文章编号:1001 - 9081(2010)02 - 0312 - 04

SIP 的 VoWLAN 通信平台设计与实现

杜忠燕,王卫星
(重庆邮电大学 计算机科学与技术学院,重庆 400065)
(dudupost@ gmail. com)

摘　要:如何将会话初始化协议(SIP)与现有的通信网络有机结合,提供安全可靠的数据及通信服务已成为当今的热点问题。VoIP 应用也受到业界的持续关注。安全问题一直都是企业实施 VoIP 的一个阻碍。提出了一个基于 SIP 的 VoWLAN 通信平台,将各种语音服务构建于无线局域网之上。利用虚拟专用网(VPN)、数据加密技术、VLAN 和防火墙等必要安全技术和策略,应对在系统中的安全威胁,实现了通话质量可靠、安全性高的企业级 VoIP 无线网络架构。描述了该系统的设计和实现过程,讨论了其中的关键技术。

关键词:VoWLAN;会话初始化协议;网络语音电话业务(VoIP)
中图分类号: TP393.03　　**文献标志码**:A

Design and implementation of communication platform over WLAN based on SIP protocol

DU Zhong-yan, WANG Wei-xing
(*College of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing* 400065, *China*)

Abstract: How to combine Session Initiation Protocol (SIP) with current communication system well so as to provide secure telecommunication services has become a hot current issue. Security issue is always the major barrier to employing Voice over Internet Protocol (VoIP) technology by enterprise. This paper presented a solution named VoWLAN for voice business over Wireless Local Area Network (WLAN) on the basis of SIP server and VoIP gateway which deploys various voice services. Virtual Private Network (VPN), data encryption, VLAN and firewall technique achieved good quality and safety enterprise VoIP platform were implemented, and the design and implementation procedure of the whole system were described.

Key words: VoWLAN; Session Initiation Protocol (SIP); Voice over Internet Protocol (VoIP)

0　引言

VoWLAN 是一种在无线宽带网络上传输语音信息的方法,主要是将 Wi-Fi 无线接入技术与 VoIP 技术相接合,利用现有的无线局域网(Wireless Local Area Network, WLAN)实现无线的 VoIP 通话能力。VoWLAN 结合了 WLAN 的移动性和 VoIP 基础网络价格低,分布广等优点,将支持 WLAN 和会话发起协议(Session Initiation Protocol,SIP)的无线终端或者手机,通过 WLAN 的接入点(Aceess Point, AP)接入 VoIP 网络,进行基于 VoIP 的语音通信及其他相关业务。

SIP 是 NGN(下一代网络)和第三代移动通信(3G)中最重要的多层次信令控制协议[1],具有很强的可扩充性、可移动性和可扩展性。SIP 已经成为构建 VoIP 系统的主要信令协议标准。

目前,VoIP 已发展成为一种将来可以替代公共交换电话网络(Public Switched Telephone Network, PSTN)的技术,并逐渐趋于成熟。VoIP 使用了大量的协议,用来确保语音通信正确地建立在通信双方,语音质量要能与 PSTN 相当[2]。这些协议包括:SIP、数据控制和传输协议(如 TCP)、实时传输协议(Real-time Transport Protocol, RTP)、用户数据报协议(如 UDP),还有 IP 协议等。将语音数据像传输数据包一样在发送方编码打包,在接收方解码解包重新排序。VoIP 系统中语音数据流处理如图 1 所示。

