基于组播和 P2P 的文件分发管理模块的设计与实现*)

满 萍 马 严

(北京邮电大学信息网络中心 北京 100876)

摘 要 本文对CNGI研究课题"组播与P2P相结合的文件分发系统"进行了简要介绍。通过对该系统文件管理模块的总体设计和详细设计,实现了基于IPv6组播与P2P技术的结合。该系统借助JXTA平台实现P2P的基本功能:节点搜索、节点资源搜索、节点间的通讯和文件的统一管理等,实现了尽量利用可靠的组播并利用P2P实现跨组播域的信息传输。最后通过对管理模块在不同环境下的测试数据进行分析,表明该设计思想的有效性。

关键词 P2P,IPv6,JXTA,文件管理

Design and Implementation of File Distribution Management Module Based on Multicast and P2P

MAN Ping MA Yan

(Network Information Center, Beijing University of Posts and Telecommunication, Beijing 100876)

Abstract This paper introduces a CNGI research project "A File Distributing System by The Cooperation of IP Multicast and P2P". Through careful design of the file management module of the system, a combined function of IPv6 multicast and P2P fulfilled can be realized. By using the JXTA P2P platform, the system implements the basic functions of node searching, node resource searching, communication among nodes and unified file management. The system uses the multicast function if it is available, then P2P function is used to deliver information across multicast domain. The final part of this paper reveals the successful design of the file management module by analyzing the test results in different environment.

Keywords P2P, IPv6, JXTA, File management

1 引言

本课题作为"CNGI大规模路由和组播研究实验"的子项目,主要目的是验证IPv6环境下的P2P可行性及性能、大规模IPv6组播的性能,以及在IPv4和IPv6组播下组播性能的对比。因此,设计和实现"组播和P2P相结合的文件分发系统"是本项目的主要内容,性能比对测试是本项目的目的。

本课题的创新点是IPv6组播与P2P技术的结合,即利用P2P实现可靠的组播和跨域的组播。一方面利用IP层的组播技术解决应用层服务的一些缺陷,有效地利用网络资源;另一方面提出并实现一个可控、可管的P2P文件分发应用系统,对实现P2P应用的可控制性、可管理性进行有益的尝试。

2 模块的总体设计

2.1 系统总览

如图1所示,系统把整个应用分为八大模块。

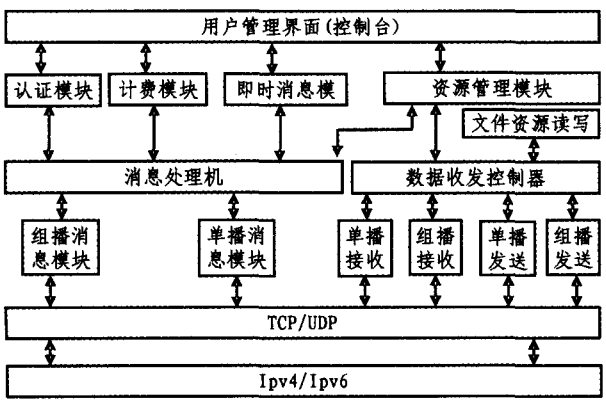

图1 系统体系结构

下面简要介绍这八大模块的主要功能。

(1)消息处理模块:它包括系统消息的组播单播接收发送模块,以及消息处理机。

(2)数据处理模块:包括组播、单播接收和发送模块,以及一个数据收发控制器。

(3)文件资源读写模块:主要是对文件的读写操作。

(4)认证模块:主要是检测用户的合法性,跟后台数据库还有一定的联系,可能要对数据库有查询、更新等操作。

(5)计费模块:该模块目前只作为一个接口存在,以便日后方便扩展,同时还可以跟认证模块联系起来,比如说AAA认证。

(6)资源管理模块:该模块由作者负责,后文会有详细介绍。

(7)即时消息模块:它的任务就是处理一些即时消息,如对等体(Peer)用户间的聊天信息,还有一些广播型消息,如天气预报等。

(8)用户管理界面:是人机的接口,主要提供给用户一个可视的友好界面[1]。

2.2 管理模块基本功能介绍

本模块也是本系统的关键模块,系统的可管理性就在本模块集中体现。主要功能是记录并管理网络共享资源,维护网络拓扑,发现和探测网络资源等,同时留有网管接口,以便本系统日后扩展。

