



(12) 发明专利申请

(10) 申请公布号 CN 102724173 A

(43) 申请公布日 2012. 10. 10

(21) 申请号 201110213475. 5

H04L 12/56(2006. 01)

(22) 申请日 2011. 07. 28

(71) 申请人 北京天地互连信息技术有限公司

地址 100028 北京市朝阳区曙光西里甲 6 号
时间国际 A 座 2508

(72) 发明人 刘东 刘铭 步日欣 谷晨 董伟
程远

(74) 专利代理机构 北京北新智诚知识产权代理
有限公司 11100

代理人 张卫华

(51) Int. Cl.

H04L 29/06(2006. 01)

H04L 29/08(2006. 01)

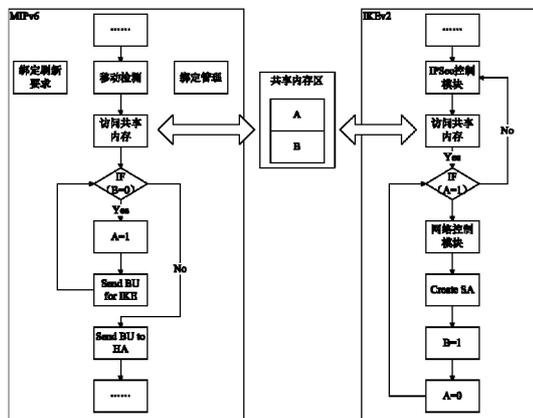
权利要求书 1 页 说明书 5 页 附图 3 页

(54) 发明名称

在 MIPv6 环境下实现 IKEv2 协议的系统及方法

(57) 摘要

本发明公开了在 MIPv6 环境下实现 IKEv2 协议的系统。该系统在 MN 端建立一种路由机制,即将网络中所有接入路由器 AR 统一配置一个相同的本地链路地址 X,在 MN 端设置一条默认路由,网关即为地址 X;MN 向 HA 发送的数据包,首先被路由到 AR 端,AR 根据目的地址将其转发给 HA;HA 向 MN 回复的数据包,先路由到 AR,之后 AR 转发给 MN;在 MN 端于用户空间创建一组标志位 flag,于内核空间加入 SA 触发机制,MIPv6 进程通过判断 flag 的值决定是否启动 SA 触发机制;IKEv2 进程通过判断 flag 值以决定是否发起 MN 与 HA 之间的 IKE 通信,协商密钥。本发明有效解决了 MIPv6 移动注册前 MN 与 HA 之间实现 IKEv2 协商及 MIPv6 触发 IKEv2 协议进行协商的问题,进而在 MIPv6 环境下实现了 IKEv2 协议,突破了 MIPv6 环境下的网络安全难题。



1. 一种在 MIPv6 环境下实现 IKEv2 协议的系统,其特征在于:

该系统在 MN 端建立一种路由机制,即将网络中所有接入路由器 AR 统一配置一个相同的本地链路地址 X,在 MN 端设置一条默认路由,网关即为地址 X;MN 向 HA 发送的数据包首先被路由到 AR 端,AR 根据目的地址将其转发给 HA;HA 向 MN 回复的数据包先路由到 AR,之后 AR 转发给 MN;

该系统在 MN 端还建立一种 MIPv6 触发 IKEv2 协议的协商机制,即于用户空间创建一组标志位 flag,于内核空间加入 SA 触发机制,MIPv6 进程通过判断 flag 的值以决定是否启动 SA 触发机制;IKEv2 进程通过判断 flag 值以决定是否发起 MN 与 HA 之间的 IKE 通信,协商密钥。

2. 如权利要求 1 所述的 MIPv6 环境下实现 IKEv2 协议的系统,其特征在于:

所述 MN 端采用共享内存策略实现所述 MIPv6 进程和 IKEv2 进程间的通信。

3. 如权利要求 1 所述的 MIPv6 环境下实现 IKEv2 协议的系统,其特征在于:

在所述启动 SA 触发机制中,首先构建一个 BU 消息,通过通信接口发出,该 BU 消息在经过内核 IPSec 模块时将调用 IKEv2 进程创建 SA,当 SA 建立成功时,MN 再向 HA 发送正常的 BU 消息。

4. 一种在 MIPv6 环境下实现 IKEv2 协议的方法,其特征在于包括以下步骤:

MN 不断进行路由器发现;

