Mobile IP 系统中的 AAA 接口研究与设计

王玉辉,黄传河,陈 莺

(武汉大学 计算机学院,湖北 武汉 430079)

摘要:在全IP无线互联网包分多址(PDMA)系统中,移动用户可以通过简单IP或移动IP两种接入方式接入Internet。如何对以上两种接入方式的用户提供基于RADIUS协议的身份认证、授权及基于流量方式的计费功能,是PDMA系统面临的一个重要问题。文章提出了支持微移动和宏移动两层协议体系分别进行AAA机制处理,以及两层AAA机制间有效协调的设计方案,在某地试验网的实际运行中取得了良好的效果。

关键词:包分多址;MPPP;移动IP;AAA

中图分类号:TN92 **文献标识码**:A **文章编号**:1005-8788(2005)02-0035-03

The reasearch and design of AAA interface in mobile IP systems

WANG Yu-hui, HUANG Chuan-he, CHEN Ying

(Computer School of Wuhan University, Wuhan 430079, China)

Abstract: In the PDMA system of mobile Internet, the users can access Internet through simple IP or mobile IP. A great challenge the PDMA faces is how to implement the function of AAA (authentication, authorization and flow pattern-based accounting) based on RADIUS protocol. this paper offers a design scheme which support two layered protocols of micro-mobility and macro-mobility to carry out the AAA mechanisms processing respectively and realize the effective coordination between the AAA mechanisms of two layers. This scheme has achieved good results in the practical operation of a certain base of PLA.

Key words: PDMA; MPPP; mobile IP; AAA

1 概 述

在国家"八六三计划"重大项目"新一代蜂窝移动通信系统技术研究与开发"包分多址(PDMA)系统(全IP无线互联网)中,AAA接口的功能目标主要是实现对移动IP接入用户的身份认证、授权和计费。本文旨在为自主开发的PDMA系统真正走向实际商用运营提供全功能的计费、鉴权和认证支持,并创造性地通过移动PPP(MPP))和移动IP(MIP)两层协议结构使得系统在多用户、移动IP的环境中可持续稳定地运行。这种解决方式目前在国内全IP无线互联网领域还属于一种比较创新的解决方案。本文论述的系统平面协议栈如图1所示。

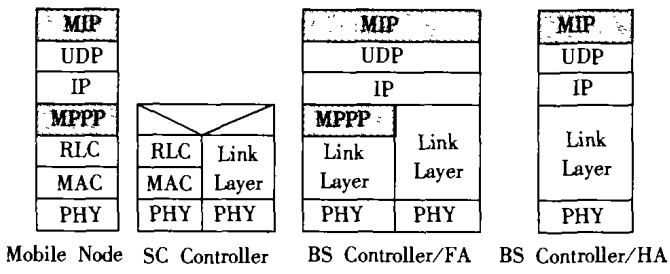

图1 系统平面协议图

其中涂黑部分为自主开发的重点。本文最大的创新就是支持MPPP和MIP两层分别执行AAA机制并分别进行处理以及两层AAA机制间有效协调的设计。本文阐述的解决方案主要体现在从用户开始访问网络直至访问结束的整个流程中与AAA体系进行交互环节的设计:在MPPP的链路建立过程中的AAA认证、授权;在移动IP注册请求中的AAA认证及分发HA与FA之间的密匙。

2 MPPP的链路建立中的AAA接口

在MPPP的链路建立阶段,各实体所需完成的功能描述如下:

· 用户User(MN):作为接入客户端,完成与NAS的PPP协商过程;

· 接入服务器NAS(FA):作为接入服务器,同时又作为RADIUS客户端,完成基于CHAP协议的用户身份认证过程及PPP链路建立过程;

· RADIUS AAA服务器:作为RADIUS服务器,完成User的身份认证。

其网络拓扑结构如图2所示。

在PPP认证过程中,NAS使用CHAP协议对User发送一个CHAP Challenge消息,其中包含服务提供者名称、一个随机数 r 以及一个标识符id;User对标识符id、与服务提供商共享的密钥以及随机数 r 计算MD5消息摘要,然后发送Response

