第 34 卷　第 17 期　　计　算　机　工　程　　2008 年 9 月
Vol.34　No.17　　Computer Engineering　　September 2008
·网络与通信·　文章编号：1000—3428(2008)17—0105—03　文献标识码：A　中图分类号：TP393.08

基于认证的移动 IPv6 地址自动配置方法

皇甫璐子，罗军勇，有业斌
(信息工程大学信息工程学院，郑州 450002)

摘　要：在普遍发生 MIPv6 切换的网络环境下，针对 MN 执行重复地址检测和家乡注册所造成的切换延迟问题，分析 MIPv6 支持的 2 种地址自动配置方式，结合网络上部署的 AAA 及 Diameter 协议在 MIPv6 上的应用，提出一种基于认证的 MIPv6 地址自动配置方法。该方法融合 AAA 身份认证、MIPv6 家乡注册以及地址配置，能有效缩短切换时延、提高接入网的安全性。

关键词：移动 IPv6；切换延迟；认证；融合

Mobile IPv6 Address Auto-configuration Method Based on Authentication

HUANGFU Lu-zi, LUO Jun-yong, YOU Ye-bin
(Information Engineering College, Information Engineering University, Zhengzhou 450002)

【Abstract】According to the handover latency caused by the duplicate address detection and home registration in the network environment of general mobile IPv6 handover, this paper anaylzes two address auto-configuration methods supported by MIPv6, combines AAA and the application of Diameter protocol with MIPv6, and brings forwards an MIPv6 address auto-configuration method based on authentication. This method combines AAA authentication, MIPv6 home registration and address auto-configuration, which can decrease the handover latency and enhance the security of network effectively.

【Key words】mobile IPv6; handover latency; authentication; combination

1　概述

随着无线网络技术与便携式终端的不断发展，在网络的 IP 层中实现对移动性的支持变得越来越重要。移动 IPv6 (Mobile IPv6, MIPv6)不仅仅是无线接入和漫游在概念上的简单叠加，其更重要的意义在于 MIPv6 协议[1]中定义的“移动”强调寻址的连续性和网络连接的连续性，并且对 TCP, UDP 等高层协议完全透明。

文献[2]提出使用 AAA(Authentication, Authorization and Accounting)消息搭载 MIPv6 信令来减少消息的往返次数，从而降低总的切换时延。但对于未经过认证的移动节点(Mobile Node, MN)，则直接提供 IP 层的访问权限，即使对访问网络的区域加以限制，也可能导致一些安全问题，如 IP 欺骗、MAC 地址欺骗[3]。这种情况在无线网络环境中会更加严重，因为无线信道容易受到干扰和窃听的影响。为了增强安全性，MIPv6 协议提出用 IPSec 协议保护家乡代理(Home Agent, HA)和移动节点之间的通信数据[4]，但是 MN 移动到异地网络后，无须接入网络的认证即可进行地址自动配置，这就造成接入网络拓扑信息的泄露，从而引发出一系列安全问题。

本文提出基于认证的移动 IPv6 自动配置方法(MIPv6 address Auto-Configuration based on Authentication, MACA)，保证移动用户在得到认证后才能获得访问网络的权限，不仅降低了切换时延，还提高了网络安全性。

2　地址自动配置

MIPv6 支持 2 种地址自动配置方式：无状态的自动配置和有状态的自动配置。前者使用起来比较简单，而且无需任何服务器的支持，移动节点通过与访问路由器交换 ICMPv6 协议报文来实现地址的无状态配置，但是这种方式使地址空间的利用率相对较低，不易管理，还可能造成网络被恶意用户窃听和截取；后者则通过地址配置服务器(如 DHCP 服务器)实现，克服了无状态配置的不足，能够对地址空间和网络资源进行有效的管理和分配，而且 DHCP 服务器能够对移动节点进行有状态的监控，有利于实现对移动节点的访问控制。

3　MACA 方法的基本思想

MACA 方法主要解决以下 3 个问题：(1)访问网络如何对移动节点实现接入认证；(2)移动节点移动到异地链路上时如何配置新的转交地址；(3)移动节点如何完成家乡注册。下面结合图 1 对 MACA 方法的实现作详细描述，MACA 方法的报文交换过程如图 2 所示。

