

蓝牙系统中适配层程序的设计与实现

Design and Realization of Adaptation Protocol in Bluetooth

彭春华 蒋新华 (中南大学 信息科学与工程学院 湖南 长沙 410075)

摘要: 为实现蓝牙系统中低层传输协议和高层传输协议数据分组的匹配, 论文利用 Dephi 提出了对上下层数据进行分段与重组的算法, 实现了上下层数据的交互。实验表明, 论文提出的算法实现了逻辑链路控制与适配协议对数据的拆包与解包。

关键词: 蓝牙 逻辑链路控制与适配层 分段 重组

在蓝牙系统中, 蓝牙协议规范遵循开放互连参考模型 (OSI), 其对应的 OSI 协议如图 1 所示。按照蓝牙协议的逻辑功能, 协议堆栈可分为三个部分: 传输协议、中介协议和应用协议^[1,2]。

应用协议是位于蓝牙协议堆栈之上的应用软件及协议; 中介协议为高层应用协议在蓝牙逻辑链路上工作提供支持, 包括串口仿真协议、服务发现协议、电话控制协议等;

传输协议负责蓝牙设备间相互确认对方的位置, 以及建立和管理蓝牙设备的物理和逻辑链路。它可分为低层和高层传输协议, 低层传输协议包括射频 (Radio)、基带与链路控制器 (Baseband & Link Controller) 和链路管理协议 (Link Manager Protocol, LMP), 侧重于语音与数据无线传输的物理实现以及蓝牙设备间的连接与组网。高层传输协议包括逻辑链路控制与适配层协议 (Logical Link Control and Adaptation Protocol, L2CAP) 和主机控制接口 (Host Controller Interface, HCI), 它为高层应用程序屏蔽了低层传输操作, 为高层应用程序提供更加有效的数据分组格式。

在实际应用中, 低层传输协议的功能集成在蓝牙模块中, 对于面向高层协议应用的开发人员来讲, 并不需要知道低层协议细节。同时, 基带层数据分组长度较短, 而高层协议一般使用较大的数据分组, 二者很难匹配。因此, 需要一个适配层来为高层和低层协议之间不同长度的 PDU (协议数据单元) 的传输建立一座桥梁。本文主要讨论适配层协议的设计与实现。

1 逻辑链路控制与适配层协议 (L2CAP)

1.1 L2CAP 功能^[3]

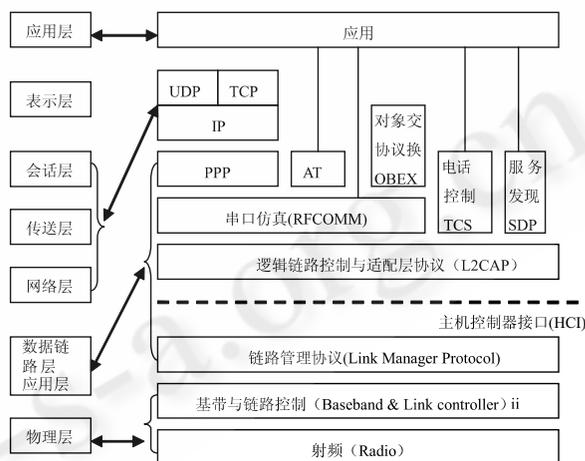


图 1 蓝牙协议栈结构图

L2CAP 层只支持 ACL (异步无连接) 的数据传输, 不支持 SCO (同步面向连接) 数据传输。L2CAP 允许上层协议和应用传输最大为 64KB 的数据分组 (L2CAP_PDU)。L2CAP_PDU 到达基带层之后被分段, 并由基带数据分组 (ACL BB_PDU) 传送。L2CAP 的主要功能包括:

a. 协议复用。因为蓝牙基带协议不能识别所有类型的上层协议, L2CAP 必须能够区分串口仿真协议 (RFCOMM)、服务发现协议 (SDP)、电话控制协议 (TCS) 等。

