蓝牙设计

1. 问：什么是蓝牙通信？

答：蓝牙通讯最初设计初衷是方便移动电话（手机）与配件之间进行低成本、低功耗无线通信连接，现在已经成为IEEE802.15标准，得到全球上万家厂商支持。

2. 问：如果从事蓝牙开发有没有前途？

答：严格地说，这不是一个技术问题，而是一个世界观问题。什么是前途？如果单纯是金钱，从事技术是不太可能暴富的（注意比尔.盖茨是个技术商人）；如果想用你所能改善世界，这是可能的，毕竟蓝牙的主要用途是民用。附带说一句，考虑赚钱和改变世界是中国和西方人世界观的主要差别。

3. 问：蓝牙有什么优势？

答：首先是低功耗，以BLE 4.0为例，一节钮扣电池在静态工作状态可以支持一年；其次是低成本，TI公司的CC2540蓝牙SOC方案芯片出售价仅1美元，可以让人们低廉使用蓝牙技术；再次是开放性，2.4GHz的频段全球开放，没有政府监管；最后是适合时代潮流，现在是手机的时代，蓝牙技术本来就为它而生。

4. 问：蓝牙4.0协议和BLE是什么？

答：蓝牙4.0协议是2010年6月由SIG（Special Interest Group）发布的最新标准，它有2种模式：BLE（Bluetooth low energy）只能与4.0协议设备通信，适应节能且仅收发少量数据的设备（如家用电子）；BR/EDR（Basic Rate / Enhanced Data Rate），向下兼容（能与3.0/2.1/2.0通信），适应收发数据较多的设备（如耳机）。

5. 问：目前支持蓝牙4.0的移动设备有哪些？

答：苹果公司的iPhone 4S、iPhone 5、miniPad和iPad 3；小米手机2；三星公司的Galaxy SIII和Note II；HTC ONE系列。

6. 问：如何开始蓝牙4.0的开发呢？

答：概括地讲至少以下三方面的准备吧。硬件方面，需要购买TI公司蓝牙迷你套件，包括蓝牙USB电子狗和KeyFob以及CC Debugger传真器；软件方面，安装IAR for 8051，TI公司BTool软件；技术知识，《CC2540/41 BLE Software Developer’s Guide 1.3》和《CC2540/41 User’s Guide》。

7. 问：刚开始接触蓝牙如何快速上手？

答：理论联系实践是比较好的学习方法，建议先学习《CC2540/41 BLE Software Developer’s Guide 1.3》，然后将SimpleBLEPerepheral工程导入IAR for 8051，结合电子狗和BTool，调试蓝牙通讯中的广播/连接/绑定/访问。光看书不动手，空虚；不看书光动手，浅薄。

8. 问：IAR调试CC2540时程序导入到了芯片的Flash中了吗？

答：确实。CC2540是SOC（System On Chip）芯片，它的内核就是8051，它需要从ROM中取指令，从RAM中取数据来运行。仿真时，CC Debugger会把程序导入芯片Flash中，再执行仿真。

9. 问：当IAR调试中出现警告“缺少断点，无法运行到main()”？

答：出现这个错误的原因是，IAR for 8051最多只能设置3个断点，如果设置过多，当程序下载后，将出现些调试警告。解决的方法很简单，去掉一些断点，再重新载入程序。

10. 问：为什么IAR调试时有很多变量无法查看它的值？

答：主要的原因是IAR编译器设置了优化功能，函数中的自动变量以及一些静态函数都被优化过了，所以没有生成对应的调试信息，无法查看和设置断点。解决的方法是关闭编译器的优化功能，右键点击工程的Options -> C/C++ Compiler -> Optimizations中的Level设置为None。

11. 问：蓝牙协议分层很多且比较复杂，该如何掌握呢？

答：蓝牙协议从应用层到物理层一共分了8层，看上去比较复杂且API函数很多。首先不必要知道每一层的具体实现，掌握与应用紧密关联GAP/GATT（或者GAP Role和GATT Profiles）层就可以满足大部分设计需要；每一层的软件都是通过OSAL来调用的，因此需要了解OSAL的基本原理：任务/事件/消息/定时器/动态分配内存；最后把蓝牙通讯过程理解，将有助于开发。