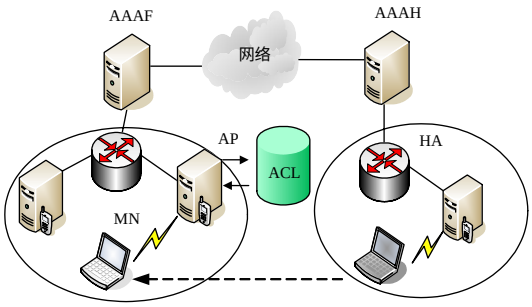

图 1　基于认证的 MIPv6 地址自动配置

作者简介：皇甫璐子(1982－)，女，硕士，主研方向：网络与信息安全；罗军勇，教授；有业斌，硕士

收稿日期：2008-01-10　**E-mail：**swolf_lulu@sina.com

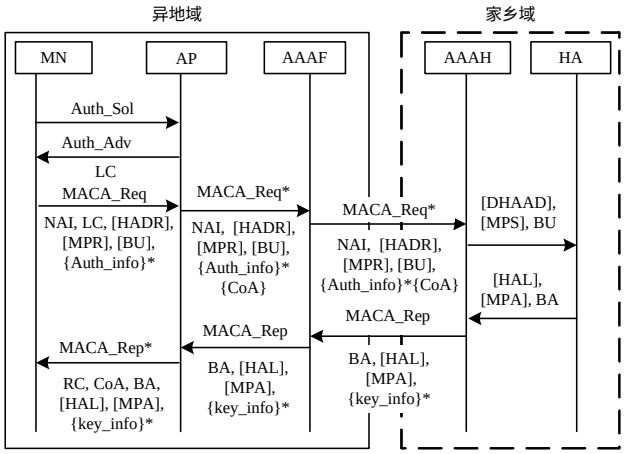

图 2　MACA 报文交换过程

在图 2 中，AAAF 表示异地 AAA 服务器；AAAH 表示家乡 AAA 服务器；[XX]表示 XX 是备选项，可根据实际需要选择；{XX}*表示 XX 是经过加密的信息；Auth_Sol 表示 Authentication Solicitation；Auth_Adv 表示 Authentication Advertisement；DHAAD 表示动态家乡代理地址发现；MPS 表示移动前缀请求；HAL 表示家乡代理列表；MPA 表示移动前缀通告。

参见图 1，认证点(Authentication Point, AP)负责对新接入的 MN 进行认证和访问控制，并把 MN 发出的认证消息重组成 AAA 服务器能够识别的报文格式，转发给 AAA 服务器，同时将 AAA 服务器的响应消息转发给 MN。

当 MN 发现(链路层触发或接收到新的路由器通告)自己移动到新的链路上时，立即启动认证过程：

(1)MN 通过发送 Auth_Sol 消息选择新接入网络中的可用 AP，初始化认证授权过程。

(2)AP 收到 Auth_Sol 消息后，返回一个响应消息 Auth_Adv，其中包括 AP 分发给 MN 的 LC(Local Challenge)。LC 用来验证 MN 是否是第 1 次进行认证请求，并可抗重放攻击。

(3)收到响应消息 Auth_Adv 后，MN 向 AP 发送一个 MACA 请求认证消息 MACA_Req，其中包括 MN 的访问网络标识符 NAI(Network Access Identity, MN 的唯一身份标识，用来识别 MN 的家乡 AAA 服务器)、经过加密的认证信息 $\{\text{Auth\_info}\}^*$、绑定更新(BU)、MN 的数字签名以及一些必要的 MIPv6 请求选项，如家乡代理发现请求(HADR)和移动前缀请求(MPR)。

如果在认证初始化阶段，MN 的家乡代理或者移动前缀的生命周期即将结束，需要立即执行动态家乡代理发现或移动前缀发现。在这种情况下，为了减少上述过程中数据传输所导致的往返时间(Round Trip Time, RTT)，可以同时请求认证服务器代替 MN 执行这些功能，此时需要在请求认证消息 MACA_Req 中分别附加对应的 HADR 选项或者 MPR 选项。

$$\text{MACA\_Req} = \{\text{NAI}\}\{\text{LC}\}\{\text{BU}\}[\text{HADR} \mid \text{MPR}]\{\text{Auth\_info}\}^* \{\text{Signature}_{\text{MN}}\}$$

