文章编号:1001-2486(2006)05-0035-07

一种基于VMN的移动IP快速切换方法*

石东海,赵 磊,唐朝京
(国防科技大学 电子科学与工程学院,湖南 长沙 410073)

摘 要:为了满足用户对移动IP服务的安全性、低时延方面的要求,弥补现有移动IPv4协议中切换方案的不足,在移动IP/AAA模型的基础上,提出了一种基于VMN(虚拟移动节点)的移动IP快速切换方法。该方法增强了移动IP联合AAA的基本模型,并在MA(移动代理)上构建了一种新的数据结构;通过在NFA和OFA之间建立一个新的双向隧道,将VMN中的数据报文进行快速转移,在没有数据报文丢失的情况下,实现了快速低时延的切换;通过分发新的临时安全关联以及认证票据,有效地提高了移动IP在注册和切换过程中的安全,同时有效地降低了AAAH和AAAF之间的网络负载;通过对该方法进行安全性分析和仿真试验表明,我们提交的方法是安全有效的。

关键词:虚拟移动节点;移动IP;认证票据;低时延切换
中图分类号:TP393 **文献标识码**:A

A VMN-based Fast Handoff Method for Mobile IP

SHI Dong-hai, ZHAO Lei, TANG Chao-jing
(College of Electronic Science and Engineering, National Univ. of Defense Technology, Changsha 410073, China)

Abstract: A VMN-based MIPv4 fast handoff method based on the basic MIP/AAA model was presented for satisfying the users' demands of security and low latency in MIP services and making up the existing insufficiency in the current MIPv4 handoff method. The method strengthens the basic MIP/AAA model, and sets up a novel data structure in the mobile agents. Through establishing a new bidirectional tunnel between NFA and OFA, it fast transforms the data packets of VMN between them, and realizes the fast low latency handoff under no data packets losing. Through distributing the new temporary security association and the authentication ticket, it enhances the security in the MIP's registration and handoff process, and effectively reduces the network loads between AAAH and the AAAF. The secure analysis and the simulation experiment for the presented method indicates that the method is more secure and effective.

Key words: virtual mobile node; mobile IP; authentication ticket; LLH

随着Internet商业应用的普及和对Internet移动性访问的增长,移动IP正将取代IP提供移动环境的解决方案,然而,在移动IPv4的注册和快速切换方案[1-3]不能满足用户对服务的安全性、低时延方面的要求。为此,IETF工作组建议采用AAA(认证、授权和记帐)服务器机制来解决移动IPv4中存在的安全问题,并开发低时延切换标准(LLH)来减小移动IP在认证和注册过程中的时延和数据包的丢失。LLH支持两种模式,即移动IP常规模式[1]和区域注册模式[4]。后者能够当MN在同一个拜访域内进行微移时,有效地减少传向家乡网络的信号的数量和信号的时延。然而,在移动IP联合AAA的基本模型[5-7]中,当MN(移动节点)移入新的外地网络后,必须向家乡网络发送区域注册信息才能获得外地网络的访问权以及相关的会话密钥。当外地网络和家乡网络之间的距离比较远时,这种注册延时对数据传输的实时性影响很大。文献[8]提出了一种重复使用先前移动IP会话过程中应用的会话密钥以减少内建时延的方法,然而,这种方法在实际应用过程中存在很多缺陷。

在文献[5-7]的基础上,本文提出了一种基于VMN的移动IP快速切换方法。该方法对移动IP联

* **收稿日期**:2006-03-20
基金项目:国家部委基金资助项目(41329080101);国家自然科学基金资助项目(60372039)
作者简介:石东海(1977—),男,博士生。