12. 问：OSAL是一个操作系统吗？

答：OSAL（Operating System Abstraction Layer）操作系统抽象层，它不是一个真正的操作系统（它没有Context Switch上下文切换功能），但它巧妙地组织各任务，支持任务优先级，任务之间可以通过事件和消息来通信，为任务提供软定时器和动态内存分配。要避免的陷阱是，应用任务的单个函数运行时间不能太长（如操作大批量数据的Flash写），否则它无法及时调度高优先级的LL（Link Layer）任务而导致蓝牙通信中断。

13. 问：蓝牙节点是如何组成微微网的呢？

答：蓝牙节点组网中，只能存在一个主节点（Central）和多个从节点（Peripheral），从节点是发出信号者，主节点是扫描且发起连接者。

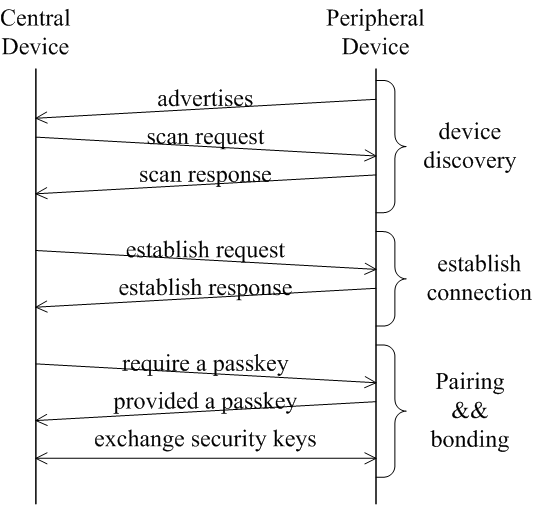
14. 问：主节点和从节点通信的过程是怎样的呢？

答：当从节点发出广告信号（包括设备地址和设备名称之类的附加信息）；主节点收到此广告信号后，向从节点发出扫描请求；当从节点回应扫描时，就完成了设备发现过程。

接着主节点向从节点发出连接请求（包括连接时隙、从节点待机次数、连接超时值），从节点回应连接，就完成了建立连接。

为了安全起见，一些数据的访问需要认证，它的完成是这样的：一方（可以是主节点，也可以是从节点）向另一方索要6位数字的密码，之后，两个节点彼此交换安全密钥用于加密和认证，此过程称为配对。

认证的过程比较繁琐，BLE协议支持两节点保存认证的安全密钥（一般是非易失性存储器中），以便于两节点下次连接后快速认证，这就是绑定技术。



15. 问：蓝牙通信中两个节点如何交换数据？

答：这是蓝牙通信中最让初学者迷惑的地方。大部分通信，尤其是TCP/IP，交换数据的婚介是数据包，但蓝牙通信中，工程师找不到数据包访问方式，于是就产生疑问。其实蓝牙最底层也是基于无线数据包交换，只是通过层层封装，交付给工程师的API接口就变成了Client访问Server的方式。

16. 问：Client和Server节点是如何定义呢？

答：通俗地说吧，Server（服务器）就是数据中心，Client（客户端）就是访问数据者。特别说明，它与主/从设备是独立的概念：一个主设备既可以充当Server，又可以充当Client；从设备亦然。

17. 问：Server是如何提供数据呢？

答：Server首先将一个服务按“属性/句柄/数值/描述”这种格式予以组织，然后调用API函数GATTServApp\_RegisterService将服务数据进行注册。举个实例吧，设提供一个电池电量服务字节，它允许Client读取，数据为一个8比特无符号数（0～100%），它的组织如下：02 25 00 19 2A, 这5个数据（小端格式）分别是：0x02=只读属性，0x0025=句柄；0x2A19=服务UUID。

18. 问：不明白Server提供服务中的UUID？

答：UUID(Universal Unique Identifier)全球惟一标识符，本来是SIC组织分配给特定蓝牙服务的标识，如分配0x2A25为设备序列号的UUID，这样任意蓝牙设备都可以通过它得到另一个设备的序列号。

