移动互联网访问控制支持移动感知的研究*)

李 军[1,2,3] 王 淼[1,3] 张瀚文[1,3] 叶新铭[1,2]
(中国科学院计算技术研究所 北京 100080)[1] (内蒙古大学计算机学院 呼和浩特 010021)[2]
(中国科学院研究生院 北京 100080)[3]

摘 要 移动互联网的访问控制使移动 IPv6 面临切换延迟显著增加的困境。本文在分析移动 IPv6 协议特点与访问控制机制行为特征的基础上,提出了一种在移动互联网访问控制应用中实现快速移动感知的方法,它能有效缩短移动 IPv6 切换前的认证等待时间。文中给出了实现方法,进行了比较分析。

关键词 访问控制,移动 IPv6,移动感知

Supporting Mobile-awareness in Mobile Internet Access Control

LI Jun[1,2,3] WANG Miao[1,3] ZHANG Han-Wen[1,3] YE Xin-Ming[1,2]
(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)[1]
(College of Computer Science of Inner Mongolia University, Hohhot 010021)[2]
(Postgraduate School of Chinese Academy of Sciences, Beijing 100080)[3]

Abstract In mobile Internet environment, MIPv6 suffers from increased handover latency because of access control's cut-in. A fast mobile-awareness method for access control is proposed based on the analysis of MIPv6 protocol and access control's behavior to reduce waiting time. And its implementation and evaluation is given.

Keywords Access control, Mobile IPv6, Mobile-awareness

1 引言

网络的访问控制是网络安全防范和保护的主要策略,它的主要任务是保证网络资源不被非法使用和非常访问,也是维护网络系统安全、保护网络资源的重要手段。可以说,访问控制是保证网络安全最重要的核心策略之一。在这方面 IETF 和 IEEE 都发布了很多相关的标准[1,2],而且几乎所有的 ISP 也在其运营网络中采用了入网访问控制,并为此部署了大量的基础设施。

移动 IPv6(Mobile IPv6,MIPv6)协议[3]是 IETF 发布的标准,它使 IPv6 协议[4]能够支持主机移动性。在 MIPv6 协议中定义的"移动"更强调"连续性"。首先是寻址的连续性,支持 MIPv6 协议的移动主机(Mobile Host,MH)的家乡地址(Home Address,HoA)在其活动期内是固定不变的。当某个通信节点(Correspondent Node,CN)希望与 MH 通信时,无论 MH 身在何处,CN 都可以将 MH 的 HoA 作为目标地址寻址到 MH 当前所在的网络位置。其次是网络连接的连续性,MH 在发生网络切换后,由于作为连接标识之一的 IPv6 地址 HoA 没有改变,原来的网络连接,例如 TCP 或者是 UDP 的连接,可以继续保持,不需要重新进行连接,而且不需要对 TCP 等上层协议做任何改动。由于 MIPv6 具有以上的寻址连续性和网络连接连续性,加上不断改进的切换性能,使得 MH 获得了一定服务质量的连续性。

然而,虽然 MIPv6 协议是一个独立的协议,其功能相当于 IPv6 协议的一个路由协议,但是它是 IPv6 协议整体中的一个有机的组成部分,并不能脱离 IPv6 协议单独发挥作用。因此,面对像网络访问控制这样通过 IPv6 协议层发挥作用的网络应用,MH 仍然要受其约束。这样一来,MH 必须通过网络的认证并获得授权,才能够向网络发送或者接收消息。这就破坏了 MIPv6 的连续特性,降低了 MH 可获得的服务质量。究其原因,是目前的访问控制方法没有考虑移动互联网环境对快速切换的实际需求,因而不支持移动感知,无法根据需要快速启动认证,以减少不必要的等待时间。

本文提出了一种使访问控制支持 MIPv6 移动感知的方法,能够使身份认证随着网络切换自动完成,缩短了 MH 的认证等待时间,从而减小了切换延迟,在一定程度上保证了 MH 可获得的网络服务的质量。文章第 2 节介绍本文研究的背景和相关工作分析;第 3 节详细阐述本文提出的快速移动感知方法;第 4 节介绍具体的实现;第 5 节给出比较分析;最后总结全文。

2 研究背景

2.1 移动 IPv6

IPv6 协议及其有机组成部分 MIPv6 协议是专门为解决目前 IPv4 协议面临的困境而制定的:IPv6 协议具有比 IPv4 协议更大的可用地址空间;MIPv6 比 MIPv4 能够更好地支持主机的移动性;IPv6 协议支持可预见的时期内可能的扩展等等。

