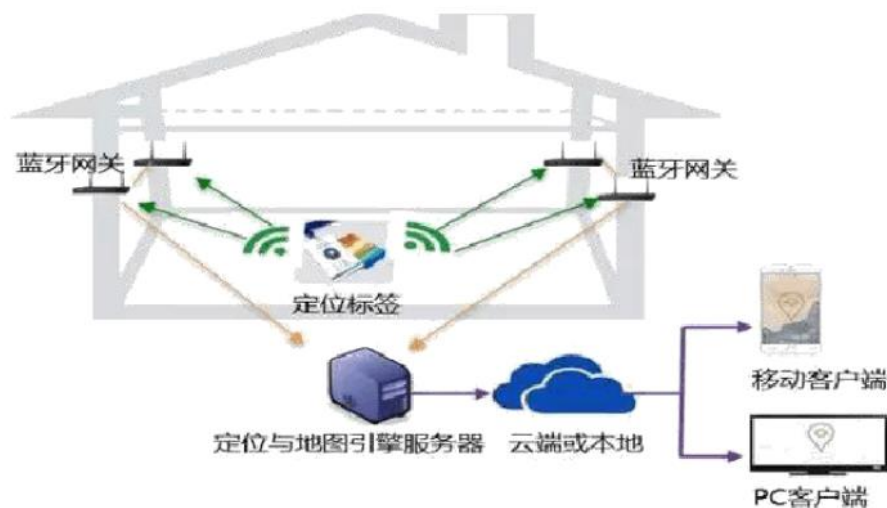
>

# BLE定位

- BLE定位模式

- BLE网关+BLE定位标签

- 定位算法：距离（由传播模型确定）交会，NN，KNN，WKNN等

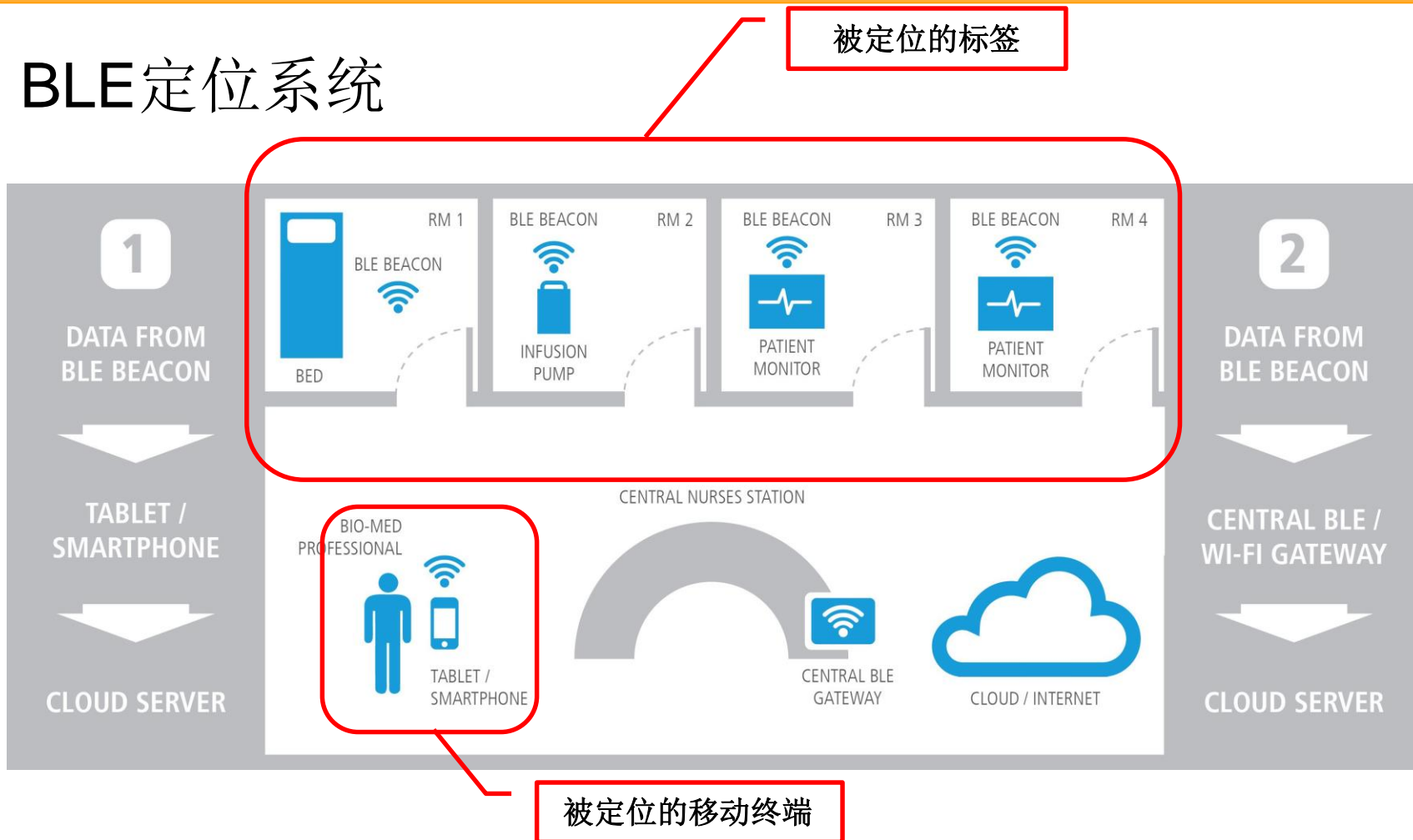


- BLE定位标签+移动终端（支持BLE）

- 此模式中，BLE定位标签相当于WiFi定位中的AP，定位算法与WiFi定位相似。

# BLE定位

- BLE定位系统

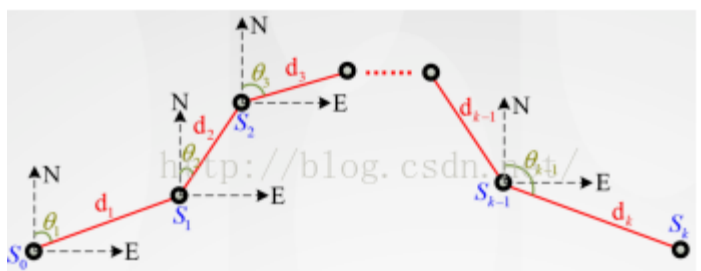