合 AAA 的基本模型进行了增强,并在 MA(移动代理)上构建了一种新型的数据结构。通过在 NFA(新的外地代理)和 OFA(旧的外地代理)之间建立一个新的双向隧道,将 VMN 中的数据报文进行快速转移,在没有数据报文丢失的情况下,实现了快速低时延的切换;通过分发新的临时安全关联以及认证票据,有效地提高了移动 IP 在注册和切换过程中的安全,并降低了 AAAH(家乡域中的 AAA 服务器)和 AAAF(外地域中的 AAA 服务器)之间的网络负载。

1 基于会话密钥交换的切换方法

1.1 基本模型

根据 LLH 的相关描述[9],当 MN 移入一个新的外地域内时,LLH 在拜访外地域内时执行本地的注册管理。由于 NFA 没有会话密钥,需要对 MN 进行重新认证并由 AAAH 发放新的会话密钥,这些过程将导致时延。文献[8]的方法的基本假设是:如果当前会话密钥的生命周期足够长,当前会话密钥就可以被重复使用,以消除由于 AAAH 对 MN 重新认证所带来的时间延时。文中提出了一种基于 D-H 密钥管理协议的方法来保护 OFA 和 NFA 之间的密钥交换。图 1 显示了该方法的场景。

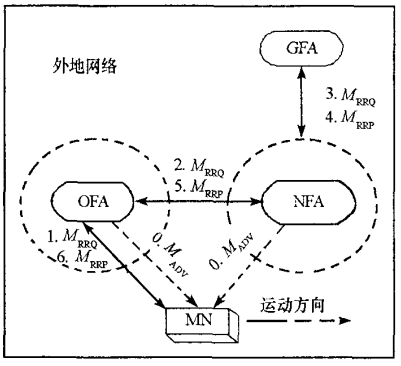

图 1 基于会话密钥交换切换的场景图

Fig. 1 The scenario of session key exchange method

1.2 安全性分析

根据文献[8]的描述和分析,我们发现该方法存在着诸多的缺陷。首先,GFA 参加了参数 a 的计算,并且拥有会话密钥 $S_{FA\text{-}HA}$。从安全角度来讲,GFA 完全可以利用该会话密钥来伪造 FA(外地代理)的身份对 HA(家乡代理)和 FA 之间的安全造成重大威胁。当 GFA 拥有在其域内所有 FA 的会话密钥时,它就成为了该移动网络的安全瓶颈。其次,受限的会话密钥的生命周期是用来避免密钥被攻击者盗用的一种方法。尤其是对于 OFA 和 HA(家乡代理)之间应用的会话密钥 $S_{FA\text{-}HA}$,它是一个少于 64 位的未经过哈希变化的随机值[1],很容易遭到破解攻击。当 MN 移入一个新域并通过 AAAH 的重新认证获得新的会话时,能够有效地减少会话密钥被破解进而被利用的概率,先前会话密钥的重复使用增加了这种危险的概率。最后,该方法采用基于 D-H 密钥管理协议的方法增加了 FA 的计算负担,并且该算法容易遭受中间人、重传和其它攻击。因此,我们认为文献[8]中提到的基于会话密钥交换的切换方法是不安全的。

2 基于 VMN 的切换方法

2.1 基本模型和假定

我们的方法是基于移动 IP/AAA 的基本模型[7],在该模型中存在着四个基本的安全关联,并列出了移动 IP/AAA 基本信任模型的相关要求。这里将 HA 和 FA 统称为 MA(移动代理),该方法主要对 MA 进行适当修改,而不对其它实体进行更改。在基于虚拟移动节点(VMN)原理的方案中,每个 MN 与一个 VMN 关联,其中,VMN 是存在于 MA 中的一种数据结构。如果一个发送者想向某个移动节点发送一个数据包,它首先需要简单地向代表接收者的虚拟移动节点发送该数据包,随后,接收者从其虚拟移动节点中获得该数据包。