参见图 1,MH 是支持 MIPv6 协议的主机,它有至少一个固定的由其注册网络分配的 IPv6 地址,即家乡地址 HoA。它的注册网络就被称为家乡网络(Home Network),除了家乡网络以外的其它网络称为外地网络(Foreign Network)。每当 MH 移动到一个外地网络或者在一个外地网络中启动时,它就可以通过当地访问路由器(Access Router,AR)广播的路

*)北京市科技计划项目:无线移动互联网络的商用认证、授权和计账(AAA)系统(Y0104002000091)资助。李 军 博士生、内蒙古大学讲师;王淼、张瀚文 博士生;叶新铭 博士生导师、教授。

由器宣告(Router Advertisement,RA)来确定自己的位置并获得转交地址(Care-of Address,CoA)等相关的网络配置信息[5],见图1中的消息①。然后,它会向位于家乡网络的一个称为家乡代理(Home Agent,HA)的固定节点发出绑定更新消息(Binding Update,BU),见图1中的消息②,该消息中含有地址对〈HoA,CCoA〉,其中CCoA是MH的当前转交地址(Current CoA)。HA收到BU后,会更新自己保存的对应的MH的〈HoA,CCoA〉地址对,并向MH发回绑定应答消息(Binding Acknowledge,BA),见图1中的消息③。消息②和消息③构成的过程称为家乡登记。

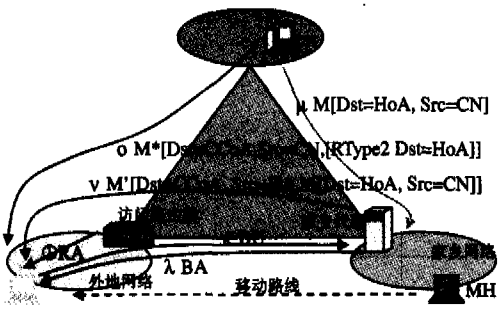

图1 MH在切换网络时的通信

这个过程完成后,HA才能够利用代理邻居发现机制[6],代表离家的MH收下送达家乡网络的目的地是MH的HoA的数据包,见图1中的消息④,并通过目的地是MH的CCoA的隧道转发给MH,见图1中的消息⑤。另外,MH可选择将HoA为选项、CCoA为源地址,直接把数据包发给CN。这样,当CN再次向MH发数据包时,就可以将HoA为选项、CCoA为目标地址直接发向MH,而不必再绕道HA了,见图1中的消息⑥,这一过程称为"三角路由优化"。这样,前面提到的寻址连续性和连接连续性得以实现。

2.2 网络访问控制

一般的访问控制方法的组成如图2所示。访问路由器部分包含转发控制、认证管理以及合法地址池,认证管理部分又由身份认证过程和定时器组两部分组成。移动主机部分只包括身份认证组件。图中的实心箭头表示控制流,空心箭头表示数据流。合法地址池用来保存那些获得授权的MH的CCoA(如果MH是在家乡网络,则保存的是MH的HoA)。后台服务器并非是必需的,它专司认证职责,可以协助AR完成对MH的认证。

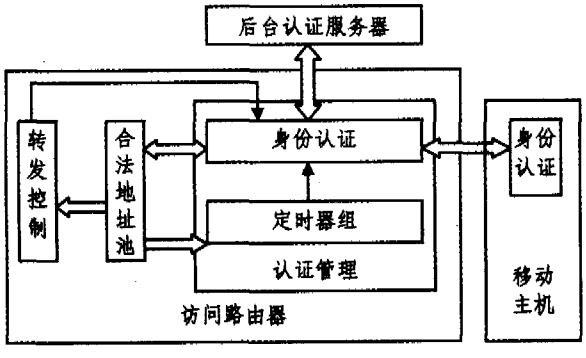

图2 网络访问控制基本组成

身份认证过程是AR与MH交换消息的过程。一般情况是MH首先向AR发认证开始消息Auth_Start;AR回复MH认证请求消息Auth_Req;MH收到Auth_Req后,将自己的认证信息包含在认证应答消息Auth_Ack中,发给AR;AR依据Auth_Ack中包含的认证信息对MH进行认证,或者将认证信息转发给后台的认证服务器,最后将认证结果Auth_Result发给MH。根据认证的结果,AR分别采取如下行动之一:(1)如果认证结果是"成功",AR将MH的地址加入到合法地址池(如果不存在),将该地址的定时器复位,并将认证结果通知给MH;(2)如果认证结果是"失败",删除合法地址池中MH的地址(如果存在),并将结果转发给MH。以上过程中的Auth_Start不是必需的,AR可以在未收到Auth_Start的情况下直接向MH发Auth_Req。但是一般Auth_Req不能被省略,因为其中含有身份认证必需的信息,如临时质询字(Nonce Challenge)或者是随机数等等。