当发现接入到新的 AR 下时,MN 根据共享内存区标志位判断与 HA 间是否存在对应的 SA,若存在,则直接发送 BU 进行注册;若不存在,则发送自定义 BU,触发 IKE 交互,通过 IKE 协议建立所需 IPSec SA;

SA 生成后 MN 再进行移动注册,此时的 BU、BA 消息已可由 IPSec ESP 保护;

当 MN、HA 间的 IPSec SA 过期时,MN 发起 IKE 交互,重新建立 SA。

在 MIPv6 环境下实现 IKEv2 协议的系统及方法

技术领域

[0001] 本发明涉及一种在 MIPv6 环境下实现 IKEv2 协议的系统及方法。

背景技术

[0002] 随着 Internet 的迅速发展和移动便携式终端的广泛应用,在互联网中实现对移动性的支持越来越重要。但传统的 IP 设计并不支持移动性。因为传统的 IP 协议把节点的 IP 地址作为节点在接入网中的唯一标识,节点通过其 IP 地址收发数据,而网络中的路由器使用的路由协议一般是基于目的网络前缀转发,若节点若发生移动,目的地是该 IP 网络前缀的包仍将发送到原来的网络,这样已经移动的节点收不到发给它的数据包,通信会中断。为此, IETF 组织提出了移动 IP (Mobile IP, MIP) 的概念。并针对不同的网络类型,分别设计了移动 IPv4 协议 (Mobile IPv4, MIPv4) 和移动 IPv6 协议 (Mobile IPv6, MIPv6)。

[0003] MIP 协议是一种可部署于全球互联网的移动性解决方案,它工作与网络层,这使得上层协议对移动透明。MIP 协议的提出,可使节点在不改变其 IP 地址和现有的路由框架的前提下,在网络中自由漫游,并保持通信的持续性。

[0004] 对于 MIPv6 环境下的身份认证和信令加密, IETF 提出了采用 IPSec 协议保护移动节点 MN 和家乡代理 HA 间的移动信令消息。它可以有效防止线路窃听、消息拦截或伪造及 DoS 等攻击。而 IPSec 协议的使用就涉及到移动节点与家乡代理间的安全联盟 SA (security association) 的建立。目前较成熟的方案是因特网密钥交换协议 IKE 协议 (Internet Key Exchange), 它建立在因特网安全联盟和密钥管理协议 ISAKMP 的框架上,定义了通信实体间身份认证、协商加密算法以及生成共享会话密钥的方法,在 MIPv6 环境下,通过 IKE 协议动态协商 SA,实现移动节点与家乡代理间的移动信令消息 IPSec 加密。

[0005] IETF 在 RFC 3776 中详细介绍了 MIPv6 下与 IPSec 协议的实施标准。在其中提出通过采用 IKE 协议动态创建并维护 MN 与 HA 间的 SA,实现 MN 与 HA 间的移动性信令的 IPSec ESP 加密保护。之后随着 IPSec 协议在 RFC24301 中的改进,使得 IPSec 选择器可识别移动头 (Mobility Header, MH) 类型,实现了 IPSec 协议对 MIPv6 的支持。IETF 在 2007 年发布的 RFC4877,针对这一变革对原有的 RFC 3776 标准改进,并采用新的 IKEv2 协议实现密钥协商,大大简化了 MIPv6 与 IPSec 及 IKEv2 协议的交互复杂度。但 IKEv2 协议是建立在静态节点间的密钥协商协议, MIPv6 协议中移动节点 MN 的通信地址会随着 MN 移动而改变,如何在 MIPv6 环境中实现 IKEv2 协议,尚无明确的解决方案。

发明内容

[0006] 鉴于上述存在的问题,本发明的目的在于提供一种 MIPv6 环境下实现 IKEv2 协议的系统及方法。

[0007] 为实现上述目的,本发明采用如下技术方案:

[0008] 一种在 MIPv6 环境下实现 IKEv2 协议的系统,该系统在 MN 端建立了一种路由机制,即将网络中所有接入路由器 AR 统一配置一个相同的本地链路地址 X,在 MN 端设置一条

默认路由,网关即为地址 X;MN 向 HA 发送的数据包首先被路由到 AR 端,AR 根据目的地址将其转发给 HA;HA 向 MN 回复的数据包先路由到 AR,之后 AR 转发给 MN;

