一种代理移动IPv6认证协议

周华春,张宏科,秦雅娟
(北京交通大学 电子信息工程学院,北京 100044)

摘 要: 代理移动IPv6为移动节点提供了基于网络的移动性管理方法,移动节点不参与管理移动性信令.为了在移动互联网络中应用代理移动IPv6协议,需要定义安全有效的认证协议.目前还没有见到关于代理移动IPv6认证协议方面的研究,本文提出了一种代理移动IPv6的认证协议,该认证协议可以提供接入认证功能,并可防止重放攻击和密钥暴露.为了分析该认证协议的性能,本文给出了认证费用和认证延迟分析的解析模型,分析了移动性和流量参数对认证费用和认证延迟的影响.研究结果表明提出的代理移动IPv6认证协议安全有效.

关键词: 代理移动IPv6; 认证延迟; 认证费用; 解析模型
中图分类号: TN915.03 **文献标识码:** A **文章编号:** 0372-2112 (2008) 10-1873-08

An Authentication Protocol for Proxy Mobile IPv6

ZHOU Hua-chun, ZHANG Hong-ke, QIN Ya-juan
(*School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing* 100044, *China*)

Abstract: Proxy Mobile IPv6 provides a means of network-based mobility management for mobile nodes without involving the mobile nodes themselves in the mobility signaling. To make Proxy Mobile IPv6 protocol feasible in mobile Internet, a new defined authentication protocol should be accompanied. To the best of our knowledge, no studies have been conducted in the area of Proxy Mobile IPv6 authentication protocol. This paper proposes an authentication protocol in Proxy Mobile IPv6. In addition to providing access authentication, the proposed authentication protocol prevents threats such as replay attack and key exposure. Also, we develop analytic models for the authentication latency and cost analysis. Then, the impacts of mobility and traffic parameters on the authentication cost and latency are analyzed, respectively. The results reveal that the proposed authentication protocol for Proxy Mobile IPv6 is secure and effective.

Key words: proxy mobile IPv6; authentication latency; authentication cost; analytic model

1 引言

移动IPv6[1]保证移动节点在切换时维持与互联网的连通性.然而,移动IP协议以移动节点为中心,切换相关的决策多数由移动节点单独做出.

最近WiMAX论坛和3GPP等标准化组织有关网络结构的研究进展表明了支持代理移动IP方案的需求.WiMAX网络结构[2]当前支持代理移动IPv4,保证没有移动IPv4客户端的主机的移动性.代理移动IPv6方案正好与WiMAX结构方向一致.3GPP也对代理移动IPv6表示了一定兴趣,主要在系统结构演进工作文档[3].代理移动IPv6标准化的目标是定义移动IPv6的简单扩展,支持IPv6主机的基于网络的移动性管理并重用移动IPv6的信令和特性.

文献[4]定义了代理移动IPv6(Proxy Mobile IPv6, PMIPv6)协议,它是一个基于网络的移动性管理协议,设计时尽量重用移动IPv6实体和概念.该协议中,移动节点由标识符(Network Access Identifier, NAI)区分,其家乡前缀等相关信息存放在网络的配置文件中.移动接入网关(Mobile Access Gateway, MAG)配置在接入路由器上,从AAA服务器(Authentication, Authorization and Accounting)检索移动节点的配置信息,发送定制的路由器通告到移动节点,仿真移动节点的家乡网络行为.移动节点在网络接口上配置其家乡地址.由于移动节点总是接受到同样的家乡前缀,就认为自己在家乡网络域.进一步,移动接入网关代替移动节点完成到区域移动性锚点(Local Mobility Anchor, LMA)的绑定更新,通知区域移动性锚点当前附着的移动节点的代理转交地址(Proxy

收稿日期:2007-07-09;修订日期:2008-08-31
基金项目:国家973重点基础研究发展规划(No.2007CB307106);国家自然科学基金(No.60573001, No.60674008, No.60870015);高等学校科技创新工程重大项目培育资金(No.706005)

Care-of Address, PCoA)就是移动接入网关的地址.这些过程导致区域移动性锚点和移动接入网关之间隧道的建立.

然而,代理移动 IPv6 协议假定移动节点实现了移动节点标识符选项,移动节点和移动接入网关在接入链路上建立了信任关系,点到点接入链路和每移动节点一个前缀地址模型.该协议没有给出得到移动节点配置文件的移动接入网关与 AAA 服务器的交互模式,移动接入网关代替移动节点发送代理绑定更新消息的授权方法,区域移动性锚点发现机制,移动接入网关之间的序列号同步方法,代理移动 IPv6 和移动 IPv6 集成方法,路由优化技术以及移动接入网关检测拜访移动节点丢失机制.

为了在移动互联网络中应用代理移动 IPv6 协议,需要定义安全有效的认证协议.目前,还没有针对代理移动 IPv6 的认证协议.虽然针对移动 IPv4/IPv6 主机移动性提出了一些 AAA 协议,但这些协议实现按节点认证模式.

IETF RFC4721[5](RFC3012 的更新)定义了代理通告和注册请求扩展选项,允许外地代理使用质询/应答机制认证移动节点,以及移动-AAA 认证扩展允许移动节点提供证书获得授权.外地代理可以与 AAA 服务器交互得到安全指示授权移动节点使用本地网络资源.文献[6]提出了基于质询/应答机制[5]的系统模型,定量地分析了认证对安全和服务质量的影响.