除了虚拟移动节点之外,每个移动代理中还存在名为注册表的数据结构。注册表的每个入口中存在 6 个属性:移动节点的家乡地址(HoA)、虚拟移动节点的地址(VoA)、移动节点的转交地址(CoA)、合法标签、认证服务器(AS)以及虚拟移动节点指针。其中,合法标签被用于标识虚拟移动节点地址是否过期,认证服务器指向为 MN 的身份提供认证的 AAA 服务器。表 1 提供了一个注册表的例子,其中第一个入口显示了位于另外一个移动代理上的远端虚拟移动节点,第二个入口显示了本地虚拟移动节点。另外,采用认证票据的方式对 MN 进行身份认证。表 2 是对 MN 身份进行认证的认证票据的基本信息,

该认证票据由 MN 所在外地域内的 AAAF 服务器进行签名,其中包含认证票据索引(authentication ticket index)、移动节点的身份标识信息(NAI_MN)、票据的生命周期(lifetime)、签发票据的认证服务器(AS)、虚拟移动节点所在移动代理的身份标识信息(NAI_MA)以及用于验证该票据唯一性的随机数。

表 1 移动代理中的注册表

Tab.1 The register table of MA

HoA	VoA	Valid Tag	CoA	AS	Pointer to VMN
Pre A	Remote Add	True	Null	Null	Null
Pre B	Local Add	True	Addr C	AAAF	A Pointer

表 2 认证票据的基本信息

Tab.2 The basic information of authentication ticket

ATI	NAI_MN	Lifetime	AS	NAI_MA	RAND
Ticket A	A@B.C	T	AAAF	D@E.F	128bit

另外,为了增强切换的速度和安全,我们对基本模型[7]进行了扩展,提出了以下假定条件:

当 MN 在外地域内第一次获得 AAAH 的认证后,AAAH 将会把 MN 的身份标识信息发送给 AAAF,并授权 AAAF 为其管理域内的 MN 发放认证票据以及执行身份认证;当 MN 从 AAAH 获得认证之后,AAAH 产生一个 AAAF 和 MN 之间的临时安全关联 SA5($SA_{AAAF\text{-}MN}$),AAAF 可以通过该安全关联与 MN 交换秘密信息;AAA 服务器负责分发各个移动代理和 MN 彼此之间的会话密钥,我们指定 AAAH 负责分发 HA 与 MN 之间的会话密钥 KMN-HA 与 AAAF 和 MN 之间的临时关联密钥 $SA_{AAAF\text{-}MN}$,AAAF 负责分发 MN 与 FA 之间的会话密钥以及 FA 和 HA 之间的会话密钥;OFA 和 NFA 同属于由一个 AAAF 管理的外地域,在 AAAF 与 NFA 之间存在安全关联 $SA_{AAAF\text{-}NFA}$,在 AAAF 和 OFA 之间存在安全关联 $SA_{AAAF\text{-}OFA}$,AAAF 可以通过这些安全关联发放二者之间的临时会话密钥 $K_{OFA\text{-}NFA}$。临时会话密钥 $K_{OFA\text{-}NFA}$ 在其周期内用于将 OFA 中 VMN 保存的数据报文转交给 NFA 中新建立的虚拟移动节点 VMN′。

2.2 基本操作流程

2.2.1 在家乡域内与 AAAH 的初次注册

当 MN 结束家乡域内与 AAAH 初次注册后,MN 可以获得其身份证书,MN 和 HA 同时获得二者之间的会话密钥 $K_{HA\text{-}MN}$,MN 获得安全关联 SA1,并且 MN 获准能够使用家乡域内的服务和资源。