P2P资源管理功能。这一功能计划分以下几个步骤:

(1)首先实现子网内部对等组、对等点和管道的发现,并实现子网内对等点之间的通信;

(2)实现跨子网的对等组、对等点和管道的发现,实现跨子网的对等点之间的通信;

*)由国拨资金[CNGI-04-13-2T]和北京邮电大学自筹资金支持。满 萍 硕士研究生;马 严 教授。

(3)实现完整的 P2P 资源管理功能。

2.3 管理模块总体设计

P2P 通信模块用于数据模块启动前应用系统的配置和文件信息的传送。只通过 P2P 通信,才能接收到其它 Peer 的配置参数,才能把自己的配置参数公布在 JXTA 网络上。

在此应用中,Peer 可分为三种:文件源 Peer(Source Peer)、接收 Peer(Receive Peer)、代理 Peer(Agent Peer)。

文件源 Peer 是文件的最初来源,它在整个应用中是唯一的,即整个应用中只有一个文件的来源,它主要负责对文件进行分片,然后把分好的片按照规则封闭成数据包,以组播形式发送到应用网络上。同时文件源还需对其他 Peer 发出的分片请求做出应答,以重新发送请求方丢失的分片。

代理 Peer 在应用中的角色可从两个角度来看:一方面在同一组播域中,代理 Peer 扮演着和文件源 Peer 相同的角色,即它是该组播域的"文件源",负责把从文件源 Peer 获得的文件以组播形式发送到该组播域的其他结点;另一方面代理 Peer 也是一个特殊的接收 Peer,它以单播的形式从文件源或其他 Peer 处取得文件分片,并力图保证文件的完整性。

接收 Peer 在大规模的应用中所占的比例比较大,应用中绝大多数对等体都属于这种类型。它的功能一方面是从处于同一组播域的文件源 Peer 或代理 Peer 处以组播方式接收文件分片,另一方面以单播方式从其他 Peer 取得丢失的分片。

3 应用管理详细设计

应用管理目的是实现 P2P 功能,为了使应用能够简单有效、稳定安全地工作,为了降低设计开发周期,通过比较论证决定采用 JXTA 平台来实现主要功能:资源搜索。

3.1 JXTA 平台

3.1.1 JXTA 平台简介

JXTA 是项目创始人 Sun 首席科学家 Bill Joy20 多年酝酿的结晶,"JXTA 技术是网络编程和计算的平台,用以解决现代分布计算尤其是点对点计算中出现的问题"[2]。

JXTA 是为了构建 P2P 网络而制订的一组协议,是处理构建 P2P 网络所碰到的问题的解决方法。JXTA 标准协议规范介绍如下:"JXTA 由六个协议组成,这些协议是专为特定的、分布式的、对等的网络计算而设计的。使用这些协议,Peer 可以互相合作来建立自我组织、自我管理的对等组,而不必关心它们在网络中所处的位置,也不需要集中的管理机构。"

3.1.2 JXTA 协议

JXTA 在 JXTA 协议规范中定义了它的协议。此规范描述了 Peer 间如何通信和交互,它并未描述实现的细节或如何编写 P2P 应用程序。下面是 JXTA 协议的列表,其中包含了协议名称的首字母缩略词,这六个协议如图 2 所示[3]。

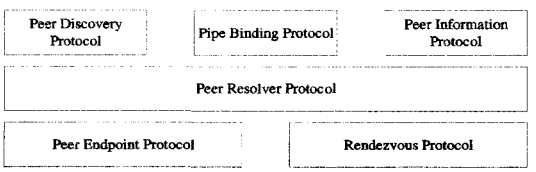

图 2 JXTA 的核心协议

(1)Peer Discovery Protocol(PDP)对等点发现协议:Peer 使用这个协议来发现被发布出来的 JXTA 资源。广告就是代表着发布的资源。