按照 Diameter[7]协议针对移动 IPv4 的扩展[8],移动节点可以从家乡和外地服务运营商接受服务,允许 Diameter 服务器为移动 IPv4 节点提供认证、授权服务和收集计费信息.Diameter 协议针对移动 IPv6 的扩展[9]允许移动 IPv6 节点在完成 Diameter 协议后接入服务网络.文献[10]基于文献[9]提出了移动路由器和附着拜访移动节点的局域 AAA 协议.

利用移动节点和家乡代理之间的预共享密钥,IETF 移动 IPv6 工作组设计了保护移动 IPv6 信令消息的认证协议[11,12].该机制类似于移动 IPv4 协议[13]内嵌的信令认证机制.ITEF MIPSHOP 工作组正在设计快速移动 IPv6 认证协议保护移动节点和接入路由器之间的切换信令安全[14].由于切换信令消息的认证[12,14]仅限于保护绑定更新消息,文献[15]描述了一种新的接入路由器授权移动节点接入网络的安全认证协议,需要的认证密钥与前接入路由器使用的认证密钥分离.文献[12,14,15]中的密钥生成机制类似于移动 IPv4 密钥生成机制[16],允许 AAA 服务器从移动节点和 AAA 服务器之间的 AAA 安全联盟(Security Association, SA)动态创建移动节点和家乡代理(Home Agent, HA)之间的基于共享密钥的 MN-HA 安全联盟.

代理移动 IPv6 协议是基于网络的移动性协议,移动节点的移动性管理信令由网络实体代替完成.这里,移动接入网关通常配置在接入路由器上,向区域移动性锚点更新移动节点的位置.因此,所有的移动 IPv4/IPv6 认证协议[5~16]不能直接应用到代理移动 IPv6 协议中,需要为代理移动 IPv6 域中的移动节点设计新的认证过程.

本文提出一种代理移动 IPv6 认证协议.该协议给出获取移动节点配置文件的移动接入网关与 Diameter AAA 服务器的交互过程,代理移动 IPv6 网络认证移动节点的方法,移动接入网关代替移动节点发送代理绑定更新消息的授权方法.

本文在第 2 节描述了代理移动 IPv6 协议,然后在第 3 节给出了代理移动 IPv6 的认证模式,在第 4 节给出了认证费用和延迟的解析模型以及性能分析结果,最后一节给出了结论.

2 代理移动 IPv6 协议

本节利用 IEEE 802.21 定义的链路层触发子[17]描述代理移动 IPv6 方法,并给出代理移动 IPv6 快速切换方法.

2.1 代理移动 IPv6 移动检测方法

链路层触发子可看作是链路层通知某一特定事件已经发生或者即将发生的一种抽象.链路层信息例如信号强度可以连续不断地获得,同时还可以提供关于当前链路质量的有价值的信息.相比 3 层路由器通告算法,链路层触发子允许移动节点或移动接入网关快速检测连接丢失.

链路将断开(Link Going Down)触发子表明移动节点测量到当前移动接入网关差的信号,在某个时间内即将断开.链路断开(Link Down)触发子表明移动节点与前一个移动接入网关之间(Previous Mobile Access Gateway, PMAG)的链路已断开,而链路连接(Link Up)触发子表明移动节点与新移动接入网关(New Mobile Access Gateway, NMAG)之间的链路已建立.

链路层与网络层的交互有多种方法[17,18].本文采用移动节点触发而网络发起的切换方法.移动节点连续检测当前移动接入网关的信道.得到的链路层信息通过 IEEE 802.21 UDP/IP 媒质独立切换消息传输协议[19]传送到移动接入网关.

. 如果移动节点接收的信号强度低于门限值,移动节点将发送 Link Going Down 触发子.移动接入网关在链路层触发移动节点将要切换的网络层.

2.2 代理移动 IPv6 方法

代理移动 IPv6 是基于网络的移动性管理协议,基于移动 IPv6.代理移动 IPv6 域是一个区域移动性管理

域.该域是接入网的一部分,移动节点的移动性管理由代理移动 IPv6 协议处理.区域移动性锚点 LMA 是移动节点在代理移动 IPv6 域的家乡代理.LMA 拥有移动 IPv6 定义的家乡代理的全部功能.另外,LMA 是移动节点家乡前缀的拓扑锚点,管理移动节点的可达性状态.移动接入网关 MAG 是网络中代理移动代理,负责移动节点的移动性管理.移动接入网关检测移动节点的运动,代替移动节点向区域移动性锚点发出移动性信令更新到移动节点家乡地址的路由.

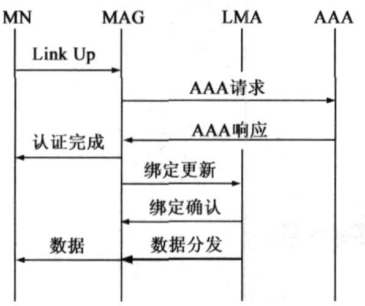

图1　代理移动IPv6协议操作流程

代理移动 IPv6 协议操作流程如图 1 所示.

当移动节点进入代理移动 IPv6 域,Link Up 触发子出现表明移动节点与移动接入网关之间的链路已建立.移动节点发送 Link Up 触发子信息到移动接入网关.