[0009] 该系统在 MN 端还建立了一种 MIPv6 触发 IKEv2 协议的协商机制,即于用户空间创建一组标志位 flag,于内核空间加入 SA 触发机制,MIPv6 进程通过判断 flag 的值以决定是否启动 SA 触发机制;IKEv2 进程通过判断 flag 值以决定是否发起 MN 与 HA 之间的 IKE 通信,协商密钥。

[0010] 进一步地:

[0011] 所述 MN 端采用共享内存策略实现所述 MIPv6 进程和 IKEv2 进程间的通信。

[0012] 所述启动 SA 触发机制,首先构建一个 BU 消息,通过通信接口发出,该 BU 消息在经过内核 IPSec 模块时将调用 IKEv2 进程创建 SA,当 SA 建立成功时,MN 再向 HA 发送正常的 BU 消息。

[0013] 一种在 MIPv6 环境下实现 IKEv2 协议的方法,包括以下步骤:

[0014] MN 不断进行路由器发现;

[0015] 当发现接入到新的 AR 下时,MN 根据共享内存区标志位判断与 HA 间是否存在对应的 SA,若存在,则直接发送 BU 进行注册;若不存在,则发送自定义 BU,触发 IKE 交互,通过 IKE 协议建立所需 IPSec SA;

[0016] SA 生成后 MN 再进行移动注册,此时的 BU、BA 消息已可由 IPSec ESP 保护;

[0017] 当 MN、HA 间的 IPSec SA 过期时,MN 发起 IKE 交互,重新建立 SA。

[0018] 本发明有效解决了 MIPv6 移动注册前 MN 与 HA 之间实现 IKEv2 协商及 MIPv6 触发 IKEv2 协议进行协商的问题,进而在 MIPv6 环境下实现了 IKEv2 协议,突破了下一代互联网 MIPv6 环境下的一个网络安全难题。

附图说明

[0019] 图 1 为本发明中 MN 端的路由机制示意图;

[0020] 图 2 为本发明中 MN 端的 MIPv6 触发 IKEv2 的协商机制示意图;

[0021] 图 3 为本发明中 MN 端的 MIPv6 触发 IKEv2 进行协商的实施例示意图;

[0022] 图 4 为本发明的 MIPv6 环境下实现 IKEv2 协议的消息处理流程图。

具体实施方式

[0023] IKE 协议是一种通用混合型协议,它建立在 Internet 安全联盟和密钥管理协议 (ISAKMP) 定义的框架上,定义了通信实体间进行身份认证、加密算法协商以及共享会话密钥生成的方法。IKE 协议通过一系列强安全性的非对称算法交换非密钥数据,实现双方的密钥交换,它解决了在不安全的网络中安全的建立或更新共享密钥的问题。

[0024] IKEv2 协议是当前互联网最认可的 IKE 协议,它采用 UDP 承载,对上一个版本 IKEv1 做出了很大改进,简化了消息交换,替换了加密语法等等。它为通信对等体动态协商密钥提供支持。IKEv2 协议中定义了三种消息交互类型,分别是 Initial 交互、CREATE-CHILD-SA 交互和 Informational 交互。Initial 交互过程完成建立 IKE SA 和 CHILD SA (即 IPSec SA)。该过程由 4 条消息完成:前两条消息称为 IKE SA INIT 交互,主要进行加密算法协商、nonce 交换和一次 D.H 密钥交换,从而生成用于加密和认证的密钥材料;后两

条消息称为 IKE AUTH 交互,主要对前两条消息进行认证,同时完成身份认证,然后建立 IKE SA 和第一次的 CHILD SA。IKE AUTH 交互过程中的数据都采用了 IKE SA INIT 生成的密钥材料加密,保证其中的身份信息不被窃取。CREATE CHILD SA 交互过程是在 Initial 交互完成后,生成额外的 CHILD SA 或者进行密钥重协商 (rekeying)。Informational 交互过程传输控制消息,用来通知对端发生错误或某些事件。该过程须在 Initial 交互之后,并在 IKE SA 的保护下进行。

[0025] 但要在 MIPv6 环境中部署 IKEv2 协议,实现 MN 和 HA 间的 SA 动态协商始终面临两个关键的问题:

[0026] 第一个问题是,当 MN 在外地获得新的转交地址 CoA (Care of Address) 后,需要进行移动注册过程,通知 HA 新的 CoA。若这时 MN、HA 间尚未建立 IPSec SA 或 SA 过期,则双方在移动注册前先要进行 IKE 协商。而此时 MN 并没有到 HA 的路由,HA 也不知道 MN 的 CoA,UDP 的通信是不通的,这导致 IKE 交互协商无法进行,从而不能建立 IPSec SA。