打个类比，它就像书名，如《现代操作系统》，所有人一看就知道它是计算机大师Andrew S. Tanenbaum写的书。

19. 问：什么是Server提供服务中的句柄呢？

答：句柄(Handle)就是服务数据在数据中心的地址，当所有的服务数据组织起来后，它总得有个先后顺序，某个服务的位置就是它的句柄。还是上面的类比，如果想去图书馆借阅《现代操作系统》，需要查明该书在哪一层楼，哪个房间，这就是该书的Hanle。

20. 问：为什么Server提供的服务中有描述？

答：有些服务是有描述（Descriptor）的，它是用于Client配置该服务的功能（通知或者显示）。像某人没有借到《现代操作系统》该书（可能是被别人借光了），他（她）可以打个电话给图书馆工作人员，请求一旦该书可以借阅了给他一个通知，这个过程相当于配置该书的Descriptor。

21. 问：服务的属性与描述有区别吗？

答：有区别，服务的属性是Server设置访问权限。就像图书馆的工作人员可以设置《现代操作系统》仅能在阅览室看不能外借（只读），或者即可以看也可以外借（读/写）。

22. 问：Client如何访问Server的服务呢？

答：大致分三类：读取服务的值，需要知道服务的UUID或者Handle；写服务的值，需要知道服务的Hanle；写服务描述符，需要知道该Descriptor的Hanle。

23. 问：如何知道一个服务的Handle？

答：根据服务的UUID调用API函数GATT\_ReadUsingCharUUID

协议栈会返回该服务的Handle。特别注意的是，一个服务的Descriptor的Handle总是该服务的Handle+1，如电池电量服务的Handle是0x0025，那么它的Descriptor的Handle是0x0026。

24. 问：Server可以访问Client吗？

答：蓝牙通信中，Server不能直接访问（读/写）Client，但是可以通知（Notification）Client，通知的前提是Client通过写Descriptor使能通知功能。例如，某Server发现电池电量已经低于安全阀值，它可以调用GATT\_Notification通知所有已连接的Client，但是Client接收后如果处理是它自己的事情。

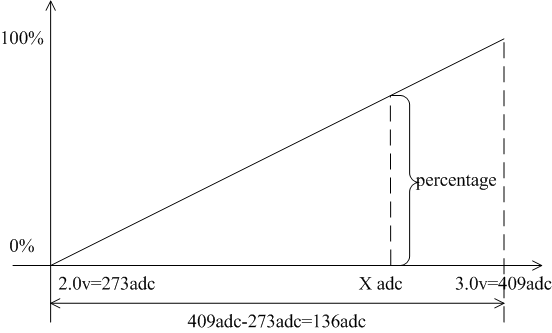
25. 问：如果得知电池容量？

答：任何使用电池供电的设备都必须精确监控电池容量，否则设备可以突然断电而停止工作，它的基本原理是通过ADC（模数转换器）计算电池电压。以CC2540芯片用一钮扣电池为例，电池电压从2.0v～3.0v，即电量的0%～100%；CC2540有一10比特的ADC，量程范围为0～511，参考电压为1.25v，最大测量电压为3.75v，以上信息可以得知：（v/3）/ 1.25 \* 511 = adc，则2.0v=273adc，3.0v=409adc，根据下图可以很容易得知ADC转换为电压的公式：

Percentage / (X – 273) = 100 / 136 = 25 / 34，变换后为：

Percentage = (X - 273) \* 25 / 34，为四舍五入提高计算精度则有：

Percentage = [(X - 273) \* 25 + 33] / 34。



26. 问：蓝牙发射信号功率调整会影响通信距离吗？

答：会，以TI公司的CC2540为例，它支持4种发射功率选择：4dBm、0dBm、-6dBm和-23dBm，按无线电功率定义：LdBm=10lg(Pwr/1mW)，以上4种分贝值换算成瓦特为：2.51mW、1mW、0.251mW和0.005mW，有效通信距离分别为：30米、10米、7米和3米。