当移动节点进入代理移动 IPv6 域附着到接入链路,在接入认证过程中移动节点需要提交它的身份标识符(network access identifier,NAI)[20].一旦认证完成,移动接入网关从策略数据库如 AAA 处,得到移动节点的配置信息.策略配置信息包括配置的基于网络移动性服务特性,以及如移动节点家乡网络前缀、允许的地址配置模式、漫游策略等配置基于网络移动性服务必要的参数.移动接入网关有了在接入链路上仿真移动节点家乡网络的所有信息.移动接入网关也向移动节点发出周期性的路由器通告,通告其家乡网络前缀.

当前代理移动 IPv6 定义支持每移动节点一个前缀地址模型.在该模型中,每个移动节点单独分配到唯一的家乡网络前缀,并且该前缀不配置在家乡链路上.区域移动性锚点仅是拓扑锚点,前缀配置在移动节点附着的接入链路上.接入链路上接受这些路由器通告的移动节点根据接入链路允许的模式,采用有/无状态配置模式配置其接口.

移动接入网关发送代理绑定更新(Proxy Binding Update,PBU)消息到移动节点的区域移动性锚点,更新移动节点的当前位置.该消息包括移动节点的标识符选项和家乡网络前缀选项.消息的源地址是移动接入网关出口的地址.在接受到代理绑定更新请求后,区域移动性锚点发出代理绑定确认(Proxy Binding Acknowledgment,PBA)消息到移动接入网关.同时,区域移动性锚点建立通过隧道到移动节点家乡网络前缀的路由.

移动接入网关接受到代理绑定确认消息后,建立到区域移动性锚点的隧道,增加通过隧道到达区域移动性锚点的缺省路由.移动节点所有数据包均通过隧道路由到移动节点的区域移动性锚点.

此时,移动节点在当前的附着点,有一个从其家乡网络前缀配置的有效家乡地址.服务移动接入网关和区域移动性锚点同时有处理与移动节点之间数据包的路由状态.对移动节点来说,整个代理移动 IPv6 域像是它的家乡链路或单个链路.

2.3　代理移动 IPv6 快速切换方法

在文献[21]中,作者探讨了利用链路层事件改进基于网络的区域移动性管理切换过程的可能性,试图利用快速移动 IPv6[22]的前/新路由器之间消息改进切换性能.该模式利用 IEEE 802.21[17]链路层事件在切换前触发建立前/新移动接入网关之间的隧道.然而,文献[21]没给出前/新路由器之间相关消息的详细定义.

根据 2 层切换信令是否在前一链路完成,代理移动 IPv6 快速切换有 2 种操作模式,分别是预先模式和反应模式.所谓预先模式是指 2 层切换信令在前一链路完成.

由于预先模式相比于反应模式有较低的切换延迟,限于篇幅,本文只讨论预先模式的代理移动 IPv6 快速切换方法,如图 2 所示.

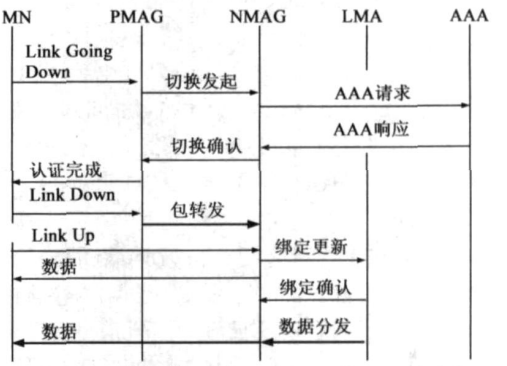

图2　预先模式代理移动IPv6快速切换协议操作流程

从家乡代理的角度来看,附着到同一个移动接入网关的所有移动节点共享一个或多个代理转交地址作为它们在代理移动 IPv6 域的转交地址.这些代理转交地址可以是移动接入网关的出口 IP 地址,或是它的环回 IP 地址.

在移动节点从前移动接入网关移动到新移动接入网关前,移动节点和前接入路由器开始了 2 层触发子信息交互.移动节点从链路层发送到网络层的 Link Going Down 触发子通知前移动接入网关链路断开事件很快发生.该触发子必须包含新移动接入网关标识(NMAG ID,NMAGID).

PMAG 在接受到 Link Going Down 消息后,检索 NMAG 的代理转交地址,发送包含移动节点的标识符选项、移动节点的 IP 地址选项、PMAG 的代理转交地址选

项和移动节点的链路层地址选项在内的切换发起消息(Handover Initiate, HI). 根据该消息, NMAG 为移动节点建立邻居缓存表项.

为响应切换发起消息, NMAG 向 PMAG 发出切换确认消息(Handover Acknowledge, HAck). 一旦 PMAG 接受到切换确认消息, 双向隧道就建立起来, 隧道端点分别是 PMAG 和 NMAG 的代理转交地址.

PMAG 对来自 LMA-PMAG 隧道的数据包解封装, 通过 PMAG-NMAG 隧道将数据包中继到 NMAG. 移动节点从链路层发送到网络层的 Link Up 触发子通知新移动接入网关移动节点已经与之建立 2 层链路. NMAG 发出包含 NMAG 信息的路由器通告, 移动节点可以发送数据包. NMAG 将缓存的数据包发给移动节点.

3 代理移动 IPv6 认证协议设计

本节给出设计的认证协议. 所提出的认证协议基于 DIAMETER 协议[7]和移动 IPv6 认证协议[9,11].