合法地址池中的每个地址条目对应一个专用定时器,该定时器在每次认证成功时复位,随时间递减。每当定时器到时,就要求对应的MH重新进行身份认证,AR向MH发Auth_Req,开始一轮身份认证消息交互过程。定时器池中的定时器还为身份认证过程提供定时服务,因为任何一轮认证过程都是有时间限制的。当超过规定的时间还没有完成认证或没有收到指定的消息,则默认为是认证失败。

转发控制专门检查每个需要转发的数据包,以决定是否允许该数据包被转发。一般的转发控制的处理流程是:当有数据包需要转发时,就在合法地址池中查找是否有匹配的地址。如果找到,则转发数据包,否则就将数据包丢弃。

2.3 访问控制对MIPv6的影响

由前面的介绍可知,切换过程是影响MIPv6应用性能的关键环节,切换过程耗时长短在很大程度上影响了上层网络应用可获得的服务质量。

在一般情况下,在MH检测到新的网络到完成移动切换之间,要完成以下步骤:(1)地址自动配置;(2)与HA进行家乡登记过程;(3)如有必要,与CN进行三角路由优化过程。

但是在有访问控制的网络中,这个过程被延长了。确切地说,是在前面步骤中的(1)和(2)之间增加了如下步骤:(1-a)MH发现发生了移动而且需要认证;(1-b)开始认证,认证交互操作;(1-c)认证处理。只有在认证的结果是成功的情况下,前面的步骤(2)和(3)才可能继续。在这之前,MH不能经由AR发送和接收任何其它消息,包括家乡登记消息,那么MIPv6所追求的寻址的连续性和网络连接的连续性就被中断了。所以,减少(1-a)至(1-c)的时延,能够有效降低访问控制对移动IPv6切换性能的不利影响。

虽然目前有多种方法[7,8]整合了认证过程中的步骤(1-c)和移动切换过程步骤(2),但是在缩短步骤(1-a)和(1-b)的时延方面并未有明显效果。因为每次切换要等待用户发现移动再进行认证交互操作[9],显然是繁琐耗时的,所以有必要研究在访问控制中支持移动感知,并采用能自动完成身份认证的方法,以加速步骤(1-a)和(1-b),从而进一步减小访问控制对移动切换的不利影响。

2.4 MIPv6协议栈

通过在网络节点的IPv6协议栈中嵌入MIPv6,就能够使该网络节点也能够支持MIPv6协议。当然,IPv6协议自己原本也是完整的,没有MIPv6照样能正常运转,只是不支持主机的移动性而已。

图3是嵌入MIPv6后的TCP/IP协议栈示意图。IPv6协议中的各个组成部分的层次顺序保持不变,MIPv6嵌入在IPv6协议基本功能子层与其它子层之间,但并不完全隔离IPv6基本功能子层和其它子层,因为并不是所有的数据包都需要MIPv6子层来处理。另外,TCP、UDP等上层协议以及以太网等下层协议不需要做任何改动。IPv4协议更不会受

到任何影响。

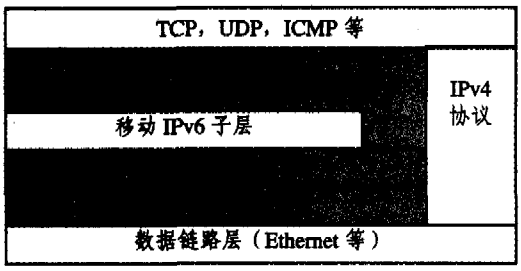

图 3　嵌入 MIPv6 后的 TCP/IP 协议栈

MIPv6 子层能最先得知发生了移动，如果需要从移动 IPv6 子层向应用程序传递这个信息，那么使用最基本的网络协议消息是最适当的了。因为移动 IPv6 子层本身就在网络协议栈中，在各个协议栈之间传递网络协议消息，比采用其它消息机制更便捷，而且开销更低。