(2)Peer Resolver Protocol(PRP) 对等点解析协议:在通常情况下,Peer 向其它 Peer 发送查询消息来定位服务或者内容。PRP 会将查询的格式标准化。

(3)Peer Information Protocol(PIP)对等点信息协议:可以在 JXTA 环境中对一个 Peer 发出 ping 消息。

(4)Peer Membership Protocol(PMP)对等点成员协议:对等点使用该协议来加入和离开 Peer group。

(5)Pipe Binding Protocol(PBP)管道绑定协议:Peer 使用管道来连接服务。一个 Peer 可以动态地将绑定 Pipe 的一端连接服务。Peer 可以新建 Pipe,把它绑定到现存的 Pipe 上,或是取消对 Pipe 的绑定。

(6)Endpoint Routing Protocol (ERP)终点路由协议:这个协议帮助 Peer 将消息路由至目的地。[4]

3.2 模块详细设计

3.2.1 管理模块

工作流程图(由于篇幅原因只列出了接收方流程图)见图 4。

3.2.2 详细说明

(1)启动 JXTA

每个对等体启动时,都要先启动 JXTA 平台。如果某一对等体位于防火墙之后,则启动时,高级选项中 HTTP Enable 选项必须配置成 Enable。

(2)加入 NetPeerGroup 组

对等体必须加入到 NetPeerGroup 组。该组是默认的对等组,其他任何对等组都是改组的子集。

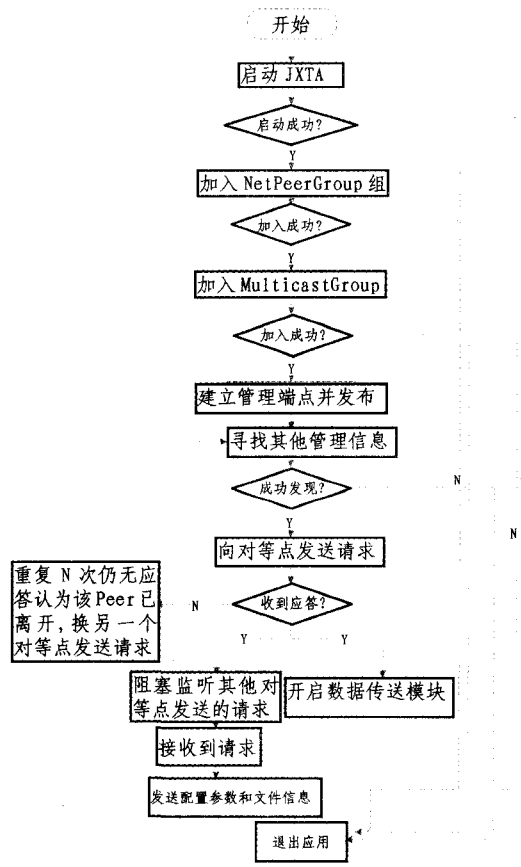

图 4 接收方流程图

(3)加入 MulticastGroup 组

Multicast 组只能由文件源创建。这里分两种情况:

一种是对等体本身就是文件源 Peer,那么该对等体必须负责创建 MulticasgGroup 组。当文件源 Peer 启动时,先检查

本地缓存中是否有 MulticastGroup 的组通告，如果有，则直接加入到该组，否则必须创建一个 MulticastGroup 对等组，并把该组发布到 JXTA 网络上，并加入该组。

另一种情况是对等体是代理 Peer 或接收 Peer，那么该对等体也应该先检查本发缓存，看有没有 MulticastGroup 的组通告。如果有，则试着加入到该组；如果没有，则远程发送发现请求，来远程发现 MulticastGroup 组。如果发现不成功，则重新尝试 N 次后，退出该应用，并报告未发现对等组的错误。

(4)创建输入管道端点，并发布

加入 MulticastGroup 组后，对等体就开始创建本地的输入管道端点。整个应用过程中，对等体以此管道端点与其他对等体建立管道，接收其他对等体的 P2P 消息。