3.1 认证结构

假定移动节点用全球唯一网络接入标识符 NAI 来标识. 假定 AAA 服务器, 区域移动性锚点 LMA 和移动接入网关 MAG 之间预先建立了安全密钥. AAA 服务器和移动接入网关 MAG 之间的信任关系通过 DIAMETER 协议维护.

每个代理移动 IPv6 域的 AAA 服务器可以 DIAMETER 模式认证每一个移动节点. AAA 服务器拥有移动节点的配置文件, 与移动节点共享一个长期密钥. 移动接入网关 MAG 负责拜访移动节点的认证过程. AAA 客户端配置在移动接入网关 MAG 上.

当移动节点发起新会话时, 移动节点需要认证, 也就是初始认证(initial authentication). MAG 作为服务员, 服务于移动节点的认证, 广播服务通告消息. 当 MAG 接受到移动节点的认证请求, MAG 触发到 AAA 服务器的认证过程, 与 AAA 服务器协作证实移动节点的身份. 当移动节点改变网络接入点时, 在接入新的 MAG 时需要进行认证, 也就是切换认证(handover authentication).

3.2 初始认证过程

当移动节点在代理移动 IPv6 域发起新的会话, 初始认证过程就被发起. 初始认证过程信息流如图 3 所示.

(1)移动节点发出服务者请求(Attendant Solicit, AS)消息到服务者 MAG. 服务者请求和通告(Attendant Advertisement, AA)消息是 2 个 ICMP 消息[10], 分别类似于路由器请求和通告消息.

(2)MAG 响应服务者请求消息, 发回包含局域质询 LC(local challenge)的服务者通告消息. LC 是 MAG 发出的质询值, 用于认证过程的一个随机数. 即使没有服务者请求消息, MAG 也周期性广播服务者通告消息.

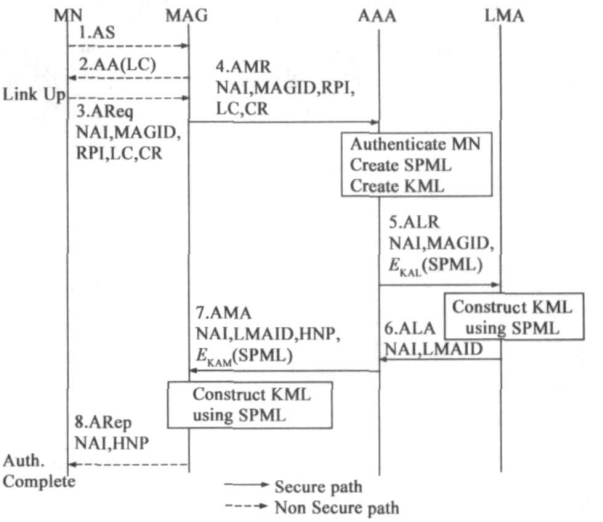

图3 移动节点初始认证过程

(3)移动节点使用与 AAA 服务器之间的长期密钥 KAAA 加密 LC 值, 产生 AAA 服务器认证移动节点的证书(credential, CR).

$$CR = E_{KAAA}(LC), \tag{1}$$

$E_K(\cdot)$是使用密钥 K 的加密函数.

移动节点在网络层接受到来自链路层的 Link Up 触发子后, 移动节点发出包含 LC 和 CR 的认证请求(AReq)消息到 MAG. AReq 消息还包含移动节点的网络接入标识符 NAI, MAG 的标识符(MAGID)和重放保护指示(replay protection indicator, RPI), 用于 AAA 服务器鉴别移动节点和防止重放攻击. RPI 是一时间戳或随机数.

(4) MAG 接受到 AReq 消息后, 将其转换成 AA-MAG-Request(AMR)消息, 然后发送到 AAA 服务器.

(5)AAA 服务器接受到 AMR 消息后, 使用预建立的 SA(KAAA)加密 LC, 并将结果与 CR 值比较. 如果 2 个值相等, 移动节点就被成功认证. 之后, AAA 服务器创建密钥生成随机数 SPML 并创建 KML. 本协议中 *KML* 表示 MAG 和 LMA 之间的动态密钥. AAA 服务器生成 *KML* 用于 MAG 和 LMA 之间的双向隧道安全.

$$KML = HMAC - SHA1(KAAA, (SPML \parallel NAI \parallel MAGID \parallel LMAID \parallel 128)), \tag{2}$$

HMAC-SHA1(K, m)[23]是消息 m 和密钥 K 的密钥哈希函数. (2)表明了移动接入网关代替移动节点发送代理绑定更新消息的授权方法.

为保证 MAG 生成 KML, AAA 服务器发送 SPML 到 MAG. 用 AAA 服务器和 MAG 之间预共享长期密钥 KAM 加密 SPML, 避免 SPML 暴露给其他网络实体.

AAA 服务器发送 AA-LMA-Request(ALR)通知 LMA 移动节点的 NAI 和 *SPML*. 用 AAA 服务器和 LMA 之间

预共享长期密钥 KAL 加密 SPML,避免 SPML 暴露给其他网络实体.

(6)LMA 使用 SPML 创建 KML,发回 AA-LMA-Answer (ALA)确认消息.

(7)AAA 服务器发出 AA-MAG-Answer(AMA)消息通知 MAG 认证结果.

