基于MIH的FMIPv6切换方案的改进

张载龙,郑 伟
(南京邮电大学 信息网络研究所 江苏 南京 210003)

摘 要:在下一代异构网络环境中为移动用户提供无缝切换以及更优的体验质量是人们面临的一大挑战。尽管FMIPv6一定程度上减小了切换的时延,但还是存在切换发起时延过大,以及无法满足垂直切换的需求等缺点。提出了一种基于IEEE 802.21 MIH(与介质无关切换)服务的FMIPv6改进机制。利用MIH信息服务优化了接入路由发现以及接入点(AP)发现过程。利用MIH事件服务优化了FMIPv6的切换过程。通过性能分析可以发现,改进机制减小了切换发起时间增加了预应式切换的可能性,减小了AP发现时间,同时也减小了切换时延。

关键词:与介质无关的切换;快速切换;异构切换
中图分类号:TP393 **文献标识码**:A **文章编号**:1673-629X(2010)07-0132-04

Optimized FMIPv6 Handover Scheme Based on MIH

ZHANG Zai-long, ZHENG Wei
(Ins. of Info. Network, Nanjing Univ. of Posts and Telecomm., Nanjing 210003, China)

Abstract: How to accomplish fast and seamless handover, and how to guarantee the users a seamless experiences in the heterogeneous networks are the critical challenges we're facing. Although Fast Mobile IPv6 reduces the long handover delay, it has some constraints. Propose an enhanced FMIPv6 based on IEEE802.21 MIH services. Use the information service provided by MIH function to optimize the access router discovery and access point discovery. Also use MIH event service to optimize the handover of FMIPv6. Through the analysis we present in the paper, can see that when our proposed mechanism is applied, it increases the probability of predictive mode of operation and reduces the overall expected handover latency in FMIPv6.

Key words: MIH; FMIPv6; heterogeneous handover

0 引 言

当今,移动终端以及各种便携设备往往是配备了多种无线网卡的多模设备。移动设备所处的网络有可能是一个混合型异构网络,包括多种接入技术,例如WiFi,WiMAX,UMTS等等。它们的核心网络都是全IP网络。为了让用户能够在这种全IP的混合网络中享受无缝漫游服务,必须采用相应的垂直切换机制来保障用户应用的服务质量(QoS, Quality of Service)。在异构网络中切换性能的控制是端到端时延和丢包率控制的至关重要的一个部分,它对能否为实时业务提供可靠的QoS保障产生直接影响[1]。切换性能主要体现在切换时延上[2]。这里主要讨论采用移动IPv6(MIPv6, Mobile IPv6)的切换,其切换时延主要包括二层的切换时延和三层的切换时延。二层的切换时延是从移动节点(MN, Mobile Node)与先前的接入点(PAP, Previous Access Point)断开到连接上新的AP(NAP, New Access Point)这段时间。三层的切换时延包括移动探测、地址配置、绑定更新等时延[3]。

VoIP等实时性业务对切换时延都有很高的要求。为了降低切换时延,IETF对MIPv6进行了改进,所提出的MIPv6快速切换(FMIPv6, Fast Mobile IPv6)通过二层触发让MN在二层切换之前提前获取新的转交地址(NCoA, New Care-of Address),从而降低切换时延。同时FMIPv6还应用缓存机制,在先前的接入路由器(PAR, Previous Access Router)和新接入路由器(NAR, New Access Router)之间建立隧道,来降低丢包率。但是FMIPv6也存在其局限性:

1)在MN高速移动的情况下,FMIPv6有可能由预应式切换转变为反应式切换,这样切换时延将会大大增加,因此切换性能就得不到保证[4]。

2)FMIPv6只是简单地根据信号来判断是否需要进行切换,它只适合于水平切换的情况[5]。在异构情况下,需要综合考虑多方面的因素,例如用户偏爱、计

收稿日期:2009-11-01;**修回日期**:2010-02-20
基金项目:江苏省高新技术研究计划(BG2003001)
作者简介:张载龙(1966-),男,江苏淮安人,副研究员,研究方向为普适计算关键技术、计算机通信与网络、下一代电信网络关键技术。