(5)发现其他对等体管道通告

如果对等体是文件源 Peer，则直接进行步骤 7 和 8。因为文件源 Peer 是文件的最初发源地。

除文件源 Peer 之外的对等体必须发现其他对等体的管道通告，以从其他对等体处获得组播地址和端口信息，以及将要发送的文件信息。

(6)向其他对等体发送请求并等待应答

当对等体发现了其他对等体的管道通告后，就可以与这些对等体进行通信了。如果所发现的管道通告中只有文件源 Peer 的管道通告，那么该对等体同文件源 Peer 建立管道，并向文件源 Peer 发送请求。如果所发现的管道通告中既包括文件源 Peer 的管道，也包括其他类型 Peer 管道，则该对等点优选其他类型 Peer 的管道端点，建立管道并发送请求。

当对等体向某个对等体发送请求后，便等待该对等体的响应。如果经过一段时间延时，还未收到响应，则重新发送请求。直到重试 N 次后，如果仍未响应，则认为该对等体已经退出该应用。在这里，延时的时间应由应用的范围决定。如果应用是在一个子网内，则时间可设置得稍微短些，例如 3 秒钟。如果是在 Internet 上应用，则延时时间还应更长些，以给被请求的对等体足够的时间进行响应。

对等体收到应答后，设置本地文件管理器和应用参数，准备接收数据，同时监听其他对等体的 P2P 请求。

(7)开启数据传送模块

这里也分为两种情况：

第一种情况，如果该对等体是文件源 Peer，则经过一段时间的延时后再开启数据传送块，以给其他对等体充足的时间来接收到应用所必需的参数(组播端口、组播地址、文件信息等)延时过后，该文件源 Peer 开始发送组播数据并等待其他对等体的数据请求和 P2P 请求。

第二种情况，如果该对等体是代理 Peer 或接收 Peer，则该对等体立即开启数据传送模块，以做好接收组播数据的准备。

当数据模块执行完毕后，应用并不立即退出，而是继续等待，直到用户手动关闭为止。目的是为了继续响应其他对等体的数据请求和 P2P 请求。

(8)接收和响应其他对等体的请求

当连接建立完毕之后，对等体就监听并响应其他对等体发送的 P2P 请求了。当对等体接收到其他对等体的 P2P 请求时，从请求通告中提取出请求者的管道端点通告信息，然后建立一个输出端点，与请求方的输入端点建立管道，并把应用的参数和将要传送的文件信息传送给请求对等体。传送完毕后，继续等待下一个请求。

3.2.3 消息格式定义

P2P 消息主要分两类：一类是由各种服务所使用的通告为内容的消息，这类消息由 JXTA 自动维护，因此不需要我们设计；另一类是以应用参数和文件信息为内容的消息，这类消息需要发送对等体和接收对等体按照统一的格式进行传递。

(1)请求消息格式设计。

```
〈Request〉
    〈InputPipe〉
        请求方的输入管道端点通告
    〈/InputPipe〉
〈/Request〉
```

这里包含请求方的输入管道端点通告，是为了让被请方应答时直接跟该管道端点建立通信。

(2)应答消息格式(这里只列出部分消息格式)。

```
〈Response〉
  〈Application〉
    〈MulticastDataSocket〉
      〈Version〉“4”或“6”〈/Version〉
      〈Address〉组播数据地址〈/Address〉
      〈Port〉组播数据端口〈/Port〉
    〈/MulticastDataSocket〉
    〈UnicastMessageSocket〉
      〈Version〉“4”或“6”〈/Version〉
      〈Address〉组播数据地址〈/Address〉
      〈Port〉组播数据端口〈/Port〉
    〈/UnicastMessageSocket〉
    〈DataSize〉数据字段最大长度〈/DataSize〉
    〈HeaderSize〉数据包包头长度〈/HeaderSize〉
    〈PacketSize〉一个数据包长度〈/PacketSize〉
  〈/Application〉
  〈File〉
    〈ID〉要传送的文件的 ID〈/ID〉
    〈Size〉要传送的文件的大小〈/Size〉
    〈Attribute〉
      〈ReadOnly〉是否只读〈/ReadOnly〉
      〈Hidden〉是否隐藏〈/Hidden〉
    〈/Attribute〉
  〈/File〉
〈/Response〉
```