# PDR定位①

- 步行者航位推算（Pedestrian Dead Reckoning, PDR）
  - 使用惯性测量单元(Inertial Measurement Unit, IMU)感知人员在行进过程中的加速度、角速度、磁力和压力等数据，并利用这些数据对行进人员进行步长与方向的推算，从而达到对人员进行定位跟踪的目的。
  - 方向也可采用电子罗盘获取。
- 主要涉及过程
  - 步态检测
  - 步长
  - 方向确定

# PDR定位②

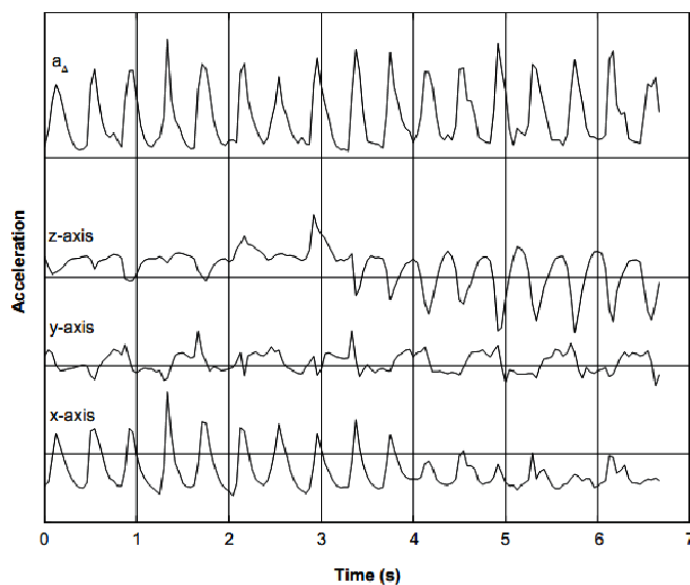
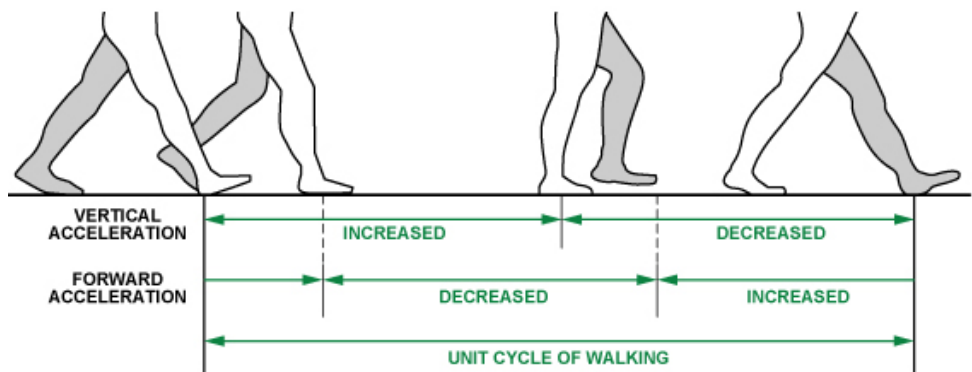
- 定位原理