费成本、上层业务需求等等。异构情况下切换决策是一种多目标的决策。因此要求系统能够采集到候选目标网络的更多参数,然后进行比较,最后计算出最优的目标网络。

在切换发生之前,MN 需要通过不断的信号扫描来发现 AP,从而获得周围可用 AP 的信息,以为将来的二层或者三层切换做准备。但是完成信号扫描需要数百毫秒的时间[6],这个期间显然网卡是处于工作状态的,需要消耗节点的能量。因此对于能量有限的节点来说,有效地减少信号扫描时间成为研究的目标[7]。

文中利用与介质无关的切换(MIH, Media Independent Handover)对 FMIPv6 进行了改进,提出了一种 FMIPv6 的改进机制,减小了切换时延,增大预应式切换的几率。另外,利用 MIH 的信息服务为 MN 的信号扫描提供了有用信息,从而有效地减少了 AP 发现的时间,进而减小了 MN 的能量消耗。

1　相关研究

1.1　移动 IPv6 快速切换机制(FMIPv6)

FMIPv6 为了减小切换时延主要考虑以下问题:

1)如何让 MN 能够在探测到一个新的子网链路后立即向其发送数据;

2)如何能够让 MN 在连接到新链路上之后立即能够收到 NAR 发来的数据包[8]。

FMIPv6 中,MN 通过路由消息来获取 NAR 的网络前缀,然后利用这一网络前缀提前配置 nCoA,提前发送绑定更新(BU, Binding Update)来发起切换。同时在网络发起阶段,FMIPv6 还利用了链路层触发机制,当链路层或物理层状态发生变化,就会触发网络层,从而进行相应的快速绑定(FBU, Fast BU)操作。

快速切换又分为预应式切换和反应式切换。当 MN 在 PAR 链路上发送 FBU 并收到快速绑定确认(FBAck, Fast Binding Acknowledgment)消息的情况下,称之为预应式切换。相反,如果 MN 从 NAR 链路发送 FBU 的情况,称之为反应式切换,这种方式下切换的时延会大大增加,因此,应该尽量避免反应式切换。图 1 为 FMIPv6 预应式切换流程图。

1.2　与介质无关的切换(MIH)

由 IEEE802.21 定义的 MIH 的目标就是通过优化异构网络中的切换机制来实现用户无缝漫游,从而提高用户体验质量[9]。在 FMIPv6 中,网络层必须能够提前探测到来自链路层的切换指示,以实现无缝的切换。因此,需要采用 MIH 来提供链路层触发功能。

MIH 定义了一个介于网络层和链路层之间的与介质无关的切换功能实体(MIHF, Media Independent Handover Function),如图 2 所示,它能够提供三种服务[10]:与介质无关事件服务(MIES, Media Independent Event Services)、与介质无关命令服务(MICS, Media Independent Command Services)、与介质无关信息服务(MIIS, Media Independent Information Service)。