b. 分段与重组。L2CAP 层本身并不完成任何的

PDU 的分段与重组,具体的分段与重组由低层和高层完成。一方面,L2CAP 层在其数据分组中提供 L2CAP_PDU 的长度信息,使其在通过低层传输后,重组机制能检查出是否进行了正确的重组;另一方面,L2CAP 层将其最大分组长度通知高层协议,高层协议对数据分段后,其长度不能超过 L2CAP 层的最大分组长度。

c. 服务质量。L2CAP 连接建立过程允许交换服务质量 (QoS) 信息。因此每个蓝牙节点必须进行资源的监视,以便向协议提供可靠的 QoS 信息。

d. 组抽象。很多协议包括地址组 (a group of addresses) 的概念。L2CAP 层通过向高层协议提供组抽象,有效地将高层协议映射到基带的微微网 (Piconet) 上,而不必让基带和链路管理器直接与高层协议打交道。

1.2 L2CAP 对数据分段与重组

a. 分段过程。L2CAP_PDU 在传送到低层协议时将被分段,如果直接位于基带层之上,则分段为基带数据分组 (BB_PDU),再进行传输;如果位于 HCI 层之上,则被分段为数据块,并送到主机控制器,再转化为 BB_PDU^[4]。

b. 重组过程。基带可以在每收到一个基带分组时都通知 L2CAP 层,也可以累积到一定数量的分组时再通知 L2CAP。

2 逻辑链路控制与适配协议的设计

下面以南京东大移动互联技术有限公司的 TTP6600 系列蓝牙产品为例,说明适配层程序的设计。

在 TTP6600 系列产品中,其高层传输协议的最大传输单元 (Maximum Transmission Uni, MTU) 只有 250 个字节,所以上层应用程序如果要一次传输更长的数据包,需要进行数据分段与重组^[5]。

本设计中的数据分段与重组方法基于蓝牙协议:将每一个对象交换协议 (Object Exchange Protocol, OBEX) 待传输的数据包拆分成长度小于 250 字节的包,最后一个包的包头添加 80,其它包的包头添加 00 (也就是每个包最多 249 个字节的数据域)。如果数据包的本身长度小于 249 字节,包头则添加 80,然后把这些分组依次发送。接收端收到的第一个字节是 00 的分组就等待,待后续的分组添加在后面 (去掉 00),直到等到的第一个字节是 80 的分组,然后将整个

PDU (协议数据单元) 提交给上层。

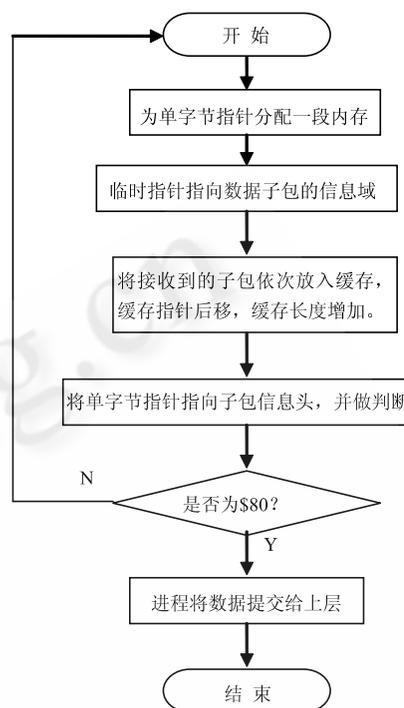


图 2 L2CAP 数据重组流程

数据分段与重组的函数设计关键在于各个指针的定义及调用。以数据重组为例,首先,由发送端分包后的数据包子包通过蓝牙硬件模块传送到接收端,应对这些数据包进行处理^[6],此处就有低层传来的数据包指针 Pk_Pointer;其次,去掉信息头的数据包先是依次放入缓存区,直到接收到最后一个数据包,再提交到上层,即要用到缓存区指针 Buf_Temp;再次,为了方便对接收到的数据包的信息头字节进行分析,则应在程序中定义一个单字节指针 PByte。若 PByte = \$00,进程等待;若 PByte = \$80,说明是最后一个包,此时可以将已处理的数据提交到上层。其程序流程如图 2 所示。