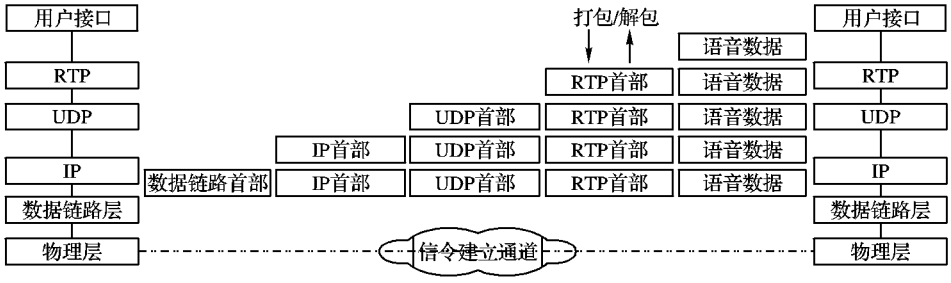

图 1　VoIP 系统中语音数据流处理

VoIP 语音数据处理分为四步:信令建立、编码、传输和网关控制。信令建立由 SIP 来完成,一旦连接建立,语音数据必须要转换成数字形式,然后将数据分段成数据包流在网络中各层传输。接下来,语音信号被合成在数据包里面,通常加上 RTP 头在网络层间传输,保证语音在接收方能够正确重组接收到的报文。封装好了的语音包被 UDP 协议层作为数据负载进行传输。在接收方,处理流程是相反的:数据包被解包,然后排序组成正常的顺序。

收稿日期:2009 - 08 - 05;**修回日期**:2009 - 09 - 18。

作者简介:杜忠燕(1976 -),女,新疆库尔勒人,硕士研究生,主要研究方向:计算机网络与通信、多媒体通信、网络安全、数字图像; 王卫星(1959 -),男,瑞典人,瑞典皇家工学院终身教授,博士生导师,主要研究方向:数字图像处理、模式识别、多媒体通信。

基于 SIP 的 VoIP 通信系统主要实现形式有两种:一种是软交换系统,即将语音通信建立在现有的数据通信网上,只是相互拨打虚拟的 IP 电话,无法与固定电话或者 GSM 手机通信;另一种是将软交换系统与 PSIN 相互接合,使用特定的 VoIP 网关,将 PSTN 与 SIP 软交换系统结合,可以拨打固定电话,实现原有模拟电话的基本功能。本文采取的是第二种形式。如何提高 VoIP 通信系统的语音质量以达到与模拟电话基本相同,以及确保通信安全一直是 VoIP 系统研究的重点。

1　系统设计

VoWLAN 框架由 AP(Access Point)、终端(SIP 电话/支持 SIP 的手机)、控制节点、网关节点及基于 IP 的网络构成。本地 VoIP 电话和远端 VoIP 电话分别使用 Intranet 和 Internet 互联,同时通过 VoIP 网关将 VoIP 电话与 PSTN 的模拟电话相互连接,使得终端用户可以直接拨打 IP 电话或者固定电话,如图 2 所示。

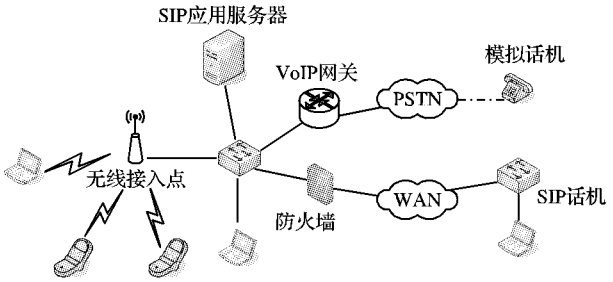

图 2　VoWLAN 应用模型

语音信号将 Internet 当作载波,在互联网上传输,其应用自身就存在未知或已知的安全缺陷(与 IP 协议相关联的)[3]。任何可以接入 Internet 的计算机设备都有通过 Internet 窃取数据流的能力,当然任何一种被设计成攻击电子计算机的算法都可以用来攻击 VoIP 系统。另外传统意义上用来攻击电话系统的手段(如监听、盗打电话等)也可以影响 VoIP 系统。所以 VoIP 系统本身就存在来自两种技术的内在安全隐患。因此,VoIP 在构建、规划、实施各个过程都要注意安全问题,提供点到点的安全服务(保证 VoIP 应用)。