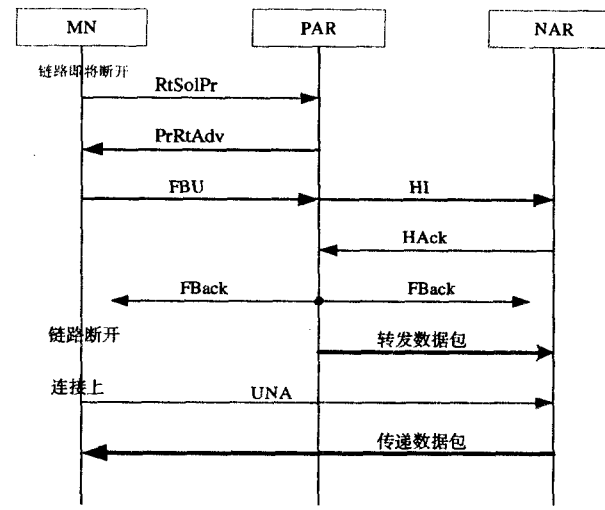

图 1　FMIPv6 预应式切换流程图

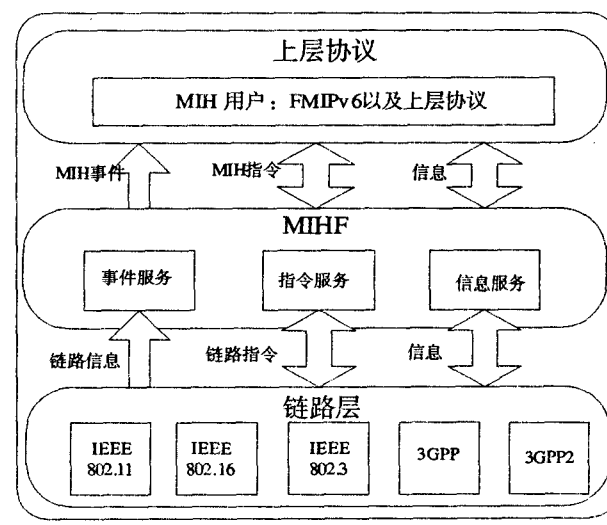

图 2　MIHF 位置及其服务

2　改进的 FMIPv6 切换方案

考虑如图 3 所示的移动场景,MN 是一个双模移动终端,配有 802.16 和 802.11 网卡,当前接入网络是 802.16 网络,且将从 802.16 网络移动到 802.11 网络中,所以将发生垂直切换。

当 MN 接入到当前网络时,MIHF 首先进行一些初始化操作,用来发现提供 MIH 服务的网络实体,这里信息服务器(IS, Information Server)的位置由 DHCP 服务器来提供[9]。切换操作信令流程如图 4 所示,具体描述如下:

(1)MN 通过 MIH_Get_Information_Request 消

息向 IS 请求邻居可用的邻居网络信息以及可用 AP 的信息。这一消息请求可以是在 MN 连接到一个新的服务网络的时候进行，MN 发现 nAP 时进行，或者周期性地进行[9]。这里考虑到 MN 的能量有限，无线信道的带宽有限，因此采用第一种方式。

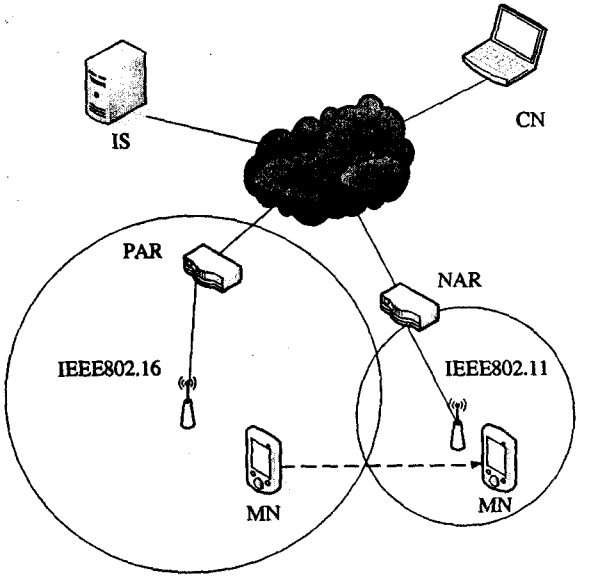

图 3 切换场景

(2)当接收到请求消息后，IS 会根据请求中的位置信息(如不包含位置信息，IS 会根据 MN 的三层地址信息来推测出它的大概位置)查询数据库，然后向 MN 返回一个 MIH_Get_Information_Response 响应消息，包含邻居网络的信息，以及邻居 AP 的信息。

(3)当 MN 接收到的信号强度逐渐变小的时候，其 MIH 层就会向上层通告 Link_going_down 事件，从而进入切换决策阶段。根据 IS 提供的候选网络的相关信息，决策机可以根据用户偏爱以及 QoS 限制选择出最佳的候选网络作为切换的目标网络，这里假设选择的是 802.11 网络。