[0027] 另一个问题是,IKEv2 是建立在 IP 地址上的密钥协商,当主机发出数据包时,首先根据源地址、目的地址、协议类型等参数查询安全策略数据库 SPD (SP Database),若 SPD 没有策略,则放过,将该包转至 IP 层处理;若 SPD 中有相关策略,则根据对应 SP 查询安全联盟数据库 SAD (SA Database),并获取对应 SA 中的加密参数对数据包进行 IPSec 处理,之后转至 IP 层处理;若没有找到对应 SA,则调用 IKE 协议,通过 SP 中的规则在两通信实体建立 SA,之后进行 IPSec 处理等。

[0028] 而在 MIPv6 协议中,MN 和 HA 之间的移动信令绑定更新消息 BU (Binding Update) 和绑定应答消息 BA (Binding Acknowledgement) 都是采用 MN 的 CoA 作为源地址 / 目的地址,而 CoA 是随 MN 移动不断变化的。虽然标准已经定义了关于 BU/BA 对于 SA 的匹配是通过 MN 的家乡地址而不是 CoA,但这时的情况是 MN、HA 间已建立有效 SA;若此时还没有 SA,则移动实体发出 BU/BA 后,根据 MN 端地址 CoA、HA 地址、协议类型等参数查询 SPD,而 SPD 中的策略都应是基于 MN 的 HoA 的。所以找不到匹配的 SP,进而无法触发 IKE 协议交互建立 SA。

[0029] 由以上分析可以看出,在 MIPv6 环境下实现 IKEv2 协议,需要解决两个问题:

[0030] 1) MIPv6 移动注册前 MN、HA 间如何实现 IKEv2 协商;

[0031] 2) MIPv6 如何触发 IKEv2 的协商。

[0032] 下面结合附图和实施例对本发明作进一步的详细说明。

[0033] 为了在 MIPv6 移动注册前实现 MN 与 HA 间的 IKEv2 协商,本发明在 MN 端建立了一种稳定的路由机制,使 MN 在任意的接入路由器 AR 下都可以和 HA 进行 UDP 通信。

[0034] 图 1 为本发明中 MN 端的路由机制示意图。如图,网络中所有接入路由器 AR 统一配置了一个相同的本地链路地址 X,在 MN 端设置一条默认路由,网关即为地址 X。这样,当 MN 移动到外地 AR 下时,MN 获得新的 CoA,然后进行地址重复检测 DAD (Duplicate Address Detection) 过程,将 MN 的 CoA 和 MAC 地址在 AR 端绑定。MN 向 HA 发送 UDP 包,源地址为 CoA,目的地址为 HA 地址,数据包首先被路由到 AR 端,之后 AR 根据目的地址将其转发给 HA;HA 向 MN 回复 UDP 包,源地址为 HA 地址,目的地地址为 CoA,UDP 包根据目的地址先路由到 AR,之后 AR 转发给 MN。

[0035] MN 端默认路由的添加可通过 Linux 系统命令实现,将该命令写到文件 /etc/rc.d/

rc.10cal 中, MN 将在开机初始化的时候配置好该默认路由。

[0036] 为解决 MIPv6 触发 IKEv2 的协商问题, 本发明在 MIPv6 协议中引入一种通过正确的匹配 IKE 进程配置的 SPD 中的 SP, 并根据此 SP 触发 IKE 协议进而在 MN 和 HA 间创建 SA 的机制。由于 MIPv6 协议中所有的移动注册过程都由 MN 端发起, 所以这种触发机制只需在 MN 端加入, HA 作为通信双方的应答端, 不需做任何改变。

[0037] 图 2 为本发明中 MN 端 MIPv6 触发 IKEv2 的协商机制示意图。如图所示, 在 MN 端, 于用户空间创建一组标志位 flag, 它的参数值由 MIPv6 进程和 IKEv2 进程决定; 于内核空间加入 SA 触发机制, 它会根据用户空间 flag 的参数值判断是否帮助 MIPv6 进程触发 IKEv2 进行 SA 的协商, 同时 SA 的状态也会影响 flag 的参数值。