(8)当接受到 AMA 消息,MAG 知道移动节点已被认证,授权移动节点网络接入.MAG 使用与 AAA 服务器的长期密钥 KAM 解密该消息,记录 LMA 的标识(LMAID),按式(2)创建 KML.此外,MAG 发出包含家乡网络前缀 HNP(home network prefix)等选项的认证响应消息(ARep),通知移动节点认证结果.

移动节点接受到 ARep 消息后,可以接入 MAG.

在 MAG 和 LMA 分别创建 KML 后,MAG 和 LMA 分别创建 MAG 和 LMA 之间的动态安全联盟.MAG 按照文献[11]构造移动性消息认证选项,发送包含该认证选项的代理绑定更新消息到 LMA.LMA 发出包含一个移动性消息认证选项的代理绑定确认消息到 MAG.代理绑定更新和代理绑定确认消息由新创建的 MAG 和 LMA 之间的安全联盟保护.

3.3　切换认证过程

图 4 给出了切换认证过程.图 3 和图 4 的不同之处解释如下.

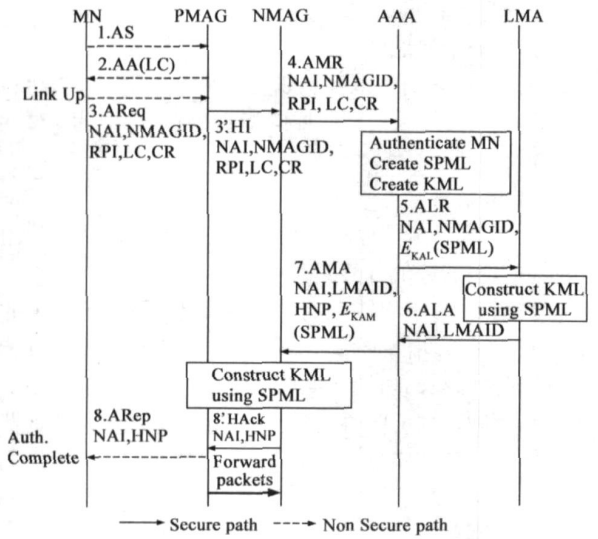

图4　移动节点切换认证过程

(3)当移动节点在网络层接受到来自链路层的 Link Going Down 触发子后,移动节点发出的 AReq 消息包含新移动接入网关 NMAG 的标识(NMAGID)到 PMAG.

(3′)PMAG 向 NMAG 发出的切换发起消息(HI)包含 AReq 消息.

(8′)为响应 HI 消息,NMAG 向 PMAG 发出的切换确认消息(HAck)包含 ARep 消息.

4　性能分析

本节分析所提出的认证协议的性能.首先得到认证请求的到达速率,然后评估平均认证费用和延迟.在给出评估平均认证费用和延迟的参数后,给出数值分析结果.

4.1　认证请求的到达速率

当一个呼叫到达时,初始认证过程就被发起.由于切换认证发生在会话中的移动节点穿越代理移动 IPv6 域的子网边界,设移动节点在当前代理移动 IPv6 域穿越 MAG 的平均数量为 N_s,则平均切换认证数量为 N_s-1.本文假定一个 MAG 控制一个子网.则认证请求到达速率 λ 可写成下式

$$\lambda = \lambda_\mu + \lambda_\mu(N_s - 1) = \lambda_\mu N_s, \tag{3}$$

上式中 λ_μ 是呼叫到达速率.移动节点的流量模式定义为移动节点的呼叫到达速率,包括呼入/出呼叫,服从平均速率为 λ_μ 的泊松(Poisson)过程.

为评估 N_s,定义移动节点的移动性模式.移动节点的移动性模式表示为移动节点在一个 MAG 内的驻留时间 T_r.假定 T_r 是一个随机变量,其概率密度函数服从均值为 $1/\mu_r$ 方差为 V 的 Gamma 分布[24].进一步假定呼叫持续时间 T_D 服从均值为 $1/\eta$ 的指数分布.由文献[25,6],N_s 可由下式得到

$$N_s = \frac{\mu_r}{\eta}, \tag{4}$$

其中 $1/\eta$ 是移动节点的平均会话持续时间,$1/\mu_r$ 是移动节点在一个 MAG 内的平均驻留时间.从而,认证请求到达速率 λ 与移动节点的流量和移动性模式相关联.

4.2　平均认证费用

定义认证费用为每次认证过程中信令费用和处理费用之和.每次认证的初始认证费用 C_i 可写成:

$$C_i = 2(N_h + 2)c_s + c_v + 3c_{us} + c_g, \tag{5}$$

其中 N_h 是移动节点和 AAA 服务器之间的跳数.(5)中第一项是信令费用,其他项是处理费用.费用参数 c_s, c_v, c_{us}, c_g 分别是每跳的传输费用,AAA 服务器的认证费用,一个值的一对加解密费用以及密钥生成费用.

由图 3 知,移动节点首先需要从 MAG 请求质询值.消息遍历的距离为 2 跳.然后,认证消息到达 AAA 服务器.移动节点和 AAA 之间的距离假定为 N_h 跳.由于在 MAG 和 LMA 没有安全联盟,需要一个到达 LMA 的认证过程,这就在整个认证消息往返传输中增加 2 跳距离.于是,整个认证消息往返传输经过的总跳数为 $2+2N_h+2=2(N_h+2)$.