2.2.2 在外地域内与 AAAH 的初次注册

当 MN 首次进入一个外地域时,它需要与家乡网络进行注册和绑定更新,其注册模型如图 2 所示。

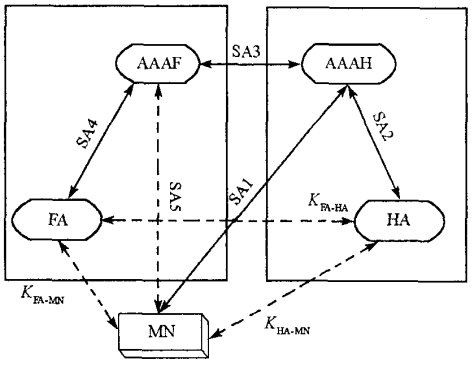

图 2 MN 在外地域首次与 AAAH 进行认证的模型

Fig.2 The model of first registration with AAAH in foreign domain

(0)FA→MN: M_{ADV}

发送通告,通知 MN 已经进入新的区域,其中包含 FA 的地址信息以及分配给 MN 的转交地址的信息。

(1)MN→FA: M_{RRQ}

MN 向 FA 发送注册请求消息 M_{RRQ},M_{RRQ} 包括 MN 的身份信息、Ticket、HoA、CoA 以及 VoA 等信息,并要求在该 FA 上产生 VMN。其中,HoA 是 MN 的家乡地址,CoA 是 FA 分配给 MN 的转交地址,VoA 是当前 VMN 所在 FA 的地址,Ticket 是 MN 的身份认证票据。对于首次进入外地域的 MN 来讲,VoA 和 Ticket 信息为空。

(2)FA→AAAF: M_{Auth}

FA 收到该消息后,生成 MN 的 VMN,将注册表内关于 VMN 的合法标签置为 False,并将消息(1)发送给 AAAF,请求 AAAF 对其进行认证。

(3)AAAF→AAAH

由于 AAAF 无法对其进行认证,转发消息(2)。

(4)AAAH→AAAF

AAAH对MN的身份认证成功后,向其HA发送绑定更新消息;向AAAF发送MN的身份信息(当MN在AAAF管辖的范围内微移时,授权AAAF对MN进行认证),AAAF与MN之间产生新的安全关联SA5($SA_{AAAF\text{-}MN}$)(AAAF用其与MN交换秘密信息);向MN发送经过SA1加密的认证成功信息和SA5。

(5)AAAF

AAAF根据从AAAH收到的信息,获得新的安全关联SA5,再根据从MN获得的信息,生成对MN的认证票据Ticket A,该认证票据用AAAF的私钥进行签名,其结构如表2所示。向FA分发$K_{FA\text{-}MN}$,$K_{FA\text{-}HA}$,并通知其对MN的认证成功;向MN分发会话密钥$K_{FA\text{-}MN}$和认证票据Ticket A(该信息经过SA5加密),并转发AAAH发送给MN的信息。

(6)FA

获得对MN认证的结果,将注册表内关于VMN的合法标签置为True,获得会话密钥$K_{FA\text{-}MN}$,$K_{FA\text{-}HA}$。通知MN新的虚拟移动节点VMN已经产生,并转交AAAH和AAAF发送的消息。

(7)MN

MN获得访问外地网络的权力,并获得Ticket A,SA5,$K_{FA\text{-}MN}$。

2.2.3 *在同一外地域内微移*

根据图3所示的场景,在同一外地域内微移期间的注册和密钥分发操作如下:

(0)~(2)过程如2.2.2中的(0)~(2)过程,其中的VoA和Ticket非空。

(3)AAAF

根据获得的注册消息,AAAF从中得到MN的认证票据Ticket A,NFA的身份标识以及新的VoA地址。如果AAAF根据获得的Ticket A验证MN的身份成功后,AAAF产生临时会话密钥$K_{NFA\text{-}OFA}$用于建立NFA和OFA之间的双向安全隧道,并产生新的会话密钥$K_{HA\text{-}NFA}$和$K_{MN\text{-}NFA}$以及新的认证票据Ticket B。然后,它发送以下消息:

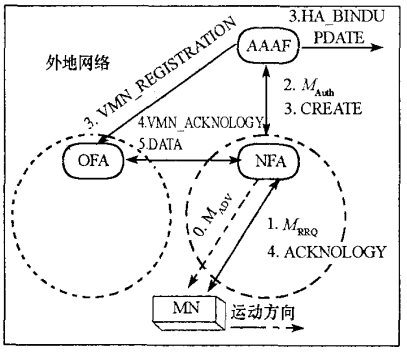

图3 提交的切换方法的场景图

Fig.3 The scenario of the presented method

- 向NFA发送"CREATE"消息,要求其创建新的虚拟移动节点VMN′,并通知其MN身份正确,发送$K_{HA\text{-}NFA}$和$K_{MN\text{-}NFA}$会话密钥以及临时会话密钥$K_{NFA\text{-}OFA}$;
- 向OFA发送"VMN _ REGISTRATION"消息,发送临时会话密钥$K_{NFA\text{-}OFA}$;
- 向MN的HA发送"HA _ BINDUPDATE"消息,包含会话密钥$K_{HA\text{-}NFA}$;
- 向MN发送经过SA5加密的新的认证票据Ticket B和新的会话密钥$K_{MN\text{-}NFA}$。

(4)NFA

当NFA收到从AAAF发来的"CREATE"消息时,获得$K_{HA\text{-}NFA}$和$K_{MN\text{-}NFA}$会话密钥以及临时会话密钥$K_{NFA\text{-}OFA}$,NFA建立与OFA之间的双向隧道。NFA将注册表中的VMN′中的合法标签置为True,基于当前的环境,它产生了以下消息:

- 发往MN的"ACKNOLOGY",通知其新的虚拟移动节点VMN′所在地址(即VoA地址),并转交AAAF发送给它的认证票据Ticket B和新的会话密钥$K_{MN\text{-}NFA}$;
- 发往OFA的"VMN _ ACKNOLOGY"消息,通知其新的虚拟移动节点VMN′地址已经产生。

(5)OFA

当接收到来自于AAAF的"VMN _ REGISTRATION"消息,将相应的实体的合法标签设置为False,即意味着该VMN不再被使用;获得临时会话密钥$K_{NFA\text{-}OFA}$后,将建立与NFA之间的双向隧道。当接收来自于NFA的"VMN _ ACKNOLOGY"消息时,OFA执行下列操作:

- 更新注册表中的虚拟移动节点VMN′地址;
- 设置合法标签为True;

• 通过与 NFA 之间的双向隧道将所有虚拟移动节点 VMN 中的存储的数据包转移到 VMN′中;

• 向虚拟移动节点 VMN 中缓存数据包的发送者发送"UPDATE"消息,通知其更新虚拟移动节点地址;

• 当所有数据包已经转移完成,解除该虚拟移动节点并将注册表中与该虚拟移动节点相关入口中的后三个属性设置为 Null,即转交地址、认证服务器和虚拟移动节点指针。

(6)HA

当收到"HA _ BINDUPDATE"消息时,根据当前环境,HA 执行下列操作:

• 向 AAAF 发送消息"HA _ BINDUPDATE _ ACK";

• 建立与 MN 关联的 VoA 的绑定更新。

为了增强上述所有信息的安全性,在每一步中的信息中都添加了时间戳和 MAC 值。

3 提交方法的安全性分析

与会话密钥交换方法[8]相比较,提交的方法具有以下安全特征:

• 采用认证票据对 MN 的身份进行认证,由于 AAAF 对该票据进行了签名处理,降低了 MN 在身份认证过程中的威胁;

• 在 AAAF 和 MN 之间建立了一个新的安全关联 SA5,用于在 AAAF 和 MN 之间传递消息和分发会话密钥 $K_{MN\text{-}NFA}$ 和认证票据,从而能够有效地阻止在密钥分发过程中的会话密钥盗用攻击和中间人攻击;

• 当 MN 在同一个外地域内进行微移时,AAAF 通过对 MN 的重新认证生成了 MN 新的会话密钥。新生成的会话密钥能够减少由于密钥破解而遭到攻击的概率;