如果缺乏相应的安全措施进行认证和数据加密,会存在几种攻击手段如:监听、攻击 VoIP 通话、截获语音攻击(中间人)、拒绝服务 DoS、破坏通话和发起无效通话请求[4]等。本文着重强调为了有效解决这些安全隐患,在系统设计时应该考虑的技术手段和相应措施。

2　关键技术

2.1　VPN 技术和数据加密

公司总部和两个分部分别位于芬兰、成都和北京。它们都有各自的局域网(Local Area Network, LAN),这些 LAN 同时连接数据终端和语音终端(IP 电话),是一个多媒体网络。这三个 LAN 通过广域网(Wide Area Network, WAN)连接在一起,使得总部不仅可以跟分部相互传输数据,还能相互传输语音。

通过 VPN 可以帮助公司总部与分支机构之间建立可信任的安全联接,并保证数据的安全传输,保证通话的安全性,解决 VoIP 面临的随意拨打,随时被监听的问题(传统 PSTN 的安全问题)。本 VoIP 系统中的 VPN 采用与 IPSec(IP Security Protocol)与 L2TP 相互结合使用,提供强大的认证机制保证数据安全。当然还要考虑单个网络节点如果出现中断,将直接导致 VoIP 通信的中断,所以系统采取的是双路由结构,一个作为主路由,另一个作为辅助路由,当主路由出现故障时,数据包可以通过辅助路由继续传送,保证通信的正常进行。

由于本系统引入无线接入,要想使得 VoIP 应用更加有效,必须考虑安全及 QoS 机制[5],所以我们选择的安全机制是在 802.X 协议 EAP(Extensible Authentication Protocol)中的 WPA 标准。认证机制是 EAP-TLS(RFC5216)标准,该机制用 X.509 数字认证,且允许在 AP 和无线用户之间的双向响应。WPA 标准的加密算法可以防范监听、窃取电话及中间人等攻击手段。

2.2　SIP 应用服务器

在本模型中,SIP 应用服务器是结合了 SIP 代理,重定向,注册,与位置服务器的所有逻辑功能,用来简化配置以及整体系统的稳定性。而且采用的是基于 Linux 的软交换系统,具有易于扩展,方便管理等特点。

SIP 服务器是整个系统的核心部分,最主要的功能是处理接收到的呼叫者发出的 SIP 请求,获取用户的 SIP URL,根据 SIP 请求向被呼叫者转发,如果是同样的 SIP 用户,那么无需经过 VoIP 网关,直接进行通信,如果是 PSTN 用户,就需要由 VoIP 网关进行相应的协议转换和处理来完成呼叫过程。

为了方便 SIP 应用服务器的管理,系统加入了嵌入式 Web 服务器,实现了 CGI 程序,使得管理员可以通过 Web 浏览器在线管理 SIP 应用服务器(如分配最新用户号码),执行相应的功能操作。

2.3　语音呼叫处理流程

VoIP 网关的主要功能有信令处理、SIP 功能、语音编码和解码和路由协议处理等功能,对外分别提供与 PSTN 连接的中继接口(BNC 的 RJ45)以及对内提供的和 IP 网络连接的接口。SIP 终端设备和网关之间通过 RTP 封装语音信息流,网关和 PSTN 交换机之通过 E1 信道传输 PCM 编码,由网关进行两种信令格式的转换。在基于 SIP 的通信网络中,SIP 终端和网关之通过 SIP 消息建立呼叫连接,而网关和 PSTN 交换机之间通过 No.7 信令消息建立电路连接[6]。SIP 消息封装 IP 分组的形式,通过 IP 网络在 SIP 终端和网关之间进行传输,而 No.7 信令消息通过 No.7 信令网络在网关和 PSTN 交换机之间进行传输,由网关完成这两种信令消息之间的转换。具体如图 3 所示。

