

基于“蓝牙”的 IP 业务

Research of IP Services over Bluetooth

蒙移发 徐惠民 高 强

(北京邮电大学 北京 100876)(中国科学院软件所 北京 100080)

Abstract The concept of IP over Bluetooth presented in our paper based on Bluetooth protocol, combines Mobile IP with Cellular IP technology, inherits all aspects of IP, in order to meet new needs of IP Services. This paper introduces Bluetooth protocol and the network framework, routing protocol handoff support and security mechanism of Bluetooth IP, finally brings forward the further work about Bluetooth IP research.

Keywords Bluetooth, IP service, Mobile IP, Cellular IP, Network framework, Routing protocol, Security mechanism

一 问题的提出

伴随着 IP 技术在信息产业中作用的不断增大,传统 IP 技术的局限性与人们对 IP 业务新需求的矛盾也日益突出,具体表现为:传统 IP 不能实现主机漫游,主机进入与原来子网不同的子网时,IP 地址必须改变,这将使其原先的通信伙伴无法再找到它,C. Perkins 提出的移动 IP 方案可解决这一矛盾,未来的 IPv6 将支持移动 IP。各终端设备依靠线缆连接,使其携带极为不便,WAP 和 Cellular IP 在一定程度上解决了这一矛盾,但因某些特殊场合(如飞机上)的限制和不经济性(移动话费太高),也不全尽人意,本文介绍的蓝牙 IP,将满足人们如下移动新需求:(1)借助蓝牙技术,克服线缆限制;(2)在用户移动不大的场合(如飞机上),结合移动 IP 技术,实现主机漫游;(3)在用户移动频繁的场合(如办公区,超级市场,火车站),结合移动 IP 和 Cellular IP 技术,实现移动主机漫游;(4)用户可根据需求获取局域网信息或互连网信息;(5)由蓝牙技术的特点,蓝牙 IP 对环境保护和节约开支都有好的效果。

蓝牙技术由 Ericsson 公司于 1994 年首先提出,1998 年 5 月联合 Intel, Nokia, Toshiba 和 IBM 等公司成立了一个蓝牙特殊兴趣小组(Bluetooth SIG),并对蓝牙协议作了规范。作为一种新的无线通信技术,其主要特点是:(1)做成的硬件是一个 0.5 平方英寸的低成本,低功率的收发芯片;(2)蓝牙模块价格便宜,可望达到每个五美元;(3)通信距离在 10 米内,也可增加功率扩展到 100 米;(4)采用 2.4GHz 的免费频段。利用蓝

牙技术,不需任何附加硬件设备和线缆,手提设备可建立一个无线网,一般叫 piconet,每个 piconet 由一个主设备(master)和最多七个从属设备(slave)组成,从属设备的时钟和跳频与主设备同步。主从之间支持面向连接的同步链路(SCO)和面向无连接的异步链路(ACL)两种方式,SCO 主要用于声音等实时数据传输,而 ACL 主要用于分组数据传输。蓝牙协议栈分层结构如图 1 所示。

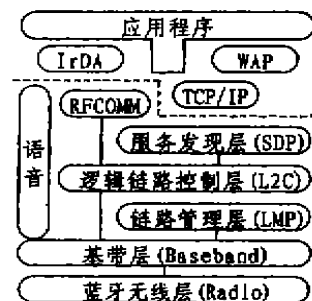


图 1

牙无线层主要负责调制位流的接收与发送,基带层负责时延,帧和分组的定义,信道和链路控制,位流控制和位流处理(加密,纠错等),链路管理层负责链路建立,安全和控制,以及连接状态管理和电源的管理,逻辑链路控制层主要负责数据的分段,重组和信道的多路复用,该层可看作是链路管理层并行工作的,不同之处在于该层为上层提供服务,而载荷数据从不以 LMP 消息发送;RFCOMM 层负责串行线路仿真,

蒙移发 博士研究生,徐惠民 教授,博士生导师,高 强 研究员。

为上层业务提供传输功能;服务发现层(SDP)发现哪些设备提供何种服务,之后,可建立蓝牙设备间的连接。

由协议栈分层结构图可见蓝牙协议主要定义了物理层需求和链路层功能(相当于 OSI 的第一、二层),如果把它与现有网络协议(如网络层(TCP/IP, WAP, IrDA)和应用层)结合在一起,可形成一个完整的通信协议体,这样,各蓝牙设备之间可相互通信,借助于 LAN, GSM, PSTN 和 Internet 等技术可实现远程通信。