(4)MN 向 PAR 发送 FBU，当 PAR 接收到 FBU 后向 NAR 发送切换发起(HI，Handover Initiate)消息。在接收到 HI 后，NAR 为 NCoA 执行重复地址检测(DAD，Duplicate Address Detection)以确定其是否可用，然后回送切换确认(HAck，Handover Acknowledge)消息，收到 HAck 之后 PAR 向 MN 和 NAR 双播快速绑定确认(FBack，Fast Binding Acknowledgment)消息。在这个期间 PAR 和 NAR 分别需要向 PAP 和 NAP 注册 link_down 和 Link_up 事件。

(5)当 MN 和旧的链路断开的时候，PAP 的 MIHF 会向 PAR 的 MIHF 通告 link_down 事件，收到此事件后 PAR 就会向 NAR 转发发向 MN 的数据，NAR 对其进行缓存。然后 MN 开始二层切换。MN 与 AP 连接上之后，NAP 的 MIHF 就会向 NAR 的 MIHF 通告 link_up 事件，然后 NAR 就开始向 MN 转发缓存的数据。而无需等待主动邻居公告(UNA，Unsolicited Neighbor Advertisement)消息。至此切换完成。

3 性能分析

3.1 时延分析

FMIPv6 时延可以分为切换发起时延 D_{init} 和切换时延 D_{ho}。这里忽略 MIH 用户与 MIHF 之间的本地交互时延，不考虑实体内部的程序运行时间。

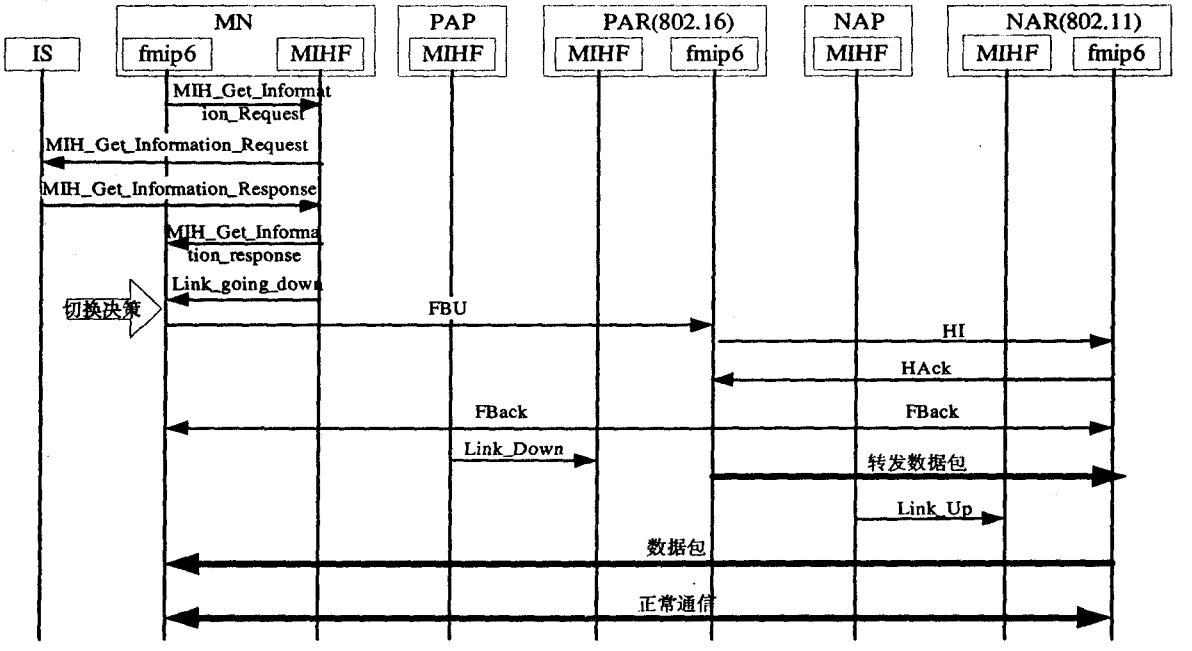

图 4 切换信令流程图

对于传统的 FMIPv6 在切换发起阶段首先需要交互 RtSolPr/PrRtAdv(Router Solicitation for Proxy Advertisement/ Proxy Router Advertisement,路由代理公告请求/代理路由器公告)[11],然后再发送 FBU,根据图 1 的流程图可知:

$$D_{init} = D_{RtSolPr} + D_{PrRtAdv} + D_{FBU} = 3D_{MN-PAR}$$

其中 D_{MN-PAR} 为 MN 到 PAR 之间的时延,这一时延包括 MN 到 PAP 的时延 D_{MN-PAR},以及 PAP 到 PAR 之间的时延 D_{MN-PAR}。同样下面的 D_{MN-PAR} 也类似。

而我们提出的方案中切换发起阶段不需要 RtSolPr/PrRtAdv 的交互,MN 在很早之前就可以通过 IS 获知邻居网络的信息[12],因此:

$$D_{init} = D_{FBU} = D_{MN-PAR}$$

显然,我们提出的方案中,切换发起时间减少了。减少切换发起时间会增加执行预应式切换的可能性,尤其是在终端快速移动以及重叠区域有限的情况下。

切换时延 D_{ho} 为 MN 无法接收到数据包的这段时间;D_{L2} 为 MN 执行二层切换所需的时间。在传统的 FMIPv6 切换方案中,当 PAR 发送完 FBAck 以后,就开始向 NAR 转发数据包,因此 D_{ho} 为从 PAR 发送完 FBAck 到接收到 NAR 转发的数据包的这段时间,因此:

$$D_{ho} = D_{MN-PAR} + 2D_{MN-NAR} + D_{L2}$$

在我们提出的方案中,是当 PAP 触发了 link_down 事件后 PAR 才开始数据的转发,因此其转发时间要晚于原始的方案。而当二层切换完成后 NAP 会向 NAR 触发 link_up 事件[13],然后 NAR 立即向 MN 转发缓存的数据包而无需等待 UNA 消息,所以转发的时刻要早于原始的方案。切换时延如下所示:

$$D_{ho} = D_{PAP-PAR} + D_{L2} + D_{NAP-NAR} + D_{MN-NAR}$$

通过上面的分析可以发现,提出的方案无论是切换发起时延还是切换时延都有了显著的降低,切换得到了优化。

3.2　AP 发现时间

在 MN 执行二层切换之前首先要进行新的 AP 发现,因此 MN 需要通过信号扫描来发现 AP[7]。由于 MN 的能量有限,所以应该避免网卡的持续扫描,同时应尽量减小扫描时间,通常采用一种间隔性的扫描方法来减少能量损耗。在没有 MIIS 信息辅助的情况下,MN 需要扫描所有的信道。

MIIS 服务器可以通过 MIH_Get_Information Response 中的信息元素(IEs, Information Elements)来向 MN 提供邻居 AP 的信息。其中一个有用的 IE 就是 TYPE_IE_POA_LOC - ALTION 它包含了 AP 的物理位置。如果 MN 获取了附近 AP 的位置信息,那么它就可以在其移动到该 AP 覆盖范围内时才打开其无线接口。IEEE802.21 标准定义了 TYPE_IE_POA_CHANNEL_RANGE 代表在某频率下 AP 的信道范围。有了这些 IE 的辅助,MN 就可以提前获取一个可用信道的列表,提前知道哪些邻居 AP 将可用。在进行信道扫描时就无需扫描所有的信道,只需要有选择性地扫描可用的信道。这样不仅减少了 AP 发现时间,同时还减少 MN 能量消耗。