在认证过程中,质询/响应值在 AAA 处被检验一次.因此,c_v 的系数为 1.在此过程中,需要 3 对加解密费用.第 1 对是移动节点和 AAA 之间的质询/响应值的加解密,第 2 对是 AAA 和 LMA 之间的会话密钥的加解密,第 3 对是 AAA 和 MAG 之间的会话密钥的加解密.

因此 c_{us} 的系数是 3. 由于 AAA 需要为 LMA 和 MAG 生成 1 个动态密钥，c_g 的系数为 1.

由图 4 知，可以确定每次认证的切换认证费用 C_h 如下：

$$C_h = 2(N_h + 2)c_s + c_v + 3c_{us} + c_g + 2N_m c_s, \quad (6)$$

其中最后一项处理费用 $2N_m c_s$ 是在 PMAG 和 NMAG 之间传输 HI 和 HAck 消息的费用. 费用参数 N_m 是 PMAG 和 NMAG 之间的跳数.

平均认证费用 $\bar{C}$ 定义为每个单位时间的所有认证请求的认证费用之和，可写成

$$\bar{C} = \lambda_\mu C_i + \lambda_\mu (N_s - 1) C_h, \quad (7)$$

其中 C_i 和 C_h 分别是(5)和(6)定义的初始认证和切换认证费用，λ_u 为呼叫到达速率.

4.3 平均认证延迟

定义认证延迟为移动节点发出认证请求到接受认证响应的时间间隔. 则初始认证延迟 T_i 可写成下式：

$$T_i = 2(N_h + 2)(t_{pr} + t_{tr}) + 3t_m + 2t_v + 3t_{us} + t_g, \quad (8)$$

其中时间参数 $t_{pr}, t_{tr}, t_m, t_v, t_{us}, t_g$ 分别是每跳的消息发布时间，每跳的消息传输时间，认证请求在 MAG 处的服务和等待时间，认证请求在 AAA 处的服务和等待时间，一个值的一对加解密时间以及在 AAA 处的密钥生成时间.

T_i 表达式中时间变量前的系数表示每次认证的时间变量的数量. 类似于(5)的分析，得到整个认证消息往返传输经过的总跳数为 $2(N_h + 2)$. 因此 $t_{pr} + t_{tr}$ 前的系数为 $2(N_h + 2)$.

由于认证过程需要穿过 MAG 共 3 次，认证请求的服务和等待时间 t_m 的系数为 3. 由于认证消息遍历 AAA 服务器 2 次，认证请求的服务和等待时间 t_v 的系数为 2. 类似于(5)中 c_{us} 和 c_g 的系数分析，得到 t_{us} 的系数为 3，t_g 的系数为 1.

由图 4 知，切换认证延迟 T_h 可写成：

$$T_h = 2(N_h + 2)(t_{pr} + t_{tr}) + 3t_m + 2t_v + 3t_{us} + t_g + 2N_m(t_{pr} + t_{tr}) \quad (9)$$

其中时间参数 N_m 是 PMAG 和 NMAG 之间的跳数.

平均认证延迟定义为每个单位时间的所有认证请求的认证延迟之和，可写成

$$\bar{T} = \lambda_\mu T_i + \lambda_\mu (N_s - 1) T_h, \quad (10)$$

其中 T_i 和 T_h 分别是(8)和(9)定义的初始认证和切换认证延迟，λ_u 为呼叫到达速率.

4.4 数值分析参数

表 1 列出了评估认证费用和延迟的参数. 一些参数来自于文献[6]和[26].

式(5)和(6)的认证费用可以采用消息数量来测量[10]. 本文采用处理时间比表示认证费用[6]，这是由于完成一个操作所需时间可表示完成该项操作的服务器的负荷. 将密钥生成费用 c_g 标准化为 1 个费用单位，由于它相对于其他费用来说，工作负荷最轻. 其他费用值用其完成操作所需时间与 c_g 的比值得出.

表 1 评估参数

c_s	c_v	c_{us}	c_g	N_h	N_m
10	20	1	1	4	1
t_{pr}	t_{tr}	t_{us}	t_g		
40μs	20ms	2ms	2ms		
λ_u	η	μ_r	ξ		
0.1min^{-1}	0.3min^{-1}	$1/3\ \text{min}^{-1}$	15s^{-1}		

在式(8)和(9)中，仅考虑时间变量 t_m 和 t_v 为随机变量，这是由于其他时间变量的变化较小. t_{pr} 是 2 点之间距离的函数，t_{tr} 由消息长度和链路速率确定，t_{us} 主要与计算机能力和消息长度有关，t_g 直接与计算机能力有关. 在实际认证情形下，2 点之间距离，消息长度，链路速率和计算机能力均固定. 因此，本文不考虑 t_{pr}，t_{tr}，t_{us} 和 t_g 为随机变量. 然而，t_m 和 t_v 均与流量负荷，队列长度和服务时间相关，而这些因素时时变化，有大的方差.

为简化讨论，考虑 MAG 和 AAA 处应用 M/M/1 排队模型，t_m 和 t_v 的概率密度函数为独立同分布，则 t_m 和 t_v 的概率密度函数 $w(t)$ 可从文献[6,27]得到，如下式所示：

$$w(t) = (\mu_s - \lambda_s)e^{-(\mu_s - \lambda_s)t}, \quad (11)$$

其中 μ_s 和 λ_s 分别是认证请求服务和到达速率. 由(11)知，随机变量 t_m 和 t_v 为同样的指数分布，均值为 $1/\xi$，$\xi = \mu_s - \lambda_s$.