• OFA 和 NFA 之间不存在密钥交换的过程,临时会话密钥 $K_{NFA\text{-}OFA}$ 是由 AAAF 通过两个安全关联进行分发的,因此,该方法能够有效地阻止 FA 遭受中间人攻击的可能;

• NFA 和 OFA 之间的安全隧道能够有效地保证虚拟移动节点中的数据报文的安全转移。另外,在消息传递的每一步中,都加入了时间戳和 MAC 信息,这能够有效地阻止重传攻击。

提交的方法能够确保移动 IP 会话密钥的完整性和机密性,因此,它能够提供比文献[8]中提到密钥交换方法更安全的 LLH,并且不需要 FA 进行额外的计算操作,而密钥交换方法在此方面耗费的时间是较多的。更为重要的是,我们提交的方法不但执行了基于 AAA 的认证操作,而且还实现了切换本地化,这些是满足 LLH 安全需求的。

4 实验结论

在我们实验中,仿真软件是运行在 Linux Red Hat 9.0 和 AMD Athlon(TM) 64 实验平台下。设计了前面所述的基于密钥交换的方法(图 1)、基于公钥的切换方法(图 4)和本文方法(图 3)三个场景,并对其进行了比较仿真。假设 MN 与 OFA 之间的最短路径的跳跃点的数目为 a;NFA 与 OFA 之间的最短路径的跳跃点的数目为 b;MN 与 NFA 之间的最短路径的跳跃点的数目为 c;NFA 与 AAAF 之间的最短路径的跳跃点的数目为 d;NFA 与 GFA 之间的最短路径的跳跃点的数目为 e;AAAF 与 OFA 之间的最短路径的跳跃点的数目为 f;AAAF 与 AAAH 之间最短路径的跳跃点的数目为 g;AAAH 与 HA 之间的最短路径的跳跃点的数目为 h。另外,假设某节点处理一个消息的消耗为 C_P;C_T 表示在路径上一个跳跃点传输一个消息所需要的消耗;L 表示由于注册造成的延时的消耗。

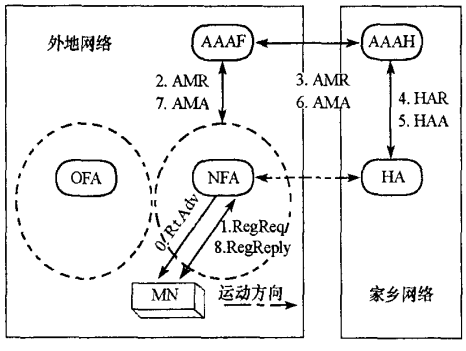

图 4 基于公钥切换的场景图

Fig.4 The scenario of public key method

可以得到,采用基于公钥的方法进行注册(图 4)的时延消耗为:

$$L_{P\_Key} = 2(c + d + g + h) \times C_T + 2(C_{P,MN} + C_{P,NFA} + C_{P,AAAF} + C_{P,AAAH}) + C_{P,HA} \quad (1)$$

采用会话密钥交换的方法造成的时延消耗为：

$$L_{E\_Key} = 2(a + b + e) \times C_T + 2(C_{P,MN} + C_{P,OFA} + C_{P,NFA}) + C_{P,GFA} \quad (2)$$

采用提交的方法造成的时延消耗为：

$$L_{VMN} = 2(d + c) \times C_T + 2C_{P,MN} + 2C_{P,NFA} + C_{P,AAAF} \quad (3)$$

假定在同一管理域内，各节点之间最短距离的跳跃点个数为1，即 $a = b = c = d = e = h = 1$，$C_T = C_P = 1$，对上面三个公式进行简化。图5、图6显示了实验的仿真结果。图6中的本地切换率(local handoff ratio)是本地注册与家乡注册的比值，其范围是0～1。密钥交换方法中的本地注册是没有经过AAAH进行认证的，本文方法是经过外地AAAF进行认证的。由于这两种认证方法都没有经过HA和AAAH进行认证，所以二者的数据曲线在走势上是基本相同，但是在图5和图6中可明显看出，本文方法在时延方面是比较小的。