4　结束语

提出了一种基于 MIH 的 FMIPv6 的改进方案。首先利用 MIH 的 MIIS 服务向 MN 提供了有用的邻居网络的信息,从而有效降低了切换发起时延。同时在 MIH_Get_Information Response 消息中还包含了有用的邻居 AP 的信息,从而减小 AP 发现时间,进一步减小了二层的切换时延,同时也减小了能量的损耗。在切换执行阶段,利用了 MIH 的 MIES 服务,通过相应的事件来触发数据包转发,从而有效地降低了切换时延和所需的缓存。在未来的研究工作中将对这一方案进行仿真研究,同时考虑利用 MIH 的指令信息 MICS 来为切换提供更多的动态信息,从而使切换决策更加智能化。

参考文献:

[1] 陈山枝,时　岩,胡　博.移动性管理理论与技术的研究[J].通信学报,2007(10):123-133.

[2] 郭　强,朱　杰,徐向华.一种无线异构网无缝切换控制方案及其仿真分析[J].上海交通大学学报,2004(12):2023-2029.

[3] Kim M, Moon T W, Cho S J. A Study on IEEE 802.21 MIH Frameworks in Heterogeneous Wireless Networks[C]// 11th International conference on Advanced Communication Techenology. Proceedings. [s.l.]:[s.n.],2009:242-246.

[4] 乔红麟,马　跃. MIPv6 与 FMIPv6 切换性能分析与优化[J].计算机工程,2007(18):119-121.

[5] Mussabbir Q B, Yao Wenbing, Niu Zeyun, et al. Optimized FMIPv6 Using IEEE 802.21 MIH Services in Vehicular Networks[J]. IEEE Transactions on Vehicular Technology, 2007,56(6):3397-3407.

[6] IEEE 802.11, Part 11: wireless lan medium access control (MAC) and physical layer (PHY) specifi cations[S]. 1999.

[7] 徐　灏,李德敏,侯广进.一种基于移动的 Ad Hoc 网络分层位置管理方案[J].计算机工程与应用, 2006(29):111-113.

[8] Koodli, Ed. Mobile IPv6 Fast Handovers[S]. RFC 5268, IETF,2008.

(下转第 148 页)

数据库的访问和操作采用 EJB 组件;漏洞信息存储数据库选用关系数据库管理系统(Microsoft SQL Server)。系统的组成与逻辑结构如图 2 所示。

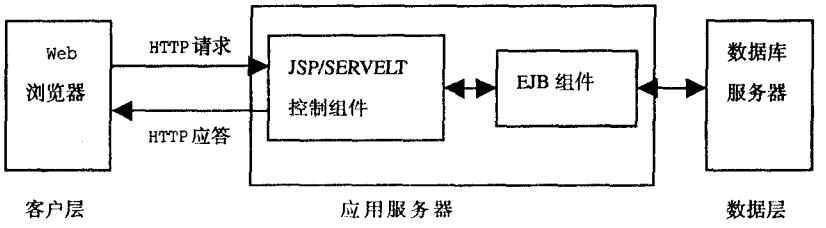

图 2 B/S 模式系统工作原理图

(1)客户层。客户层的浏览器通过 URL 访问应用层的 Web 服务器,由 Web 服务器产生供普通用户使用的服务界面和对漏洞信息存储数据库中的漏洞数据进行发布、更新、查询、删除等管理人员使用的界面,用来输入信息并反馈信息处理结果。

(2)应用服务器层。应用层负责响应浏览器的请求并连接数据库管理系统,在 Web 服务器内配置 JSP 组件以产生动态的页面和调用应用服务器内的 EJB 组件[11];在应用服务器内配置 EJB 组件以访问数据库并对数据进行必要的处理。该层的功能具有很好的扩充性,根据需要可以方便地添加或删除组件。