[0038] 共享内存是很有效的进程间通信 (Interprocess Communication, IPC) 方式, 也是最快的 IPC 形式。两个不同进程 A、B 共享内存是指, 同一块物理内存被映射到进程 A 和 B 各自的进程地址空间。进程 A 可以即时看到进程 B 对共享内存中数据的更新, 反之亦然。共享内存有 System V 和 POSIX 两种方式。本发明采用的是 System V 共享内存。

[0039] SystemV 共享内存, 主要有以下几个 API :shmget0、shmat0、shmdt0、shmctl0。其中 :shmget() 函数用来获得共享内存区域的 ID, 如果不存在指定的共享区域就创建相应的区域。shmat0 函数把共享内存区域映射到调用进程的地址空间中, 这样, 进程就可以方便的对共享内存区域进行访问操作。shmdt0 函数用来解除进程对共享内存区域的映射。shmctl0 函数实现对共享内存区域的控制操作。

[0040] 图 3 为本发明中 MN 端的 MIPv6 触发 IKEv2 进行协商的实施例示意图。在共享内存空间设置两个标志位 A、B, 标志位 A 用于标记 MN、HA 间是否存在有效的 SA; 标志位 B 用于判断 MN 端是否启动 SA 触发机制。

[0041] 如图, 由于 MIPv6 进程与 IKEv2 进程这两个进程需要共同查看、管理同一组标志位 flag, 所以在 MN 端采用共享内存策略实现两进程间的通信, 本发明采用 System V 共享内存。本实施例在共享内存区内设置标志位 A、B, 具体的:

[0042] 对于 MIPv6 进程, 当检测到要向 HA 发送 BU 消息时, 首先访问共享内存区, 读取标志位 B 的值: 若 $B = 1$, 则此时通信双方已建立了有效 SA, MN 直接向 HA 发送正常的 BU 消息, 其源地址为 CoA, 这个消息在经过内核 IPsec 模块时可找到相关的 SA, 从中提取参数并加密封装发出; 若 $B = 0$, 则此时通信双方尚未建立有效 SA, MN 启动 SA 触发机制, 首先将标志位 A 的值写为 1, 然后构建一个源地址为 MN 的 HoA, 目的地址为 HA 的 BU 消息, 通过通信接口发出。注意: 这个 BU 消息在经过内核 IPsec 模块时会查询 SPD, 在其中可以找到相关的安全策略 SP, 但在 SAD 中找不到对应的 SA, 这时将调用 IKEv2 进程创建 SA, 之后再次判断 B 的值当 $B = 1$ 时, SA 已建立成功, MN 再向 HA 发送正常的 BU 消息。

[0043] 对于 IKEv2 进程, 其 IPsec 控制模块不断侦听内核通告, 当收到创建 SA 的消息时, IKEv2 访问共享内存区, 读取标志位 A 的值: 若 $A = 0$, 说明此时 MN、HA 间已建立有效 SA, 退出继续等待内核通告; 若 $A = 1$, 则调用网络控制模块, 根据内核信息发起 MN 和 HA 之间的 IKE 通信, 协商密钥, 创建 SA, 之后令 $B = 1, A = 0$, 退出继续等待内核通告。

[0044] 图 4 为本发明的 MIPv6 环境下实现 IKEv2 协议的消息处理流程图。如图所示, MN 不断进行路由器发现, 当发现接入到新的 AR 下时, MN 发起移动注册过程, 此时 MN 会根据共享内存区标志位判断与 HA 间是否存在对应的 SA。若存在, 则直接发送 BU 进行注册; 若不存

在,则发送自定义 BU,触发 IKE 交互,通过 IKE 协议建立所需 IPSec SA ;SA 生成后 MN 再进行移动注册,此时的 BU、BA 消息已可由 IPSec ESP 保护。当 MN、HA 间的 IPSec SA 过期时,MN 还应发起 IKE 交互,重新建立 SA。

[0045] 本发明的在 MIPv6 环境下实现 IKEv2 协议的系统,有效地解决了 MIPv6 移动注册前 MN 与 HA 之间实现 IKEv2 协商及 MIPv6 触发 IKEv2 协议进行协商的问题,进而在 MIPv6 环境下实现了 IKEv2 协议,突破了下一代互联网 MIPv6 环境下的一个网络安全难题。

[0046] 以上所述是本发明的较佳实施例及其所运用的技术原理,对于本领域的技术人员来说,在不背离本发明的精神和范围的情况下,任何基于本发明技术方案基础上的等效变换、简单替换等显而易见的改变,均属于本发明保护范围之内。