二 蓝牙 IP 业务

2.1 网络结构

蓝牙 IP 的网络结构,从协议分层的观点看如图 2 所示。

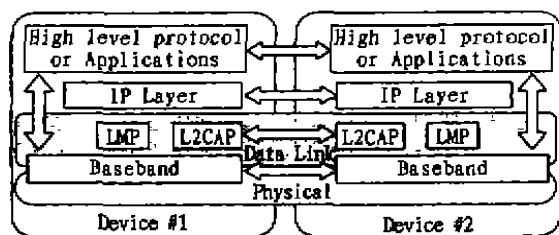


图 2

IP 层以下的协议是蓝牙协议,因此我们把这种基于蓝牙技术基础上的 IP 业务叫蓝牙 IP;从业务范围看,有图 3,图 4,图 5,图 6 所示几种情况。图中符号的含义为:BT—蓝牙设备(Bluetooth Device),BTC—蓝牙无线小区(Bluetooth Piconet Cell),BBS—蓝牙基站(Bluetooth Base Station),GW—网关(Gateway),AS—应用服务器(Application Server),HBTA—本地代理(Home BT Agent),BTA—蓝牙代理(Bluetooth Agent 相当于外部代理 Foreign Agent),BT-LAN—蓝牙局域网。

图 3 说明的是由一个蓝牙主设备和最多七个从设备组成的个人特别网,网络中各蓝牙设备可相互通信。图 4 说明的是蓝牙设备存取局域网业务,或通过局域网彼此间通信。

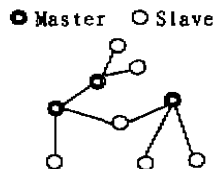


图 3

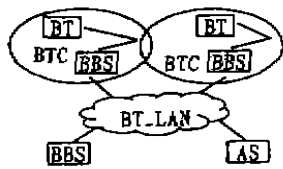


图 4

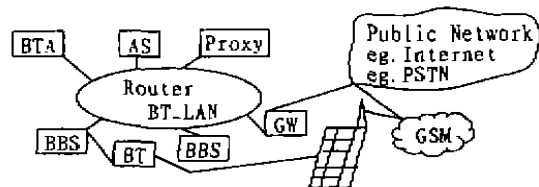


图 5

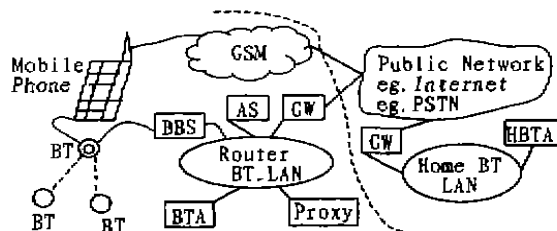


图 6

图 5 说明的是蓝牙设备存取 Internet 业务,或通过 Internet, PSTN, GSM, CDMA 等公众网络相互通信。图 6 是图 3→图 5 三种情况的综合。

组成蓝牙 IP 网络的基本构件有:蓝牙设备,蓝牙基站,路由器,蓝牙代理,局域网,应用服务器,Internet 代理服务器,网关,移动电话等。蓝牙 IP 网络互连分为两个步骤:(1)piconet 内部各设备互连,可通过蓝牙协议的无线,基带,链路管理器和逻辑链路与应用适配层实现;(2)蓝牙设备与 LAN 和公用网络(Public Network)设备互连和中间经由 LAN 和公用网络的蓝牙设备间的互连,通过蓝牙 IP 实现。

2.2 IP 路由

蓝牙 IP 的路由协议分三种情况实现:(1)蓝牙设备不离开本地子网(Home Network)时,路由协议与传统路由协议一致;(2)蓝牙设备与有线网络的接入点是静态接入时,路由协议与移动 IP 的路由协议一致;(3)蓝牙设备与有线网络是通过基站动态接入(蓝牙设备的移动性大)时,与蜂窝 IP 的路由协议一致。

两种路由协议的共同点是基本步骤一致,即代理发现,注册,封装隧道,如图 7。

具体过程如下:蓝牙设备到达一个蓝牙局部网络时,监听蓝牙代理广播信息包或主动请求广播信息包,看是否进入一个新的蓝牙局域网 BT-LAN,如果是, BT 通过请求/监听 BTA 的广播信息包或 DHCP 获得一个转交地址(COA),该地址为 BTA 地址或 DHCP 分配的临时地址;随后 BTA 帮助 BT 将 COA 注册到 HBTA (BT 的 IP 地址原来所在的网络),HBTA 将 COA 绑定,任何发往 BT 的数据包被 HBTA 截获,HBTA 将数据包作隧道封装发往 COA (BTA 或 BT 本