4 测试环境设计与测试数据分析

4.1 测试环境

4.1.1 同一网段内

在同一网段中，主机的操作系统为 Windows XP、Windows 2000、Windows 2003，手工设置 IPv4 地址。网络拓扑见图 5。

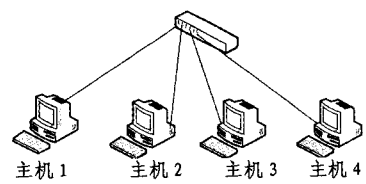

图 5 同网段测试拓扑图

4.1.2 不同网段间

路由器：日立 GR2000_2B_IPv6，3 个接口；

接口 1：fe2/1，ipv6 address：2001：254：1a03：1：：/64，不在组播域中，IPv6 地址自动获取；

接口 2：fe2/2，ipv6 address：2001：254：1a03：2：：/64，在组播域中，IPv6 地址自动获取；

接口 3：fe2/3，ipv6 address：2001：254：1a03：3：：/64，在组播域中，IPv6 地址自动获取。

网络拓扑见图 6。路由器的 3 个接口中，有两个在同一组播域中，另外一个不在。测试时，在接口 1 的子网中添加一个汇聚点，通过它从其它组播域获取文件，进而该组播域中的其它主机就可以以组播的形式从汇聚点获取文件。为说明简

(下转第 54 页)

源 MAC 地址、源 IP 地址、记录时间等，以供查看分析使用。

```
struct arp_header {
u_int16_t arp_hardware_type;/* 硬件类型 */
……
u_int8_t arp_source_ethernet_address[6];
/* 源 MAC 地址 */
u_int8_t arp_source_ip_address[4];
/* 源 IP 地址 */ u_int8_t arp_dest_ethernet_address[6];
/* 目的 MAC 地址 */
u_int8_t arp_destination_ip_address[4]; /* 目的 IP 地址 */ };
```

检测过程的结果如图 2 所示。

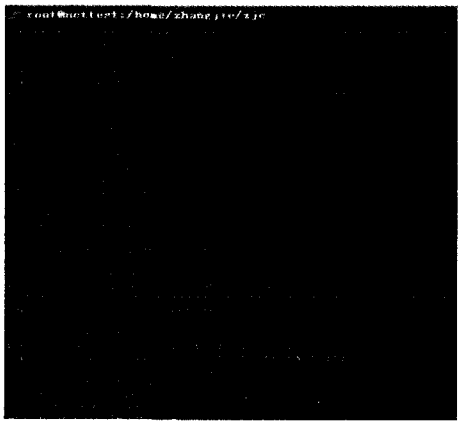

图 2　ARP 欺骗检测分析截图

4.3　检测分析

该检测系统在运行过程中，能够捕获到所有的 ARP 报文，没有发生丢包现象。本文采用 Libdnet 开发库构造 ARP 欺骗应答报文，对系统进行测试。系统能有效检测出欺骗报文，并锁定发欺骗攻击的 MAC 地址。由于 IP-MAC 地址标准对应库是检测出欺骗报文的基础，建立正确完善的地址对应关系至关重要。当采用动态学习的方法建立地址库时，由于系统没有对 IP 地址的范围进行限制，导致地址库中存在大量无用地址对应关系，对地址查找效率产生一定影响。相对地，手工建立地址库的方法保障了其精简和完整性，提高了检测效率。

结束语　ARP 协议在基于 TCP/IP 的网络中广泛应用，虽然因协议固有的安全漏洞，ARP 欺骗会导致网络运行和网络用户受到严重的安全威胁，但通过剖析掌握其攻击原理后，我们可以采用有效的防范措施，来对网络施行保护，减小其危害。本文提出的 ARP 欺骗检测方法简洁易行，可以结合其它防范措施，对检测网段提供安全保障，具有一定的实用价值。