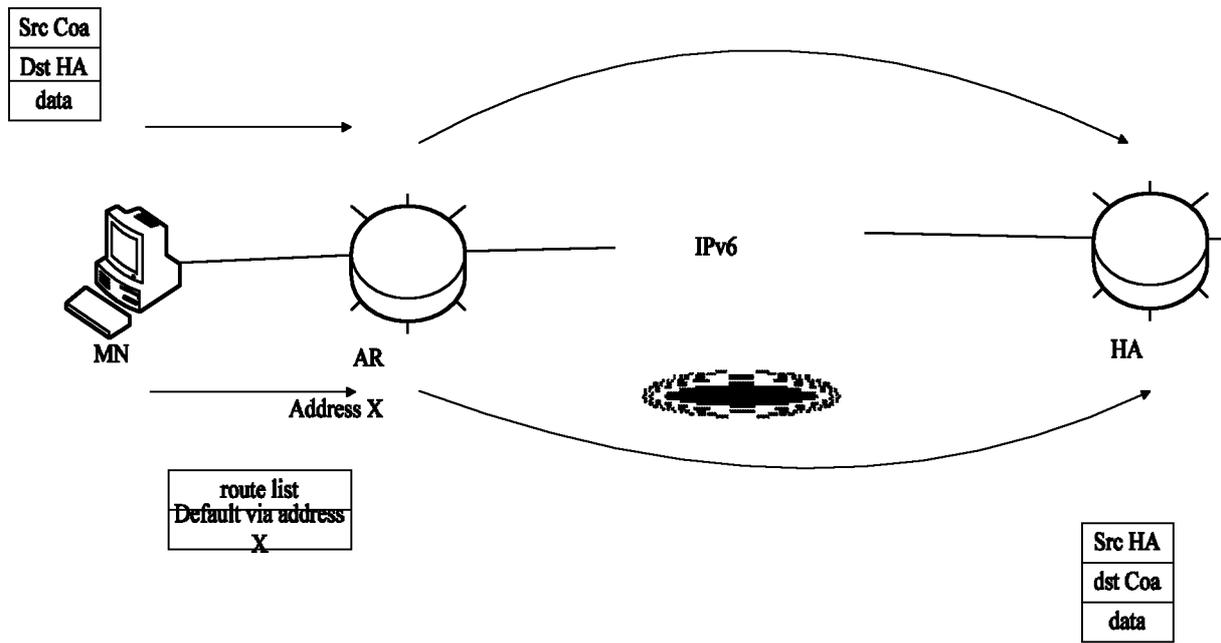


图 1