27. 问：如何知道两个蓝牙通信节点之间的距离？

答：要知道蓝牙通信节点（如手机和蓝牙设备）之间的距离，最容易实现的方法是通过读取接收RSSI（Received Signal Strength

Indication）值来计算。无线通讯中功率与距离的关系如下：

http://img.blog.csdn.net/20130531170524272 其中A可以看作是信号传输1米远时接收信号的功率，n是传播因子（它受障碍，温度和湿度等影响），r是节点之间的距离。当确定了常数A与n的值后，距离r就可以根据PR(dBm)计算出来。

28. 问：如何获取蓝牙节点的接收RSSI值？

答：具体的设备接收RSSI值的方法不一样，以iPhone手机为例，iOS提供API函数获取RSSI值；TI公司的CC2540芯片的BLE协议栈中，首先将读取RSSI值回调函数挂载到gapRolesRssiRead\_t类型的指针下，建立连接后，主设备调用GAPCentralRole\_StartRssi（），从设备调用

GAPRole\_SetParameter(GAPROLE\_RSSI\_READ\_RATE, ……)。这样就可以定时读取接收的RSSI值了。

29. 问：如何开展读取RSSI值的实验？

答：读取RSSI值的实验可以这样搭建，主设备固定位置，向从设备发送信号，从设备LED光和Buzzer报警为通信成功，逐次移动从设备，而获取RSSI值随物理距离之间的关系。下图是笔者做实验的数据：

Distance(m)

1

2

3

4

5

6

7

8

9

10

RSSI(dBm)

-47

-59

-73

-80

-80

-79

-85

-88

-86

-87

Loss(p)

0

0

9

11

27

2

50

32

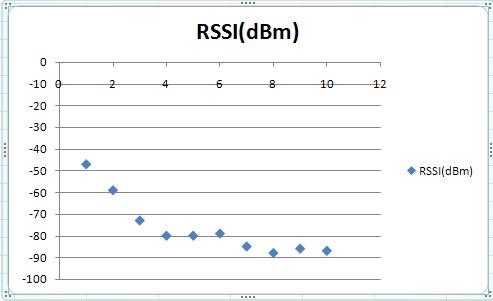
22

49

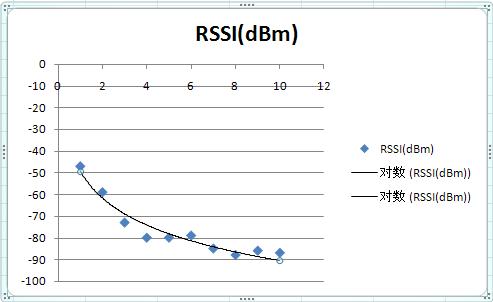
实验器材为2块CC2540芯片，主芯片发射功率为4dBm(2.51mW)，Loss是通信节点中失败次数。

30. 问：如何将接收RSSI实验数据得到距离计算公式呢？

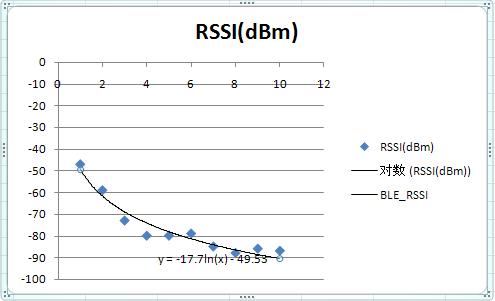
答：最好的工具是EXCEL软件，以上表中的实验数据和EXCEL 2007为例。首先选中Distance和RSSI两行，点击“插入->散列图”，软件会自动生成如下图：



选取其中任意点，点右键，“添加趋势线->对数”，将会出现下图：



可见RSSI与距离的关系是比较符合指数函数，再点击“显示公式”



此时得到指数函数公式为：y = -49.53 – 17.7 ln (x)，再把自然对数换成10常用对数，则有：y = -49.53 – 40.71 lg (x)。通过以上几步就轻松得到RSSI与距离之间的计算公式。