$$\begin{cases} E_k = E_0 + \sum_{n=1}^k d_n \sin \theta_n \\ N_k = N_0 + \sum_{n=1}^k d_n \cos \theta_n \end{cases}$$

# PDR定位③

- MEMS加速度计计步原理

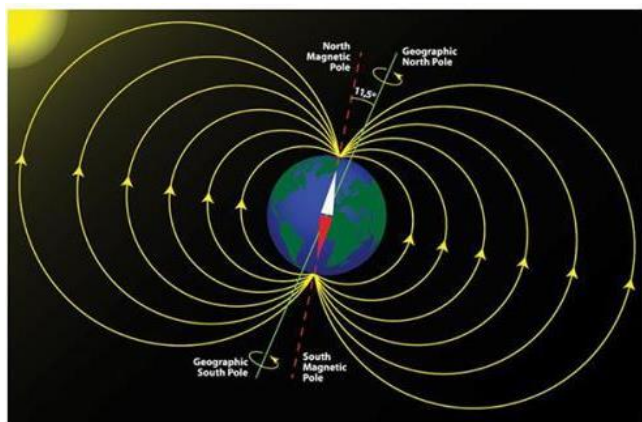


# PDR定位④

- 步长值的确定
  - 近似值：0.5~0.7m
  - 联合其他方法确定，如GNSS定位结果

# 地磁定位①

- 地球磁场



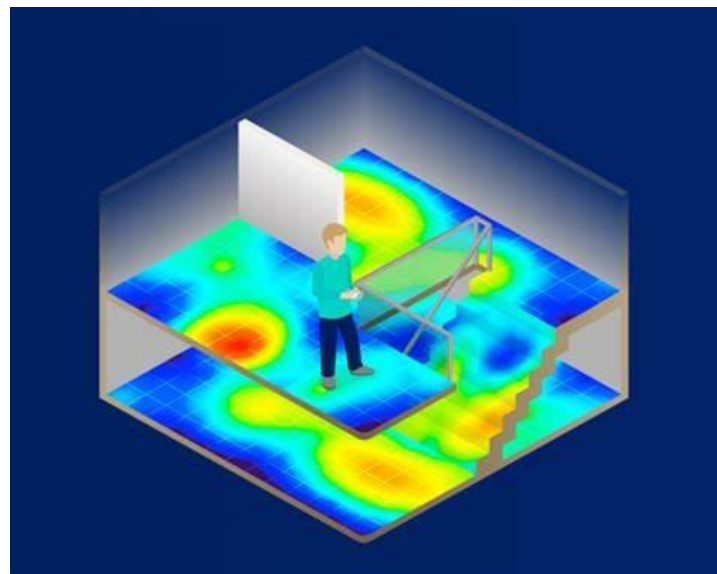
- 室内地磁场扰动

- 地球磁场会受到金属物的干扰，特别是穿过钢筋混凝土结构的建筑物时，原有磁场被建筑材料（金属结构）扰动扭曲，使得每个建筑物内都形成了独特的“磁性纹路”，在室内形成了一种有规律的“室内磁场”。