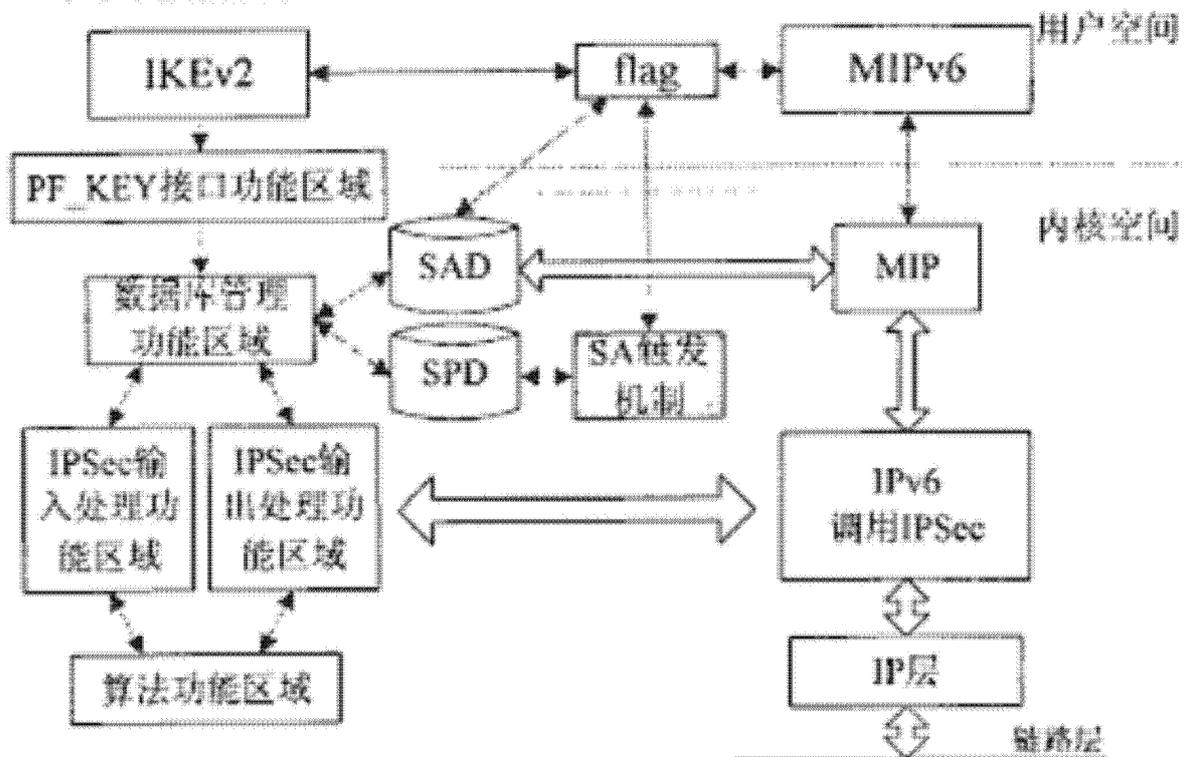


图 2

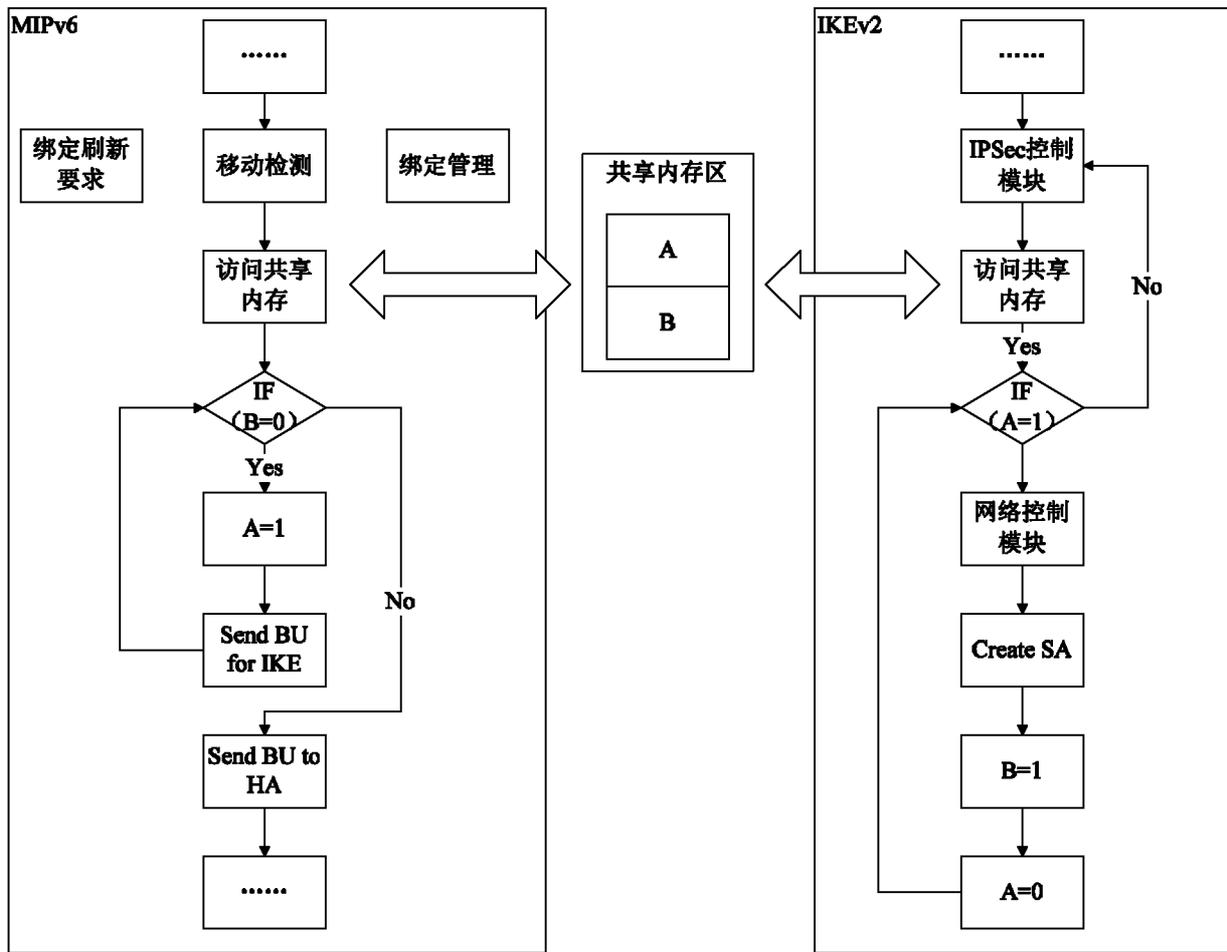