收稿日期:2004-09-01

基金项目:国家"八六三计划"资助项目(2001AA123014)

作者简介:王玉辉(1978-),男,湖北武汉人,硕士,主要研究方向为计算机系统结构。

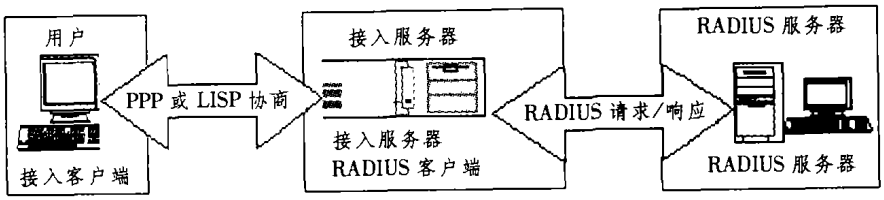

图 2 网络拓扑图

应答消息,其中应包含 User 的用户 NAI、id 及 MD5 消息摘要值[1];NAS 将 User 用户名及上述 MD5 消息摘要值以 Radius 协议 Access-Request 包格式进行封装并发送至 AAA Server 上进行认证;AAA Server 在经过用户身份认证后,向 NAS 发送 Access-Response 包,若用户身份认证通过,应答包的类型为 Access-Accept,否则为 Access-Reject; NAS 在用户身份认证通过后,将根据用户是 SIP 接入还是 MIP 接入进行相应的 IPCP 配置参数协商;否则,向用户发送认证无效消息,结束 PPP 会话。在设计的过程中需要注意的是在 IPCP 协商完成,PPP 链路建立后,如果是以 MIP 方式接入,则需立即进入代理搜索及注册过程;如果是以 SIP 方式接入,则需进入 AAA 计费。

3 MIP 注册过程中的 AAA 接口

在本系统的 MIP 中,我们首先做以下两个假设:一是 MN 只和 AAAH 之间预先存在安全关联;二是 MN 归属地址是静态分配的,MN 归属代理可动态分配。在 MIP 注册过程中,其 AAA 功能实体为 MN、FA、HA 及 AAAH/AAAF,各实体在 MIP 注册过程中所需完成的功能描述如下:MN 实现 MIP 中的注册请求功能;FA 在 MN 使用外地配置转交地址进行注册时,实现 AAAH 的客户端功能,并从 AAAH 的应答包中获取动态分配的 HA 地址及 MN-FA 共享密匙[2]; HA 在 MN 使用配置转交地址进行注册时,实现 AAAH 的客户端功能,同时完成 FA-HA 共享密匙获取功能;AAAH/AAAF 实现对 MN 身份认证及 HA 动态分配功能,还实现对 HA 分发 FA-HA 共享密匙功能。

其网络拓扑结构如图 3 所示。

其注册认证流程如下:

(1) MN 使用外地代理地址进行注册,如图 4 所示。

以上设计流程完全遵循 RFC 2002、RFC 2865、RFC 3012 标准进行,并且部分参考了 Funk Software 公司的 steel-belted radius MIP Module 解决方案,详细论述如下:

首先 FA 向 MN 发送 Advertisement/challenge 消息;MN 将注册请求(其中包含 MN-NAI 扩展和 MN-AAA 验证扩展)发送至 FA;FA 向 AAAF/AAAH 发送 Access-Request 包,在此请求包中,需要包