1)SIP 终端先要注册,通过向 SIP 应用服务器发出 Register 请求,完成号码的注册。SIP 的 URI 形式为“电话号码@SIP 应用服务器的 IP 地址”,如果该用户为合法用户,SIP 应用服务器返回一个初始化信息。当某个 SIP 话机呼叫 PSTN 用户时,SIP 话机构建一个 INVITE 消息,网关在构建初始地址消息(IAM)时,可以从 To 和 From 消息头中获取主叫和被叫号码。SIP 话机在确定 INVITE 消息的一些必需消息头后,用 SDP 给出会话描述,并将它作为 INVITE 消息的消息体。在完成 INVITE 消息构建后,将 INVITE 消息发送给 SIP 应用服务器,由它来确定下一跳为 VoIP 网关。

2)网关根据 INVITE 消息包含的信息生成 IAM,并通过 No.7 信令网络将 IAM 传输给与网关直接相连的 PSTN 交换机,由该 PSTN 交换机根据被叫号码选择另一中间局交换机,并将 IAM 通过 No.7 信令网络传输给该中间局交换机,直到将 IAM 传输到连接被叫 PSTN 话机的本地局交换机。

3)本地局交换机如果发现被叫话机空闲,就回送地址完成消息(ACM)。当网关接收到 ACM,实际上已经建立本地局→网关的单向传输信道。在传统的 PSTN 中,本地局一方面向被叫话机发送振铃信令,一方面通过本地局→网关的单向信道发送振铃回音。所以,网关的接收到 ACM 后,也需要建立网关→SIP 话机的逻辑传输信道,这一点通过网关向 SIP 终端发送状态码为 183 的临时消息实现。

4)当 PSTN 话机摘机后,与其直接相连的本地局交换机将 DS0 双向通路接通并和用户线路相连,生成 ANM 消息,并将 ANM 消息传送给网关。网关接收到 ANM 消息后,网关和 PSTN 话机之间的双向通道已经建立,网关向 SIP 话机发送 OK 响应消息。

5)当 SIP 话机挂机,SIP 话机向网关发送 BYE 消息,网关必须回送 OK 响应消息终止和 SIP 话机之间的 RTP 会话。同时,网关通过 No.7 信令网络,向其直接相连的 PSTN 交换机发出前向拆线信号(CLF),并释放已占用的语音信道。和其直接相连的 PSTN 交换机在接收到 CLF 后,立即通过 No.7 信令网络向网关发送释放监护信号(RLG),同时通过 No.7 信令网络向其他中间局交换机发送 CLF 信号,直到连接 PSTN 话机的本地局交换机收到 CLF,本地局交换机释放用户线和占用的信道,回送 RLG,呼叫通信过程结束。