3　访问控制中的移动感知

3.1　AR 被动移动感知

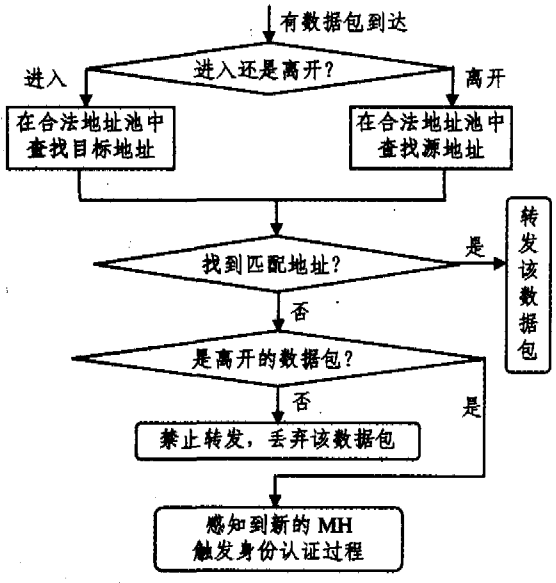

图 4　支持被动移动感知的转发控制处理流程

在访问路由器上，具有被动感知能力的转发控制流程如图 4 所示。其中“离开”是指经由 AR 离开其管辖的网络，“进入”是指经由 AR 进入其管辖的网络。凡是进入的数据包的目标地址或者是离开的数据包的源地址，只要在合法地址池中，都允许转发，否则不允许转发。转发控制的具体流程如下：(1)对达到的数据包根据其流向判断是离开的数据包还是进入的数据包；(2)如果是进入的数据包，则在合法地址池中查找目标地址；如果是离开的数据包，就在合法地址池中查找源地址；(3)如果在合法地址池中找到了匹配的地址，那么就认为该数据包是要到达或者是来自经过授权的 MH，允许转发，流程结束。(4)如果未在合法地址池中找到匹配的地址，那么再根据是离开的数据包还是进入的数据包进行如下操作：a) 如果是进入的数据包，那么说明该数据包的目的地 MH 未经授权，本方法不对这类情况做进一步处理，只简单地丢弃该数据包，流程结束。b) 如果是离开的数据包，那么说明该数据包的源 MH 未经授权，本方法将该源 MH 移交给身份认证过程，触发该对 MH 的认证，流程结束。

需要加以说明的是，对于被禁止转发的离开数据包，AR 认为是来自刚刚进入其管辖网络的 MH，则触发身份认证过程，向该数据包的源 MH 发出 Auth_Req 消息。也就是说，AR 能够感知到有新的 MH 移动到本网络，那么就应该立即启动对该 MH 的身份认证过程，以减少认证前的等待时间。

3.2　MH 主动移动感知

然而，只有 AR 具有移动感知能力是不够的。为了让 MH 的身份认证过程能够及时得知发生了移动，并自动开始认证过程，在 MIPv6 协议中需要加入必要的扩展，插入一个移动通知过程。

如图 5 所示，虚线框部分是 MIPv6 协议子层。在 MIPv6 子层中，原有的移动检测过程之后执行移动通知过程，通知身份认证过程已经发生了移动，其中也包括将获得的 AR 的信息通知给身份认证过程。这时的身份认证过程由于提前感知到了移动的发生，因而尽早主动发出 Auth_Start 给 AR，开始一轮身份认证过程。紧接着的 Auth_Ack 是依据事先缓存下来的身份信息和 Auth_Req 中的请求信息自动完成的，避免重复人工输入。

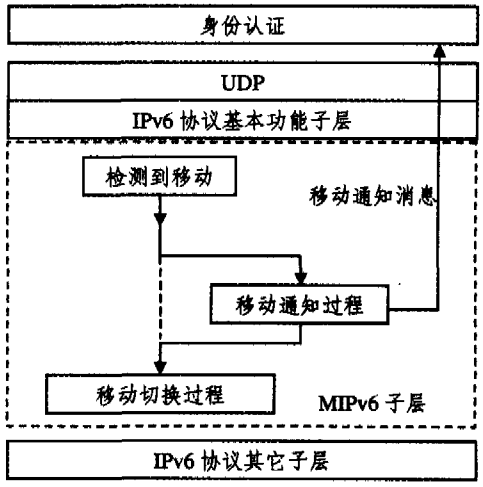

图 5　移动通知过程的工作原理

移动通知过程是被插在移动检测之后的。这样，一旦发生移动，身份认证过程能够立即获知(且先于移动切换过程得到了移动通知)。身份认证过程因为及早得知发生了移动，所以可以尽早启动认证过程，进一步减少了身份认证前的等待时间。