4.5 数值结果

图 5－8 给出了移动性和流量模式对平均认证费用和延迟影响的数值分析结果.

在图 5 中，平均认证费用随移动节点在 MAG 内的驻留时间 $1/\mu_r$ 增加而降低，这是由于移动节点在 MAG 内停留时间越长，切换认证请求就越少. 并且，当移动节点驻留时间达到无限时，认证费用会稳定在初始认证费

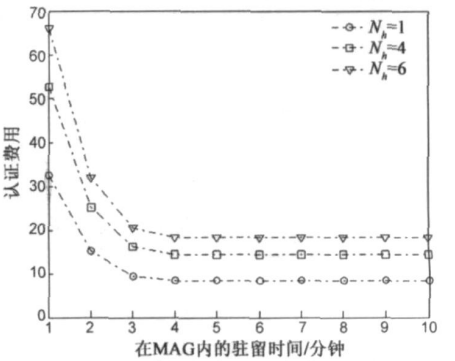

图5 认证费用与在MAG内的驻留时间

用上,这是由于此时仅有初始认证费用.相反,当驻留时间趋于0时,多数认证为切换认证,平均认证费用趋于无限,但为清晰起见,图5未画出此情形.

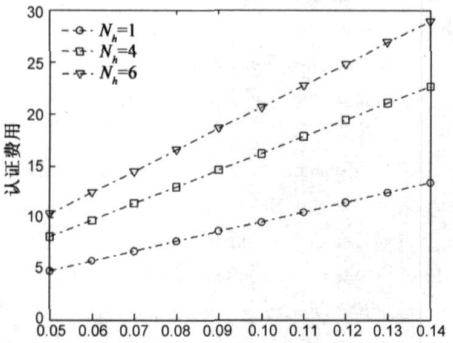

图6　认证费用与呼叫到达速率

图6显示平均认证费用随移动节点的呼叫到达速率 λ_u 增加.由(7)知认证费用比例于呼叫到达速率 λ_u.

图5和图6表明平均认证费用随移动节点和AAA服务器之间的跳数增加 N_h 而增加,这是由于需要的传输费用多一些.

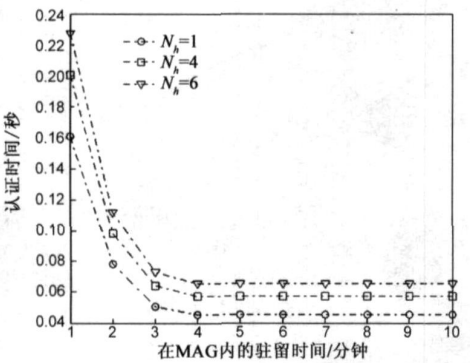

图7　认证时间与在MAG内的驻留时间

图7显示了驻留时间对平均认证延迟的影响.可见,认证延迟随移动节点在MAG内的驻留时间 $1/\mu_r$ 增加而降低.类似于认证费用的分析,该趋势是由于切换认证请求的降低引起.并且,当移动节点驻留时间达到无限时,认证延迟会稳定在初始认证延迟上.相反,当驻留时间趋于0时,多数认证为切换认证,平均认证延迟趋于无限,但为清晰起见,图7未画出此情形.

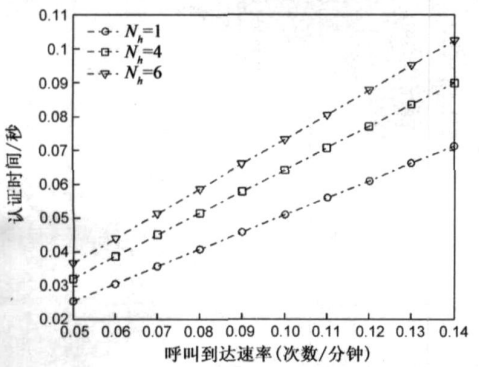

图8　认证时间与呼叫到达速率

图8显示平均认证延迟随移动节点的呼叫到达速率 λ_u 增加.由(10)知认证延迟比例于呼叫到达速率 λ_u.

图7和图8表明平均认证延迟随移动节点和AAA服务器之间的跳数增加 N_h 而增加,这是由于需要的消息发布时间和消息传输时间多一些.

5　结论

本文提出一种代理移动IPv6认证协议.该协议给出移动接入网关与Diameter AAA服务器的交互过程,代理移动IPv6网络认证移动节点的方法,移动接入网关代替移动节点发送代理绑定更新消息的授权方法.除此之外,该认证协议可以防止重放攻击和密钥暴露.为了分析该认证协议的性能,本文给出了认证费用和认证延迟分析的解析模型,分析了移动性和流量参数对认证费用和认证延迟的影响.研究结果表明提出的代理移动IPv6认证协议安全有效.

参考文献:

[1] Johnson D, Perkins C, and J Arkko. Mobility Support in IPv6 [S]. IETF RFC 3775, June 2004.

[2] WiMAX End-to-End Network Systems Architecture, (Stage 2: Architecture Tenets, Reference Model and Reference Points) [OL]. http://www.wimaxforum.org/technology/documents, 2007.

[3] 3GPP, 3GPP system architecture evolution (SAE): Report on technical options and conclusions [S]. 3GPP TR 23.882 0.10.1, February 2006.