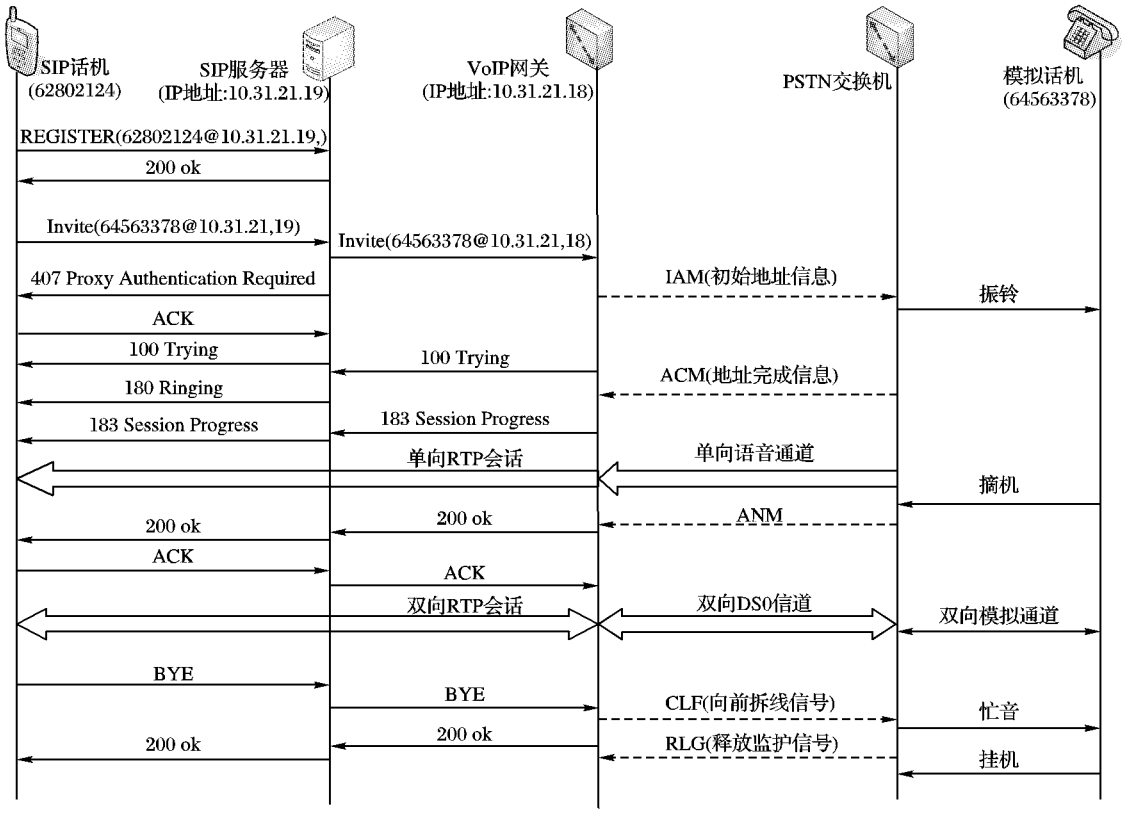

图 3 SIP 话机呼叫 PSTN 话机的操作流程

3 实现结果及讨论

在这一部分中我们通过相关的工具来对系统作一个评价。RTP 控制协议扩展报告(RTCP XR)中定义了一套指标,可以评估 VoIP 呼叫质量和诊断问题,呼叫质量可以根据估计的 R 因子或 MOS(Mean Objection Score 由 ITU-T 建议的P.800 标准提出)平均得分,直接报告呼叫质量。单纯考虑语音质量,我们采用 MOS 值作为判断语音质量标准,MOS 值的范围从 1 到 5:5 为最好;4 为可以接受(4.5 ~ 4.0 为可收费电信级);3 是有噪声(4.0 ~ 3.5 为可通话通信级);2 是不能接受(3.5 ~ 2.5 为可建立连接级);1 是无法通话。

影响 VoIP 语音质量还有一个重要的参数,Jitter(抖动),是指在一个 VoIP 呼叫过程中所有发送的数据包到达的时间差异。在电话呼叫中,它表现的影响是 Jitter 值过大会导致通话时某些字词无法听清。

本文用 WinEyeQ(由 Touchstone 公司开发的一款软件)来监控和分析所有实时会话流量及测试整个系统的两个关键参数:MOS 值和 Jitter 值,具体如图 4 所示。

3.1 通话质量分析

从图 4 中可以看出,抖动值对于 MOS 值具有一定的影响力,在 40 s 的时候,抖动值达到 22.012 ms,MOS 值也达到最低 2.925;抖动值在 4 ms 以下后,MOS 值基本趋于平稳状态达到 4.449 的最高分值。可以通过增加抖动缓冲的数量来减少抖动对通话质量的影响,但同时又会增加网络的延迟,所以要权衡网络实际状况,选取合适的缓冲数量。