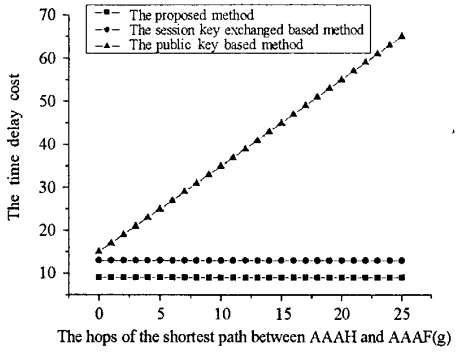

图5 三种切换方法的时延消耗

Fig.5 The delay cost of three handoff methods

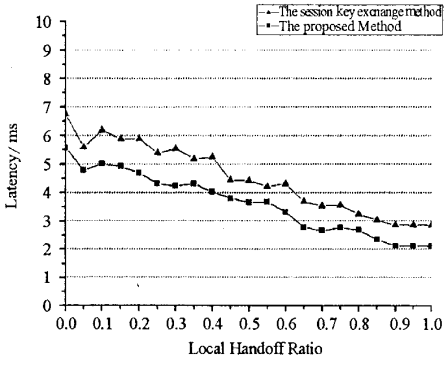

图6 基于会话密钥交换和本文提出的方法的切换时延

Fig.6 The delay cost of session key exchange method and proposed method

与基于会话密钥交换的切换方法相比较，实验结果表明本文方法具有以下特性：

(1) 降低了AAAH和AAA网络的负担。在实际的操作中，AAAH可能会同时对属于该管理域的很多MN进行认证，AAAH的计算能力和AAA网络的传输能力代表了家乡网络的认证能力。将部分认证权力转交给外地网络中AAAF能够提高认证的效率和减少家乡网络的网络负担。

(2) 采用认证票据的方式减少了由于网络传输节点进行加解密计算造成的时间延时。如果采用常用的认证方式，类似于身份信息等重要信息在从MN传输到AAAF的过程中，需要在MN、相关的FA以及AAAF进行多次的加密和解密操作。由于认证票据受到AAAF的签名保护，传输途中各个节点可以用AAAF的公钥查看票据中的内容，但却不能对其进行更改，只有AAAF在获得认证票据的时候才进行一次解密处理，这将大大降低由于计算造成的时间延迟。

(3) 减少了MN和HA的计算负载。对称密钥机制是相对比较简单的，并且对MN和HA的计算能力要求比较低，增强了它们的传输能力，但是，采用对称密钥机制增加了对密钥管理的复杂度。

(4) 降低了切换过程中的数据报文丢失概率。文中采用了一种新型的数据结构——VMN，能够在MN发生切换的时候，将来自于通信对端的数据报文进行妥善的缓存保管，当新的虚拟移动节点建立后，在双向安全隧道的保护下及时地转移到新的虚拟移动节点中，再进一步转交给MN，因而，在整个切换过程中，数据报文的丢失概率几乎为零。另外，由于文中设计的切换方法造成的时间延迟很小，数据报文转移造成的数据延迟时间相对也比较小，能够满足多种实时性比较强的IP业务需求。

5 结论

提出了一种基于VMN的移动IP快速切换方法。在该方法中，对移动IP联合AAA的基本模型进行了增强，并在MA上构建了一种新型的数据结构。通过在NFA和OFA之间建立一个新的双向隧道，将

VMN 中的数据报文进行快速转移,在没有数据报文丢失的情况下,实现了快速低时延的切换;通过分发新的临时安全关联以及认证票据,有效地提高了移动 IP 在注册和切换过程中的安全性,并有效地降低了 AAAH 和 AAAF 之间的网络负载;通过安全分析和仿真试验表明,提交的方法较文献[8]方法更为安全和有效。

参 考 文 献:

[1] Perkins C E. IP Mobility support for IPv4 [S]. IETF: RFC 3220, January 2002.