(3)数据层。规划数据层,首先要选择数据库管理系统(Microsoft SQL Server);并且根据前面对电信网的安全漏洞数据的描述,高效规划和组织数据信息,设计关系数据库模型,构建数据库。这样就建立起了电信网安全漏洞特征数据库,这一漏洞数据库是在深入分析 CVE 漏洞的特征的基础上建立起来的,能够准确详尽地描述各个漏洞的特征,便于用户根据自己的需要进行检索。同时,由于许多新的漏洞不断出现,加之人们对已有漏洞认识的不断加深,对数据库的及时更新是十分重要的。因此,必须加强对数据库的维护,及时更新数据库数据,查漏补缺,对漏洞数据库不断地进行完善[12]。

漏洞数据库的主要目的是便于用户查询检索,这样漏洞数据库才有意义。设计提供如下检索:漏洞名称(模糊查询)、CVE 编号(精确查询)、漏洞级别(分类查询)、漏洞类型(分类查询)、攻击效果(分类查询)、攻击类型(分类查询)、受影响系统(模糊查询)、关键词(模糊查询)。另外,还有供管理员操作的添加、删除、更新等功能。

5 结束语

文中对电信网漏洞分类描述及表示模型进行了较为深入的探讨,并基于 J2EE 设计了一种分布式电信网安全漏洞数据库管理系统,可以利用 Web 浏览器在不同地方存储、查询和修改各种电信网漏洞的数据,将来也可为电信网安全防御研究人员和普通用户提供数据支持和电信网安全防御方案的支持。

参考文献:

[1] Bishop M. A Taxonomy of UNIX System and Network Vulnerabilities[R]. Department of Computer Science at the University of California at Davis,1995:12-35.

[2] 单国栋,戴英侠,王 航. 计算机漏洞分类研究[J]. 计算机工程,2002,28(10):3-6.

[3] 那成亮,周廷显,王晓锋. 无线局域网的安全漏洞分析[J]. 遥测遥控,2003,24(5):35-37.

[4] Common Vulnerabilities & Exposures[EB/OL]. 2004-08-25. http://www.cve.mitre.org.

[5] Krsul I. Software vulnerability analysis[D]. USA: Department of Computer Sciences, Purdue University,2005.

[6] 方 杰,袁修贵. 基于 J2EE 规范的电信综合网管架构设计[J]. 电脑与信息技术,2005,13(5):35-38.

[7] 张 冰. 电信网网络安全漏洞与补丁管理研究[J]. 电信网技术,2006(7):14-18.

[8] 刘 波,刘 惠,胡华平,等. 计算机漏洞库系统的设计、实现与应用[J]. 计算机工程与科学,2004,26(7):31-33.

[9] 史斌星,史 佳. JAVA 基础编程贯通教程[M]. 北京:清华大学出版社,2003.

[10] 乔佩利,王春英,张 军. CVE 漏洞库体系的研究与实现[J]. 哈尔滨理工大学学报,2004,9(5):70-72.

[11] 刘 殡,唐朝京,张森强. 基于网络的安全漏洞分类与扫描分析[J]. 信息与电子工程,2004,2(4):318-320.

[12] 翟 钰,张玉清,武维善,等. 系统安全漏洞研究及数据库实现[J]. 计算机工程,2004,30(8):68-70.

(上接第 135 页)

[9] IEEE Standards Association. Draft IEEE standard for local and metropolitan area networks: media independent handover services[S]. IEEE 802.21.2008.

[10] Huang H H, Wu J S. A Pre-Binding Update Fast Handover Control Using IEEE 802.21 MIH over 802.16e Networks [C]//2009 WRI International Conference on Communications and Mobile Computing. [s.l.]:[s.n.],2009:417-421.

[11] 雷飞鹏,唐伦,陈前斌. 采用 IEEE802.21 MIH 服务优化 FMIPv6 切换的方案[J]. 通信技术,2007(9):52-53.

[12] An Y Y, Lee K W, Kum D W, et al. Enhanced fast handover mechanism using MIH services in MIPv6[J]. Wired/wireless Internet communication,2006,3970: 120-131.

[13] 唐 宏,陈前斌,吴中福,等. 移动 IP 技术中 L2-Trigger 方法研究[J]. 重庆邮电学院学报:自然科学版,2003(4):88-91.