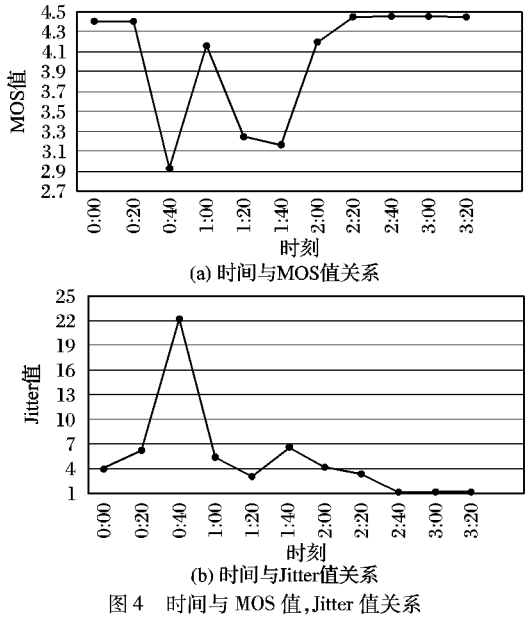

图 4 时间与 MOS 值,Jitter 值关系

3.2 安全测试

VoIP 应用中最基本的安全要求是要保证资源的保密性,只有经过认证的用户才可以使用;完整性,资源不可以被非授权用户随意修改;还有可用性,也就是合法用户可以随时使用资源。我们对系统中使用的几种技术手段:VPN、VLAN、数据

加密及防火墙在几种常见的 VoIP 攻击手段的防范能力方面做了相关分析,结果如表 1 所示(√表示能够防范;×表示不能完全或者完全不能防范)。

表 1　安全策略的防范能力

主要攻击手段	VPN	VLAN	数据加密	防火墙
DoS	√	√	√	√
SPIT	√	×	×	√
偷听	√	√	√	√
发起无效通话	×	×	×	√
拨打免费电话	√	√	√	√
中间人攻击	√	√	×	√

可以用一些抓包工具来观察具体的一个防范措施(抓包软件采用的是 WireShark),如数据加密,这是无线终端接入无线网络时采用的技术手段。无线终端发出 EAP-Response/Identify 请求包,然后 AP 将其包发给认证器,认证服务器用指定的认证算法校验终端的合法性;如果成功,则允许其进入 AP。具体如图 5 所示。

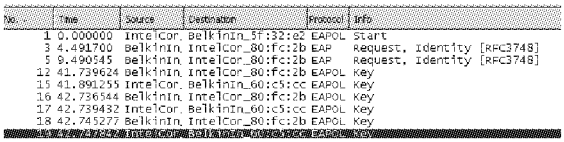

图 5　EAPOL 协议包

图 6 对 SIP 包进行分析,源端地址发出 VoIP 注册请求,如果它无法知道 VoIP 号码及密码,SIP 服务器拒绝此次请求,则它无法注册成功,即可达到阻止偷听、发起无效通话等其他攻击手段的目的。由于本公司的 SIP 服务器只是局限于公司 Intranet 内部,并没有进入公网,所以对其他防范由防火墙做相应的限制策略,即可防止非法用户进入公司内部网络,从而无法进行发起无效通话、DoS、SPIT 等以上列出的攻击手段。

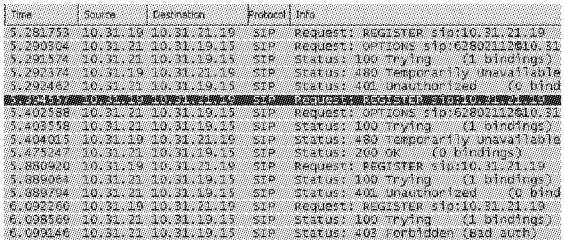

图 6　SIP 包

对于 VoIP 的安全评估目前还不太成熟,评估方法和手段都还不完善,都仅描述了VoIP安全的功能性,但是没有最佳的实施方法和保护 VoIP 网络安全的指导。所以本文在此给出了对于一些基本攻击手段的防范能力分析,旨在说明本系统对于这些攻击手段的防范能力。

4　结语

随着 VoIP 技术的持续发展和逐渐成熟,VoIP 最终会成为取代传统 PSTN 技术的主要通信技术,如何确保 VoIP 的通信安全也变得越来越重要。本文可以防范基本的攻击手段,实现基本通话安全,但对其他安全攻击没有做出相应评测。通过实施完善的安全策略来抵抗软件攻击,设计相应的入侵检测系统将是今后的工作重点。

参考文献:

[1] 司端锋, 韩心慧, 龙勤, 等. SIP 标准中的核心技术与研究进展[J]. 软件学报, 2005, 16(2): 239 - 250.