参 考 文 献

1　Stevens W R. TCP/IP Illustrated Volume 1: The Protocols [M]. 北京：机械工业出版社，2000
2　刘凯，邓兰，黄明和. 在局域网中防止 ARP 欺骗的一种方法及其实现[J]. 江西师范大学学报，2005，29(2)：173～175
3　王奇. 以太网中 ARP 欺骗原理与解决办法[J]. 网络安全技术与应用，2007
4　陈辉，陶洋. 基于 WinPcap 实现对 ARP 欺骗的检测和恢复[J]. 计算机应用，2004，24(10)：67～68
5　郑文兵，李成忠. ARP 欺骗原理及一种防范算法[J]. 江南大学学报，2003，2(6)：574～577
6　吕骥，文静华. 校园网内 ARP 欺骗攻击及防范[J]. 福建电脑，2007(5)
7　庄健平. 基于 ARP 协议入侵的安全策略[J]. 怀化学院学报，2006，25(8)：81～83

(上接第 41 页)

单，暂且将与接口 1 相连的网段称为网段 1，其它两个称为网段 2 和 3。汇聚点在网段 1 中，文件源在网段 2 中。

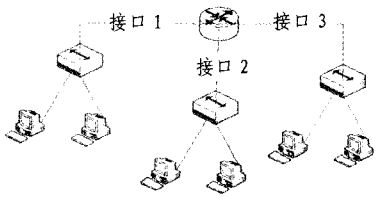

图 6　测试拓扑图

4.2　测试结果

4.2.1　同一网段内

(1)Source Peer

①JXTA 的基本配置

首先配置 Basic 选项卡，填入 Peer Name，Password 等信息；Advanced 选项卡采用默认设置；Rendezvous/Relays 选项卡也选择默认设置。

②运行结果

首先，发现并加入 NetPeerGroup 组，然后在缓存中查找 MulticastGroup。已存在，则加入之，显示出 MulticastGroup 的相关信息，同时显示加入组成功的信息，然后在缓存中查找 InputPipe 信息；若不存在，则创建。若存在，则显示其信息，并且显示成功创建 InputPipe 信息，同时等待其它 Peer 的 Request；收到其它 Peer 的 Request；向请求 Peer 发送 Response；继续等待其它 Peer 的请求。

(2)Reciver Peer

①JXTA 的基本配置

Basic 选项卡：与 Source Peer 相同；Advanced 选项卡：将 Http 的端口号改为手工配置，8000；Rendezvous/Relays 选项卡：采用默认值。

②运行结果

首先，发现并加入 NetPeerGroup 组；接着，发现并加入 MulticastGroup 组；查找管道信息；创建自己的 InputPipe；连接到文件源并向其发送请求；等待文件源的回应，显示 Response 内容，并将其写入配置文件。

4.2.2　不同网段间

JXTA 的配置与同一网段的基本一致，只需在 Rendezvous/Relays 中的 Rendezvous send peers 中添加已设置好的汇聚 Peer 的地址就可实现信息转发。

4.3　结果分析

通过对实验数据的分析，发现仍存在一些问题：①在同一网段的情况，一般很容易实现，同时开启多个 Peer 的时候也可以顺利进行。但是文件源的 Peer 要较其它 Peer 早开启，若晚开启或者同时开启都会出现找不到组的情况。②不同网段间的情况，需设置汇聚点方可通讯。③跨多个路由的情况：由于网络的复杂性，因此会影响到速度，但可以实现文件源的发现，只是速度上较同一网段上的稍慢了一些。

今后将在此基础上对系统的性能、安全性、对多媒体信息的传输等方面进行深入研究。

参 考 文 献

1　丘子隽. IP 组播的概念与应用. 世界宽带网络，2005. 25～30
2　JXTA Java Standard. Edition2. 3. 4Javadoo [EB/OL]. http://platform. jxta. 0rg/n0nav/java/api/jndex. html，2005
3　张智，李瑞轩. 基于 JXTA P2P 的 Web 服务发现模型研究[J]. 计算机工程与应用，2005，41(19)：137～139
4　Gong L. JXTA: A Network Programming Environment[J]. IEEE Internet Computing，2001，15(3)：88～95