如前面曾描述的，这里移动通知过程传给身份认证过程的信息是包含在网络消息中的。网络消息穿过网络协议栈十分便捷而且代价非常小。身份认证过程只要在约定的接口等待接收该网络消息就可以了。

4　实现方法

Linux 的 Netfilter 网络框架[10]提供了一个实现本文方法中的 AR 端的途径。另外，通过扩展 MIPL[11]的 MIPv6 协议栈，可以实现本文方法的 MH 端。实践证明，本文给出的方法切实可行，达到了在移动互联网的访问控制中支持快速移动感知的目的，有效地减少了认证前等待时间，从而提高了移动 IPv6 的切换性能。

4.1　AR 端被动感知的实现

转发控制处理程序一般是运行在内核空间的、挂接在 NF_IP6_FORWARD 的钩子函数。它通过作为参数传入的指针(struct sk_buff * * skb)逐个检查过往的数据包。以便确定是否转发该数据包。对允许转发的数据包的返回值是

NF_ACCEPT，不允许转发的数据包的返回值是 NF_DROP。

为了实现 AR 的移动感知，我们对上面描述的转发控制的一般方法进行了扩展。基本思想是，将那些已经被确定不允许转发的离开数据包改造为一个虚假的 Auth_Start 消息，直接传递给运行在用户空间的身份认证过程。身份认证过程会认为这是一个普通的 Auth_Start 消息，会照常发出 Auth_Req，触发对 MH 的认证。具体方法是：

(1) 检查数据包是否具有足够大的空间，以承载 Auth_Start 消息，对不满足该条件的数据包返回 NF_DROP；

(2) 否则，保留该数据包 IPv6 头部中的源地址，复制事先按规定格式构造 Auth_Start 消息。主要复制内容包括：IPv6 头部的目标地址、payload 的长度值、nexthdr，UDP 头部的源和目的端口、非零的 UDP 检验和(虽然 IPv6 要求 UDP 必须计算校验和，但目前 Linux 的 netfilter 认可任何非零的值)、len 值以及 Auth_Start 消息本身；

(3) 修改 skb 中特定字段的值，以使其符合新数据包的要求，其中主要包括

(* skb)→pkt_type = PACKET_LOOPBACK；

(* skb)→ip_summed = CHECKSUM_UNNECESSARY；

(* skb)→len=IPv6 头部长度+UDP 头部长度+Auth_Start 消息长度；

(4) 调用 netfilter 函数 ip6_input(* skb)，将 Auth_Start 消息传递给身份认证过程，返回 NF_STOLEN。NF_STOLEN 表示不需要 Netfilter 中的后续处理过程再关心该数据包。

4.2 MH 端移动感知的实现

经过仔细分析，发现在 MIPL 的 MIPv6 协议栈的实现中，每次发生移动都要调用函数 mipv6_mobile_node_moved，它运行在内核空间，执行“移动切换过程”。对其进行功能扩展，在前端插入了对“移动通知过程”的调用，并将新 AR 的信息通过参数 newrt 传递给移动通知过程。移动通知过程的具体实现方法是：

(1) 申请一块 sk_buff 空间，由指针 skb(struct sk_buff * 类型)来标识；

```
skb = alloc_skb(移动通知消息长度 + UDP 头部长度\
      + IPv6 头部长度, GFP_ATOMIC);
skb_reserve(skb, IPv6 头部长度);
skb_put(skb, 移动通知消息长度 + UDP 头部长度);
```

(2) 按规定格式构造移动通知消息，包括 IPv6 头部、UDP 头部以及移动通知消息本身(细节与前面的 Auth_Start 消息相似，此处略去)。

(3) 按以下内容给 sk_buff 的特定字段赋值，并将消息上传给身份认证应用程序：

```
skb→dev= dev_get_by_index(newrt→ifindex); /* 引
      用与新 AR 的接口设备 */
skb→pkt_type = PACKET_LOOPBACK;
skb→ip_summed = CHECKSUM_UNNECESSARY;
udpv6_rcv(skb); /* 直接传给 UDP 协议层处理 */
dev_put(dev); /* 释放对接口设备的引用 */
```