[2] ZHANG Y. SIP-based VoIP network and its interworking with the PSTN [J]. Electronics & Communication Engineering Journal, 2002, 14(6): 273 - 282.

[3] Voice over IP Security Alliance [EB/OL]. [2009 - 07 - 06]. http://www.voipsa.org.

[4] DENG D J, YEN D J. Quality - of - service provisioning system for multimedia transmission in IEEE802.11 Wireless LANs [J]. IEEE Journal on Selected Areas in Communications, 2005, 23(6): 1240 - 1252.

[5] EDNEY J, ARBAUGH W A. Real802.11 Security: WiFi Protected Access and 802.11i [M]. Reading, Massachusetts: Addison-Wesley, 2003.

[6] Signalling System #7(SS7) [EB/OL]. [2009 - 07 - 05]. http://www.itu.int/ITU-T/.

[7] FRIEDMAN T, CACERES R, CLARK A. RTP control protocol extended reports, RFC3611 [S/OL]. [2009 - 06 - 25]. http://www.rfc-editor.org/rfc/rfc3611.txt.

[8] WinEyeQ [EB/OL]. [2009 - 06 - 07]. http://www.touchstone-inc.com/wineyeq.htm.

[9] International Telecommunication Union. The E-model, a computational model for use in transmission planning, G.107 [S], 2000.

[10] International Telecommunication Union. Methods for subjective determination of transmission quality [S], 1996.

[11] International Telecommunication Union. Subjective performance assessment of telephone-band and wideband digital codes [S], 1996.

[12] International Telecommunication Union. Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs [S], 2001.

(上接第 308 页)

6　结语

本文针对 IXP2850 将 Tuple 空间分割思想结合到 BV 算法中,实现一种适用于网络处理器的改进算法——Tuple-BV 算法,该算法通过 Tuple 分割,缩短位向量长度,减少了存储读取次数,提高了包分类的处理速度,该算法适用于大型网络环境中,为网络处理器实现包分类算法提供了借鉴和经验。

参考文献:

[1] LAKSHMAN T V, STIDIALIS D. High speed policy-based packet forwarding using efficient multi-dimensional range matching[C]// Proceedings of ACM SIGCOMM '98. New York: ACM, 1998: 203 - 214.

[2] IYER S, RAO KOMPELA R, SHELAT A. Architecture for fast and flexible packet classification [J]. IEEE Network, 2001, 15(2): 33 - 41.

[3] 郑凯. 高性能 IP 路由查找和分组分类技术的研究[D]. 北京: 清华大学, 2006.

[4] 肖小林. 基于网络处理器的包分类引擎设计与实现[D]. 长沙: 湖南大学, 2006.

[5] 郑裕峰. 高速包分类协处理器及网络平台研究[D]. 合肥: 中国科学技术大学, 2007.

[6] Intel Croporation. Intel IXP2850 Network Processor, Hardware Reference Manual[M]. [S. l.]: Intel, 2004: 1 - 3.

[7] 张宏科, 苏伟, 武勇. 网络处理器原理和技术[M]. 北京: 北京邮电大学出版社, 2004. 郑裕峰. 高速包分类协处理器及网络平台研究[D]. 合肥: 中国科学技术大学, 2007.

[8] SRINIVASAN V, SURI S, VARGHESE G. Packet classification using Tuple space search[C]// Proceedings of ACM SIGCOMM '99. New York: ACM, 1999: 135 - 46.