在 Delphi 开发环境下,数据重组函数的主体程序如下:

```

Temp_Pointer := ptr(Integer(Pk_Pointer) + 1); //
临时指针指向信息域
move(Temp_Pointer~, Buf_Temp~, Pk_Length -
1); //将信息域内容复制到缓存
Buf_Temp := ptr(Integer(Buf_Temp) + Pk_Length
- 1

```

```

); //缓存指针后移
Buf_Length := Buf_Length + Pk_Length - 1; //缓存
长度增加
move( Pk_Pointer^, PByte^, 1); //将信息头内容赋
给单字节指针
if( PByte^ = $ 00) then
begin
result := False;
end; //进行判断,若信息头为 $ 00,则返回 False
if( PByte^ = $ 80) then
begin
result := True;
end; //若信息头为 $ 80,则返回 True

```

参考文献

- 1 徐平平,陈小硕,施荣. 蓝牙无线接入速率分析与测试. 计算机工程,2005,31(4):131-132
- 2 金纯. 蓝牙协议及其源代码分析. 北京:国防工业出版社,2006.
- 3 马建仓,等. 蓝牙核心技术及应用. 北京:科学出版社,2003.
- 4 马兴,梁剑,陈前斌. 基于 HCI 协议层的蓝牙技术应用开发. 重庆邮电学院学报,2002,14(4):78-82.
- 5 沈连丰. 通信信技术及其实验. 北京:科学出版社,2003.
- 6 杨瑞. 蓝牙通信在 Windows Mobile 移动终端中的研究与实现. 计算机系统应用,2007,16(3):59-62.

3 设计结果分析

包序号	方向	hex	长度	说明	备注
239	收到	0x50 0x03	1 2	OpCode域 长度域	Continue响应包
240	发出	0x52 0x03A 0x49 0x0197	1 2 1 2 404	OpCode域 长度域 HI 信息头长度 End-Of-Body包含的上层应用程序	Fin包(最后一个) End-Of-Body信息头
241	收到	0x40 0x03	1 2	OpCode域 长度域	Success响应包
242	发出	0x51 0x03	1 2	OpCode域 长度域	DisConnect Request包
243	收到	0x40 0x03	1 2	OpCode域 长度域	Success响应包

图 3 会话层连接的包流程

图 3 是进行文件传输后,会话层连接的实际包流程,图中描述了会话层详细的帧格式以及发出/接收帧的状态。从图 3 的包流程中可以看出,适配层实现了对上下层数据的分段与重组。

4 结束语

本设计中适配层对数据分段与重组的程序设计是基于蓝牙协议的,具有实现方法简单,冗余与数据内容无关等优点。通过实验证明,数据分段与重组函数能够对高层和低层数据进行准确拆包与组包。

(上接第 65 页)

参考文献

- 1 Braden B, Clark D. Recommendation on queue management and congestion avoidance in the internet. Request for Comments (RFC) 2309. <http://www.ietf.org/rfc>, 2003-02-15.
- 2 Floyd S, Jacobson V. Random early detection gateways for congestion avoidance. IEEE/ACM Transaction on Networking. August 1993, 1(4):397-413.
- 3 Floyd Sally. Recommendation on using the "gentle_" variant of RED. <http://www.icir.org/floyd/red/gentle.html>.
- 4 UCN/LBL/VINT. Network Simulator - NS2. <http://www-mash.cs.berkeley.edu/ns>.
- 5 Thompson K, Miller GJ, Wilder R. Wide Area Internet Traffic Patterns and Characteristics. IEEE Network, 1997, 11(6):10-23.
- 6 Floyd S. RED: Discussions of Setting Parameters. <http://www.icir.org/floyd/REDparameters.txt>, November 1997.