(4)AP 收到认证请求消息 MACA_Req 后，开始执行以下操作：1)如果链路上有可用的 DHCPv6 服务器，则由 AP 代替 MN 预先向 DHCPv6 服务器申请一个转交地址(Care-of-Address, CoA)。2)否则，AP 根据自己所在链路的前缀信息，预先为 MN 配置一个 CoA，并执行重复地址检测(Duplicate Address Detection, DAD)验证 CoA 的唯一性。3)把 CoA 存入本地的 ACL 中，并将这个 CoA 的 T 标志位置 1。在认证结束前，这个 CoA 一直处于临时配置的状态，只有待 MN 通过认证后才将 T 置 0。4)AP 将新配置的 CoA 附加到 MACA_Req 消息(用 MACA_Req^* 表示)后，将消息转发给 AAAF 服务器。

$$\text{MACA\_Req}^* = \{\text{NAI}\}\{\text{LC}\}\{\text{BU}\}[\text{HADR} \mid \text{MPR}]\{\text{Auth\_info}\}^* \{\text{CoA}\}\{\text{Signature}_{\text{MN}}\}$$

(5) MACA_Req^* 消息经 AAAF 服务器(可能需要经过多个 AAAF 服务器)转发给 AAAH 服务器后，就开始认证过程(对 MN 的身份认证和对附加的 CoA 的验证)：

1)若消息中附带 HADR 或 MPR 选项，则 AAAH 代替 MN 执行动态家乡代理地址发现或者移动前缀请求操作，同时完成 MIPv6 家乡注册(绑定更新和绑定应答)。

2)返回认证应答消息 MACA_Rep 给 AP。该消息包含认证结果、家乡注册应答 BA、密钥信息 $\{\text{Key\_info}\}^*$、AAAH 的数字签名 $\{\text{Signature}_{\text{H}}\}$ 以及 HAL 或 MPA。

$$\text{MACA\_Rep} = \{\text{BA}\}[\text{HAL} \mid \text{MPA}]\{\text{Key\_info}\}^* \{\text{Signature}_{\text{H}}\}$$

(6)MACA_Rep 消息经 AAAF 服务器转发到达 AP 后，AP 会在该消息前附加一个认证结果代码 RC(用 MACA_Rep^* 表示)：$\text{MACA\_Rep}^* = \{\text{RC}\}\{\text{CoA}\}\{\text{BA}\}[\text{HAL} \mid \text{MPA}]\{\text{Key\_info}\}^* \{\text{Signature}_{\text{H}}\}$。如果认证结果成功(RC=1)，则将消息 MACA_Req^* 转发给 MN；如果认证结果失败(RC=0)，那么 AP 就会删除附加信息，只把 RC=0 通知给 MN，这样，访问网络的拓扑信息不会在认证过程中暴露。

(7)MN 从接收到的 MACA_Rep^* 消息中提取出 CoA 以及 HAL 或 MPA，进行相应的 IPv6 地址和网关配置。再用 $\{\text{Signature}_{\text{H}}\}$ 验证 MACA_Req^* 消息的完整性，并用 $\{\text{Key\_info}\}^*$ 生成一个与 AP 之间的动态密钥，表明 MN 与 AP 之间已建立互信关系。

(8)AP 将 MN 新配置的转交地址和 MAC 地址添加到本地的 ACL 中，并将对应 MN 的 T 标志位置 0。

由此完成了访问网络对移动节点的认证授权及移动节点的家乡注册过程。

4　MACA 分析

4.1　性能分析

本文对不同的阶段采用不同的分析方法：地址配置与 DAD 阶段以实际消耗时间计算；MIPv6 的家乡注册阶段和 AAA 认证阶段以计算往返时间的方法进行评价，即以各阶段的消息往返时间作为评价参数。

定义 MN 与 HA 之间以及 MN 与 AAAH 之间的时间距离为 1*RTT*(AAAH 与 AH 之间的消息在同一管理域，它们之间的时延非常小，可以忽略不计)。

根据上述分析方法可知：(1)MN 与 AAAH 之间进行认证的时间记作 T_{auth}，$T_{\text{auth}} = 1RTT$；(2)AP 为 MN 配置一个新的 CoA 并对其执行 DAD 所需的时间记作 T_{coa}；(3)MN 完成家乡注册的时间记作 T_{hr}，$T_{\text{hr}} = 1RTT$。则总时延为

$$D = T_{\text{auth}} + T_{\text{coa}} + T_{\text{hr}} = 2RTT + T_{\text{coa}}$$

在 MACA 方法中，将认证过程、家乡注册和转交地址配置所须交换的报文融合到一次交换过程中完成，则 T_{auth} 与 T_{hr} 合并为一个 *RTT*。为加速地址分配过程的执行并实现有状态地址自动配置(不需要 DAD 操作)，可以在 DHCP 服务器中内置 AP 模块，这样 T_{coa} 可以忽略不计，总时延 $D = 1RTT$。