身);相反,BT发送的数据包与普通IP路由一致,不需要通过HBTA。这里存在三角路由问题,解决此问题的办法是HBTA把BT的地址和COA绑定,欲向BT发数据的结点(CN),先向HBTA绑定预告消息,HBTA将BT的COA及数据报封装方法告知它则可得到解决。

不同之点在于:蜂窝IP的路由段为:BT—BBS—Router—BTA—GW—Public Network。Router至少有两个接口,一个与BTA连,其它的与BBS连,BBS有两个接口,一个与有线网连,另一个与无线网连;BT是通过BBS的信标信号确定它应通过哪个BBS与有线网连接。在蜂窝IP中,每个结点都有一个路由缓冲区,将BT的IP地址(COA)映射成通向BT的接口,从BT发出的数据包就是靠路由缓冲区中的映射链选择路由的,映射链是有生命周期的,当BT从一个BBS到另一个BBS时,如果旧的映射链尚未超时,则新的映射链将与旧的映射链并存,从BT发出的数据包将有两条路由,而移动IP路由段为:BT—BTA—HBTA,无蜂窝IP的映射链。

2.3 平滑处理

无论移动IP还是蜂窝IP都存在平滑过渡问题。移动IP的平滑过渡问题是因为与BT通信的每个BT不能及时收到BT的地址绑定更新信息,当BT从一个子网进入另一个子网时,网络上可能有以BT为目的的分组。解决这一问题的办法是各BTA之间相互协作(如图8),本地BTA向前次BTA(BT进入当前子网前所在子网的BTA)发送一个地址绑定信息(a),通知前次BTA把存储的信息转发过来。如果前次BTA不能知道BT的当前位置,则把到达的分组发回HBTA,再由HBTA转发给BT(b,c)。

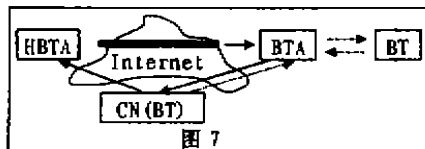


图 7

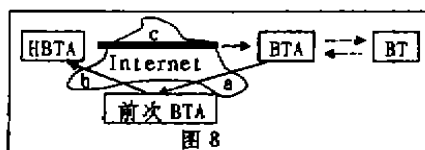


图 8

蜂窝IP的平滑过渡问题是当BT从一个小区移到另一个小区时,连接不能中断,解决的办法是,当BT没有数据发送时也发送不带数据的链路控制包以便新的映射链路更新路由缓冲区,直到旧的路由(映射链)被删除。

三 蓝牙 IP 安全机制

蓝牙IP安全机制主要包括三个层次:(1)HBTA与BT,BTA与BT,HBTA与BTA,CN(通信结点,Corresponding Node)与HBTA之间的相互认证;(2)BT与BT之间的相互认证;(3)数据加密。

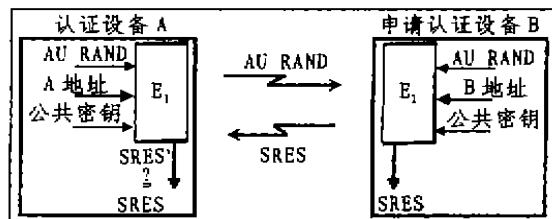


图 9

蓝牙设备(或通信结点CN)与代理之间及代理与代理之间的相互认证办法是在注册请求和注册响应的报文中增加认证扩展(Authentication extension,包括设备地址,随机数,密钥等),认证算法可参考使用MD5^[5];BT与BT之间的认证办法是:认证设备向申请认证设备发送一个PDU(包含一个随机数AU-RAND),两边根据算法E1(如图9)以各自设备地址,随机数AU-RAND,公共密钥为参数计算出结果SRES'和SRES,申请认证设备将SRES返回认证设备,认证设备判断SRES'和SRES是否相等而决定认证是否通过。

数据加密由硬件实现,首先协商好加密模式,密钥大小,然后根据算法E3算出密钥Kc和算法E0加密^[3]。

四 下一步工作

蓝牙IP建立在蓝牙协议的基础上,结合移动IP和蜂窝IP技术,给人们提供了更加方便的IP业务,有着较好的商业前景。对蓝牙IP的下一步工作是,制定出该技术的规范并实现它,对安全机制作进一步的研究,使之更加完善。

参考文献

- 1 Bluetooth SIG. Specification of the Bluetooth System Version1.0b, Specification Volume1&2 Dec. 1999
- 2 Perkins C. Mobile IP. Oct. 1996
- 3 Valko A G. Cellular IP—A New Approach to Internet Host Mobility. ACM Computer Communication Review. January 1999
- 4 吴靖编. 宽带通信网讲义(修订本). TCP/IP与Internet IP over ATM