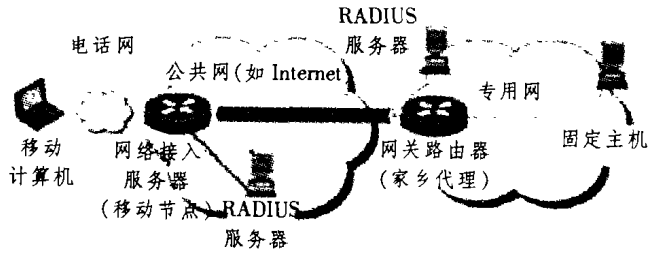

图 3 网络拓扑图

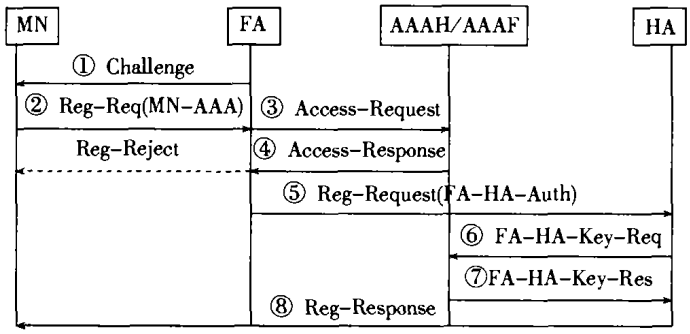

图 4 外地代理地址注册流程

含以下属性:用户名(User-Name,NAI 格式);归属代理地址(Home-Agent-Address),若为 0,为请求分配一个家乡代理地址[3];计费时所需的全局会话标识(Account-Multi-Session-ID);在用户会话过程中,可能经过多个 FA 提供服务,在计费时,需要使用该属性将多个 RADIUS 计费会话联系起来,作为一次用户会话统一计费;FA-HA 共享密匙(Pre-Shared-Secret-Request),HA 通过该共享密匙验证注册请求包的有效性;AAAF/AAAH 向 FA 发送 Access-Response 包,若用户认证成功,其 Access-Accept 应答包需要包含以下属性:Home-Agent-Address;共享密匙(Pre-Shared-Secret),在传输中需要用 FA 与 AAA 之间的共享密匙加密;FA 向 HA 转发注册请求,在此注册请求中需要包含 FA-HA-Auth 扩展[4]; HA 向 AAAH 发送 FA-HA-Key-Request 请求包,在此请求包中需要包含以下属性:HA 的 NAI 标识(User-Name);HA 密码(User-Password);AAAH 向 HA 发送 FA-HA-Key-Response 应答包,该应答包括以下属性: 共享密匙(S-Key);共享密匙存在时间(S-Lifetime)[5];HA 使用 FA-HA 共享密匙验证 FA-HA-Auth 扩展有效性,完成对移动节点的绑定表项

更新工作，并通过 FA 向移动节点发送注册应答，告知注册成功。否则，发送注册失败应答。

在设计的过程中，尤其需要注意的是，在 FA-HA 共享密匙的有效时间过期时，HA 需向 AAAH 发送 FA-HA-Key-Request 请求包，请求更新该共享密匙。

(2) MN 使用配置转交地址进行注册。

流程如图 5 所示。

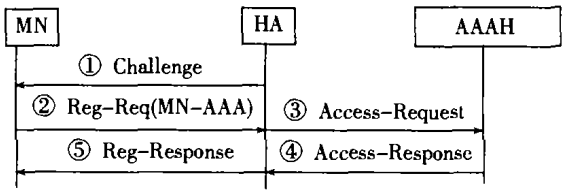

图 5 配置转交地址注册流程

对于以上流程详细说明如下：HA 向 MN 发送 Advertisement/challenge 消息；MN 将注册请求(其中包含 MN-NAI 扩展和 MN-AAA 验证扩展)发送至 HA；HA 向 AAAH 发送 Access-Request 包，包的格式遵循 RADIUS 协议中定义的一般认证请求包格式；AAAH 在经过用户身份认证后，向 NAS 发送 Access-Response 包，若用户身份认证通过，应答包的类型为 Access-Accept，否则为 Access-Reject；若用户身份认证成功，HA 完成对移动节点的绑定表项更新工作，并向移动节点发送注册应答，告知注册成功。否则，发送注册失败应答[6]。这一流程完全遵循一般的解决办法。