(4) 扩展 MH 的身份认证应用，在指定的 UDP 端口监听“移动通知消息”。一旦收到该消息，则立即发出正式的 Auth_Start 消息，启动身份认证过程。

最后，要注意的是，以上介绍的实现方法是在 Linux 内核空间的编程，必须遵守内核编程规范。

5 比较分析

在有访问控制的移动互联网中，MH 进行移动切换(家乡登记和路由优化)前，需要等待访问控制应用通过认证并获得授权，这段等待时间可以表示为，

$$T_W = T_D + T_A \tag{1}$$

其中，T_W 是移动切换前总的等待时间；T_D 是认证处理前的认证检测时延和认证交互时延；T_A 是认证处理时延，这个时延的长度取决于具体采用的认证方法、设备的计算速度以及网络传输时延，不作为本文的讨论内容。下面分别分析是否具有移动感知能力对 T_D 的影响。这里有

$$T_D = T_N + T_M \tag{2}$$

其中，T_N 是 MH 检测到发生移动需要认证的时延，T_M 是认证信息交互时延。在不具备移动感知的访问控制环境中，

$$T_{D1} = T_{N1} + T_{M1} \tag{3}$$

其中，T_{N1} 是 MH 操作员意识到需要认证的时延，T_{M1} 是所需的手工输入时延。在具有了移动感知的访问控制环境中，

$$T_{D2} = T_{N2} + T_{M2} = \min(T_{AR}, T_{MH}) + T_{M2} \tag{4}$$

其中，T_{AR} 是 AR 被动感知到移动的时延，T_{MH} 是 MH 主动感知到移动的时延，T_{N2} 等于两者中的较小者。T_{M2} 是自动完成认证交互的时延。

比较式(3)和(4)，T_{N1} 和 T_{M1} 的值分别取决于移动主机操作人员的反应时间和输入速度。T_{AR}、T_{MH} 以及 T_{M2} 的值则只取决于 AR 或者是 MH 的运算速度。这样，分别有

$$T_{N2} \ll T_{N1} \text{以及} T_{M2} \ll T_{M1} \tag{5}$$

那么，

$$T_{D2} \ll T_{D1} \tag{6}$$

也就是说，在支持移动感知的访问控制中，MH 在切换前的等待时延被大幅度压缩，这是有利于 MH 的移动切换性能的。

结论 在分析 MIPv6 网络协议特点以及访问控制机制行为特征的基础上，本文提出了一种在移动互联网访问控制应用中实现快速移动感知的方法，分别是在访问路由器端被动感知与移动主机端主动感知，并给出了具体的实现和比较分析。通过实践和分析得出，该方法能有效地缩短 MH 切换前的认证等待时间，有利于提升移动互联网中访问控制对主机移动性的支持。

参 考 文 献

1 Calhoun P, Loughney J, et al. Diameter Base Protocol. IETF RFC3588, 2003.6

2 Tony J, Neil J, Mick S, et al. Port-Based Network Access Control. IEEE Std 802.1X-2001, June 2001

3 Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. IETF RFC3775, 2004.6

4 Deering S, Hinden R. Internet Protocol, Version 6 (IPv6) Specification. IETF RFC2460, Dec 1998

5 Thomson S, Narten T. IPv6 Stateless Address Autoconfiguration. IETF RFC2462, 1998.11

6 Narten T, Nordmark E, Simpson W. Neighbor Discovery for IP Version 6 (IPv6). IETF RFC2461 1998.11

7 Pall E, Thomas H, Frederic P. Authenticated Access for IPv6 Supported Mobility. Proceeding of the Eighth IEEE International Symposium on Computers and Communication(ISCC'03), 2003.6

8 Wang R C, Chen R Y, Chao H C. AAA architecture for mobile IPv6 based on WLAN. International Journal of Network Management, 2004,14(5):305～313

9 冯红梅，郭巧，等. Linux 下实现 MIPv6 AAA 系统的接入路由器. 计算机应用，2005,25(5):1193～1195

10 李善平，刘文峰，等. Linux 内核 2.4 版源代码分析大全. 北京：机械工业出版社，2002

11 MIPL MIPv6:http://mobile-ipv6.org/

12 Rigney C, Willens S, et al. Remote Authentication Dial In User Service (RADIUS). IETF RFC2865, 2000.6

13 Kim C, Kim Y S, et al. Performance Improvement in Mobile IPv6 Using AAA and Fast Handoff. Proc. of 2nd International Conference on Computer Science and its Applications (ICCSA-2004), 2004