[2] Perkins C E. Application Statement for IP Mobility Support [S]. IETF: RFC 2005, 1996.

[3] Perkins C E. IP Mobility Support for IPv4 [S]. IETF: RFC3220, 2002.

[4] Gustafsson E, Jonsson A, Perkins C E. Mobile IPv4 Regional Registration [S]. IETF: draft-ietf-Mobileip-reg-tunnel-06.txt, 2002.

[5] Vollbrecht J, Cahoun P, et al. AAA Authorization Framework[S]. IETF: RFC 2904, 2000.

[6] Gommans L, Vollbrecht J, Generic D S. AAA Architecture[S]. IETF: RFC 2903, 2000.

[7] Perkins C E. Mobile IP Joins Forces with AAA [J]. IEEE Personal Communications, 2000, 7(4): 59-61.

[8] Kim H G, Choi D H. Session Key Exchange Based on Dynamic Security Association for Mobile IP Fast Handoff [C]. ICCSA 2004, 2004.

[9] Malki K E, et al. Low Latency Handoffs in Mobile IPv4 [S]. IETF: draft-ietf-Mobileip-lowlatency-handoffs-v4-04.txt, 2002.

(上接第 29 页)

参 考 文 献:

[1] Birot M, Pillot J P, Dunogues J. Comprehensive Chemistry of Polycarbosilanes, Polysilazanes, and Polycarbosilazanes as Precursors of Ceramics [J]. Chem. Rev., 1995, 95:1443-1477.

[2] Laine R M, Babonneau F. Preceramic Polymer Routes to Silicon Carbide [J]. Chem. Mater., 1993, 5:260-279.

[3] Schilling C L, Wesson J P, Williams T. C. Polycarbosilane Precursors for Silicon Carbide [J]. Am. Ceram. Bull., 1983, 62(8):912-915.

[4] Yajima S, Hasegawa Y, Hayashi J. Synthesis of Continuous Silicon Carbide Fiber with High Tensile Strength and High Young's Modulus. Part Ⅰ. Synthesis of Polycarbosilane as Precursor [J]. J. Mater. Sci., 1978, 13:2569-2576.

[5] Hasegawa Y, Okamura K. Synthesis of Continuous Silicon Carbide Fiber. Part Ⅳ. The Structure of Polycarbosilane as Precursor [J]. J. Mater. Sci., 1986, 21:321-328.

[6] Ly H Q, Taylor R, Day R J. Conversion of Polycarbosilane (PCS) to SiC-based Ceramic. Part Ⅰ. Characterisation of PCS and Curing Products [J]. J. Mater. Sci., 2001, 36:4037-4043.

[7] Hasegawa Y, Okamura K. Synthesis of Continuous Silicon Carbide Fiber. Part Ⅲ. Pyrolysis process of Polycarbosilane and Structure of the Products [J]. J. Mater. Sci., 1983, 18:3633-3648.

[8] Cheng X Z, Xie Z F, Xiao J Y, et al. Influence of Temperature on the Properties of Polycarbosilane [J]. J. Inorgan. & Organometal. Polym., 2005, 15(2): 253-259.

[9] 宋永才, 王岭, 冯春祥. 聚碳硅烷的合成与特性研究[J]. 高分子材料科学与工程, 1997,13(4): 30-33.

[10] Stevens M P. Polymer Chemistry [M]. Oxford University Press, New York Oxford, 1999.

[11] 楚增勇. 先驱体法碳化硅纤维缺陷形成机理与性能提高研究[D]. 长沙:国防科技大学,2003.

[12] 刘辉. 聚碳硅烷纤维成型的基础研究[D]. 长沙: 国防科技大学, 2002.