[4] S Gundavelli, K Leung, V Devarapalli, K Chowdhury and B Patil. Proxy Mobile IPv6 [S]. IETF draft-ietf-netlmm-proxymip6-00, April 2007.

[5] C Perkins, P Calhoun and J Bharatia. Mobile IPv4 Challenge/Response Extensions (Revised) [S]. IETF RFC 4721, January 2007.

[6] Wei Liang and Wenye Wang. On performance analysis of challenge/respons based authentication in wireless local area networks [J]. In Computer Networks (Elsevier), 2005, 48(2): 267 - 288.

[7] Calhoun P, Loughney J, Guttman E, Zorn G, and J Arkko. Diameter Base Protocol [S]. IETF RFC 3588, September 2003.

[8] P Calhoun, T Johansson, C Perkins, T Hiller, Ed. P McCann. Diameter mobile IPv4 application [A]. IETF RFC 4004 [C], August 2005.

[9] Franck Le, Basavaraj Patil, Charles E. Perkins, Stefano Faccin, Diameter Mobile IPv6 Application [S]. IETF draft-le-aaa-diameter-mobileipv6-04, Nov. 2004.

[10] Sungmin Baek, Sangheon Pack, Taekyoung Kwon, and Yanghee Choi. A localized authentication, authorization, and accounting (AAA) protocol for mobile hotspots [A]. In Proc. IEEE/IFIP Annual Conference on Wireless On demand Network Systems and Services (WONS) 2006 [OL]. http://citi. insa-lyon. fr/wons2006/Articles/17-Baek. pdf, Les Menuires, France, January 2006.

[11] Patel, A. Authentication Protocol for Mobile IPv6 [S]. IETF RFC 4285, January 2006.

[12] V Devarapalli, A Patel, K Leung and K Chowdhury. Mobile IPv6 Bootstrapping for the Authentication Option Protocol [S]. IETF draft-devarapalli-mip6-authprotocol-bootstrap-02, March 2007.

[13] Perkins, C. IP Mobility Support for IPv4 [S]. IETF RFC 3344, August 2002.

[14] V Narayanan, N Venkitaraman, H Tschofenig, G Giaretta and J Bournelle. Handover Keys Using AAA [S]. IETF draft-vidya-mipshop-handover-keys-aaa-04, March 2007.

[15] Souhwan Jung and Jaeduck Choi. Access Authentication Protocol in FMIP6 [S]. IETF draft-jung-mipshop-access-auth-00, February 2006.

[16] Perkins C and P Calhoun. Authentication, Authorization, and Accounting (AAA) Registration Keys for Mobile IPv4 [S]. IETF RFC 3957, March 2005.

[17] IEEE, Draft IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services [S]. IEEE P802.21/D04.00, February 2007.

[18] A Festag. *Optimization of handover performance by link layer triggers in IP-based networks*; parameters, protocol extensions, and APIs for implementation [R]. Technical Report TKN-02-014, Telecommunication Networks Group, Technische Universität Berlin, July 2002.

[19] A Rahman, U Olvera-Hernandez, M Watfa. Transport of media independent handover messages over IP [S]. ITEF draft-rahman-mipshop-mih-transport-00, June 2006

[20] Patel A, Leung K, Khalil M, Akhtar H, and K Chowdhury. Mobile Node Identifier Option for Mobile IPv6 (MIPv6) [S]. IETF RFC 4283, November 2005.

[21] Xia F and B Sarikaya. Mobile Node Agnostic Fast Handovers for Proxy Mobile IPv6 [S]. IETF draft-xia-netlmm-fmip-mnagno-00, February 2007.

[22] Koodli R. Fast Handovers for Mobile IPv6 [S]. IETF RFC 4068, July 2005.

[23] Krawczyk H, Bellare M and R Canetti. HMAC: Keyed-Hashing for Message Authentication [S]. IETF RFC 2104, February 1997.

[24] J Ho, I Akyildiz. Mobile user location update and paging under delay constraints [J]. Wireless Networks, 1995, 1(4): 413 - 425.

[25] Y Fang, I Chlamtac, Y Lin. Channel occupancy times and handoff rate for mobile computing and PCS networks [J]. IEEE Transactions on Computer, 1998, 47(6): 679 - 692.

[26] A Hess, G Schafer. Performance evaluation of AAA/mobile IP authentication [OL]. http://www-tkn.ee.tu-berlin.de/publications/papers/pgts2002.pdf, 2002.

[27] D Gross, C Harris. Fundamentals of Queueing Theory [M]. Wiley, New York, 1974.

作者简介:

周华春 男,1965 年 8 月生于安徽,硕士,副教授,主要研究方向为 IPv6 路由器、移动互联网、网络与信息安全、通信软件等研究和开发.
E-mail: hchzhou@bjtu.edu.cn

张宏科 男,1957 年 9 月生于山西,博士、教授、博士生导师,现在北京交通大学电子信息学院下一代互联网研究中心工作. 研究方向: IPv6 网络、路由理论和下一代网络理论与技术等. 国家 973 重点基础研究发展规划项目"一体化可信网络与普适服务体系基础研究"首席科学家.

秦雅娟 女,1963 年 6 月生于山西,博士、副教授. 主要研究方向为一代网络路由交换技术、移动互联网技术、宽带无线通信.