在 PDMA 系统中，本文阐述的 Mobile IP 中的 AAA 接口程序主要模块结构如图 6 所示。

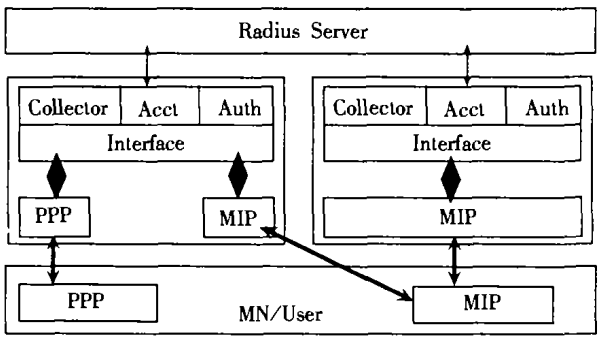

图 6 程序模块设计图示

其中粗箭头所示部分为本文阐述的解决方案所涉及的工作，理顺这一部分的关系，并把遵循本文阐述方案所做的程序纳入到原有的基站源代码中进行联调，是本文设计者的工作。

说明如下：MN 主要实现 PPP 及 MIP 注册客户端功能。对于程序模块结构中涉及到的实体以及实体的作用概述如下：AAA Server 主要实现基于 RADIUS 协议的认证、授权及计费功能；FA/NAS 主要实现 PPP Server、MIP 中的 FA 功能、流量采集及作为 Radius Client 的功能，其与 AAA 接口的主要模块可划分为 RadiusAcct(实现 Radius 计费客户端功能)、RadiusAuth(实现 Radius 认证客户端功能)、RadiusInterface(实现与 PPP 及 MIP 的接口功能)、RadiusCollector(实现 Radius 计费流量采集功能)；HA 主要实现 MIP 中的 HA 功能、流量采集及作为 RADIUS Client 功能，其与 AAA 接口的主要模块可划分为 RadiusAcct(实现 RADIUS 计费客户端功能)、RadiusAuth(实现 Radius 认证客户端及密匙请求功能)、RadiusInterface(实现与 MIP 的接口功能)、RadiusCollector(实现 Radius 计费流量采集功能)。

4 结论及展望

依据本文论述的设计方案所做出的软件代码已经成功纳入到 PDMA 系统某地试验网工程，并完全支持 PDMA 系统分层移动性管理策略。从 2004 年 2 月开始在试验网两个基站上运行以来，其中每基站接入用户数为 10 个，在屡次的演示中一直稳定工作。能够实现设计目标中认证、鉴权、计费功能，完全支持用户在单基站多扇区间的平滑切换，完全支持用户在多基站间的平滑切换。目前已达到理论可以支持 8192 用户单基站的理论实现能力，各项测试指标已达到基本商用指标。由于已经有实际应用平台的运行结果，故本文未给出试验结果仿真数据。

由于 RADIUS 协议先天的一些缺陷，如端到端安全性不足，面临扩容就需要添加新的 AAA 服务器，基于 UDP 无法完全确保传输可靠性，故障切换能力不足等等，针对 RADIUS 协议缺陷而设计的功能更强大的 DIEMETER 协议应运而生。设计基于 DIAMETER 协议的全 IP 无线互联网新的 AAA 解决方案并且和已有 RADIUS 解决方案有效互通正是笔者目前正在从事的工作。

参考文献：

[1] Solomon J. Mobile-IPv4 configuration option for PPP IPCP [EB/OL]. IETF RFC2290, http://bgp.potaroo.net/ietf/idref/rfc2290/, 1998-02.

[2] Solomon J. Applicability statement for IP mobility support [EB/OL]. RFC2005, http://bgp.potaroo.net/ietf/idref/rfc2005/, 1996-10.