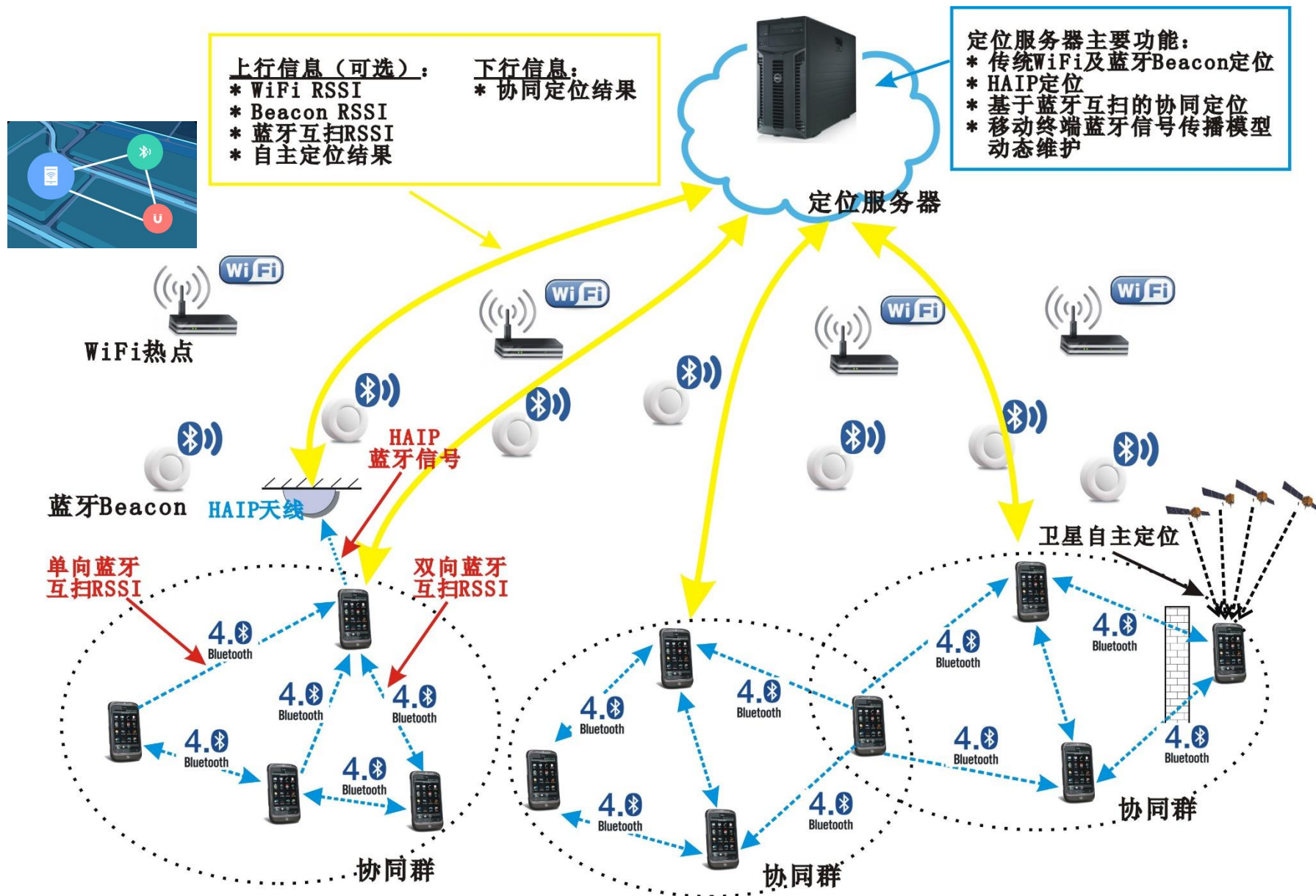


# 地磁定位②

- 室内地磁定位原理
  - 两个阶段：
    - ① 室内地磁场纹理采集
    - ② 地磁匹配
- 地磁匹配的特点
  - 磁场无所不在（优点）
  - 室内地磁场特征随室内环境的变化而变化
  - 易受干扰
  - 匹配无法在一点上进行



# 协同定位



定位服务器主要功能:

- \* 传统WiFi及蓝牙Beacon定位
- \* HAIP定位
- \* 基于蓝牙互扫的协同定位
- \* 移动终端蓝牙信号传播模型动态维护

# 作业

- 写一篇小论文，介绍如何在Android下编程实现WiFi RSSI信息的获取。
- 从下列题目中任选一题，编写完成报告：
  1. 寻找一款可用于采集WiFi RSSI信息的app并学会其使用方法。
  2. 寻找一款可用于采集WiFi及BLE RSSI信息的app。
  3. 编写一个可用于采集BLE RSSI信息的程序。
  4. 编写一个可用于采集WiFi 及BLE RSSI信息的程序。