图 3

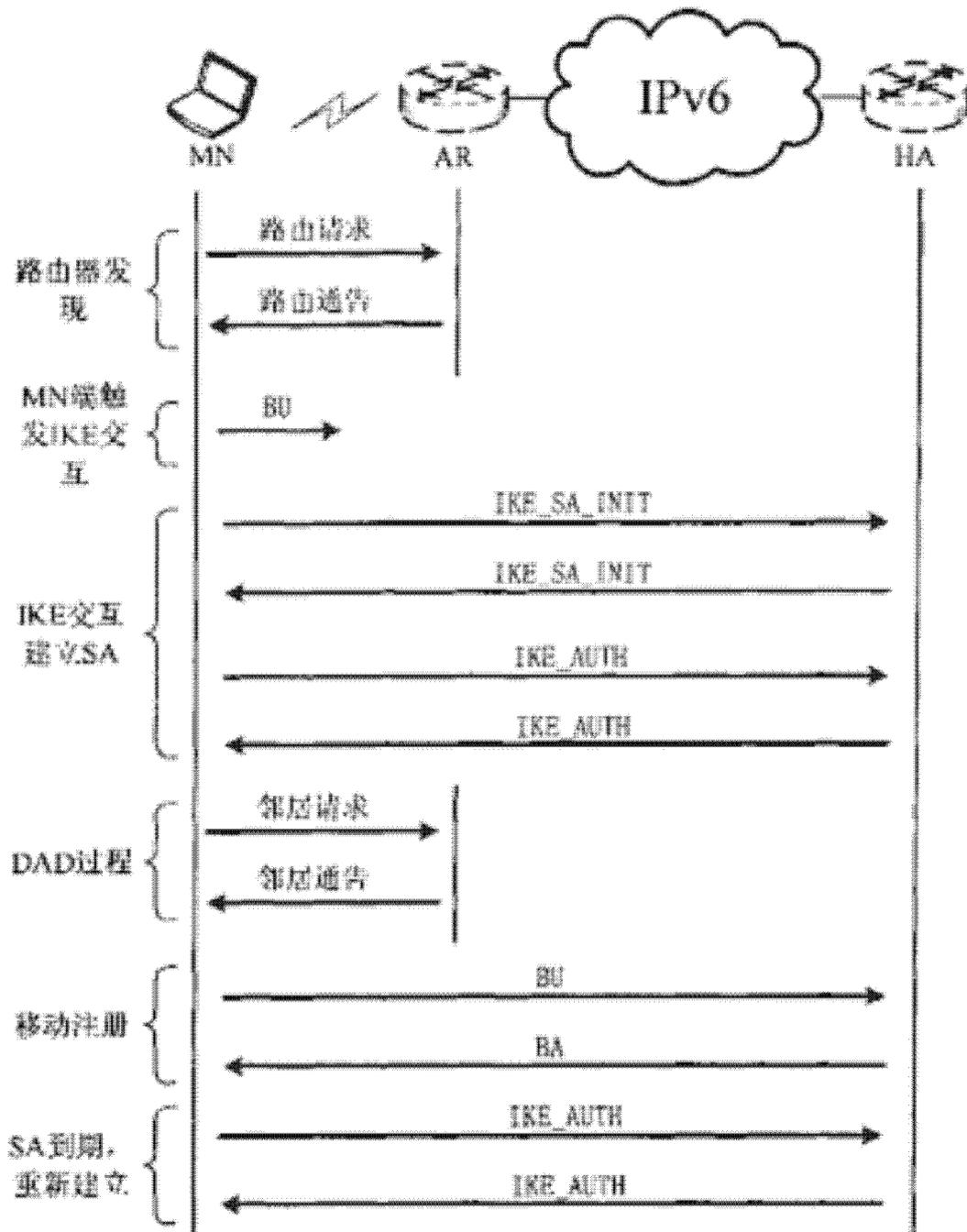


图 4