(下转第 58 页)

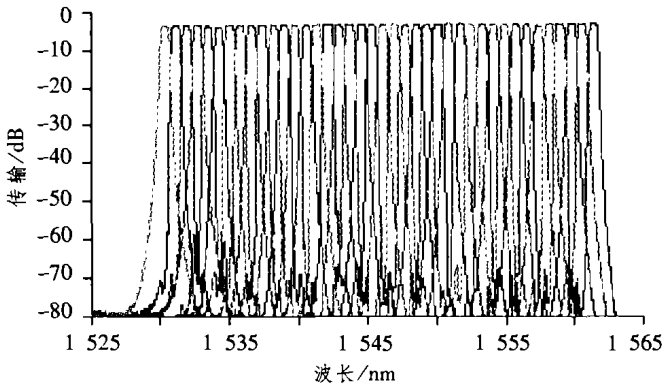

图4 均衡型100 GHz 40通道介质膜型DWDM谱线图

另外,我们对200只TFF型100 GHz 40通道DWDM器件的插入损耗和插损均匀性进行了统计,得到了统计图(均衡型的TFF型DWDM器件插入损耗统计图见图5,均衡型的TFF型DWDM器件插入损耗均匀性统计图见图6)。

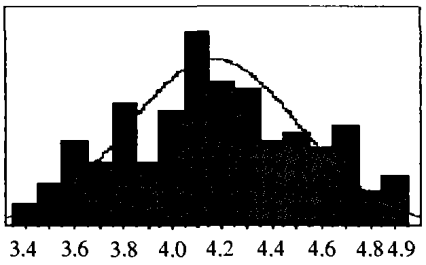

图5 均衡型的TFF型DWDM器件插入损耗统计图

通过统计计算得到插入损耗的典型值为4.17 dB,插入损耗均匀性的典型值为0.67 dB。

通过上述比较和统计结果可以看出,采用了多级均衡方案的均衡型TFF器件在保持了原有TFF器件的优点(稳定性好、PDL小和无需温控)的前提下,插入损耗和插损均匀性两项指标已经与AWG型器件相当,甚至略优于AWG器件。从而使均衡型TFF器件在与AWG型器件的竞争中具有更大的优势,因此TFF器件可以成为目前光通信系统中制作DWDM器件的主流技术。

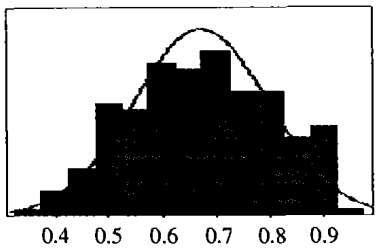

图6 均衡型DWDM器件插入损耗均匀性统计图

4 结 论

本文介绍了一种采用新型多级均衡的方案的介质膜型光WDM器。该TFF型DWDM器件的典型插入损耗为4.17 dB,典型插入损耗均匀性为0.67 dB。通过与AWG型DWDM器件的比较,可以看出均衡型的TFF型DWDM器件克服了TFF器件的固有缺陷,成功地突破了TFF型DWDM器件通道数无法达到32、40的瓶颈,从而使TFF器件可以成为目前光通信系统中制作DWDM器件的主流技术。

参考文献:

[1] 王传林,余重秀,忻向军,等。光通信中的波分复用技术及关键器件的原理及应用[J]。物理,2002,31(9):596-600。

(上接第37页)

[3] 庄宏成,张光昭。无线IP网络的平滑切换和QoS保证[J]。计算机工程与应用,2002(8):23-25。

[4] Rigney C. RADIUS Accounting [EB/OL]. IETF RFC2866. http://bgp.potaroo.net/ietf/idref/rfc2866/, 2000-06.

[5] 侯自强。新3G系统——无线移动因特网[J]。电信科学,2002(5):5-9。

[6] Iames D.Solomm(著). 裘晓峰(译)。移动IP[M]。北京:机械工业出版社,2001。