MACA 引入的加密、解密和数字签名需要一定的处理时间，这些时间开销与所选用算法的复杂度相关。但总体上，算法处理时间与报文交换时间相比可以忽略不计。

综上所述，MACA 方法总的时间代价最终缩小为一个 *RTT*。因此，MIPv6 的切换性能有了较大提高。

4.2 安全性分析

(1)提高了接入网络的安全性。在认证完成前，MN 在新链路上无法配置新的转交地址，更不知道当前网关的 IP 地址，甚至可能没有本地地址或者家乡代理地址。这就极大地提高了访问网络的安全性，防止在未授权的情况下暴露接入网络的拓扑信息。

(2)有效地防止了数据包被篡改和重放攻击。在认证初始化阶段，AP 会给 MN 分发一个 LC，用来防止 MN 重复请求认证，即实现了防重放攻击。每个 AAA 服务器都需要维护一个网络状态表(Network Status Table, NST)，以保证了解管理域内以及相邻管理域的网络状态。AAAH 通过核对 NST，验证 AP 所在网络与其附加的 MN 新转交地址是否一致。

当 MN 需要 MACA 认证时，交换的认证信息 $\{\text{Auth\_info}\}^*$ 和 $\{\text{Key\_info}\}^*$ 都是被加密的，可以防止信息被中间人窃听。并且 MACA_Req 消息由 MN 的数字签名 $\{\text{Signature}_{\text{MN}}\}$ 保护，能够防止中间人在 MN 到 AAAH 的路径上恶意篡改 MACA_Req 消息。最后 AAAH 在返回的消息中加上数字签名 $\{\text{Signature}_{\text{H}}\}$，也可以防止被中间人篡改。

(3)避免了 MN 暴露位置信息。在无状态地址自动配置的过程中，一般接口地址是根据 MAC 地址计算出的，因此，与 MN 进行直接通信的 CN 可以根据 CoA 中的接口地址得到 MN 的 MAC。MAC 地址的全球唯一性会导致 MN 暴露其位置信息。MACA 方法采用有状态地址自动配置，在为 MN 指定 CoA 的同时使 MN 免于暴露位置信息。

当然 MACA 方法也存在一定的安全脆弱性。在访问网络完成对 MN 的认证之前，就预先执行地址分配，为 MN 分配一个 CoA。当采用有状态的 DHCP 分配方式时，攻击者可以大量冒充 MN 请求 AP 进行认证，在这种情况下导致 DHCP 服务器中的地址池被耗尽，最终引发服务器的拒绝服务。

5 结束语

本文以 AAA 消息搭载 MIPv6 信令的方法来减少消息的往返次数，降低总的切换时延。在无线网络环境中对未经认证的移动节点提供 IP 层的访问权限存在着一些安全隐患，本文针对该问题提出了一种基于认证的 MIPv6 地址自动配置方法，在 MIPv6 切换普遍发生的网络环境中，将 AAA 认证过程与 MIPv6 家乡注册相融合，使得 AAA 认证、MIPv6 家乡注册和地址配置在一个 *RTT* 内完成。该方法不仅消除了计算 CoA 和执行 DAD 的时间开销，缩短了 MIPv6 切换过程中地址配置和家乡注册所消耗的时间，而且提高了切换性能，有效地增强了网络的安全性。但是，MACA 方法可能引发恶意移动节点对 DHCP 服务器的拒绝服务攻击。

参考文献

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

[2] Faccin S M, Le Patil B. Diameter Mobile IPv6 Application[Z]. (2004-11-20). www.draft-le-aaa-diameter-mobileipv6-04.txt.

[3] 鲁士文. 下一代因特网的移动支持技术[M]. 北京: 清华大学出版社, 2007.

[4] Arkko J, Devarapalli V, Dupont F. Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents[S]. RFC 3776, 2004.

（上接第 98 页）

UAV 计算能力的要求。选用何种组织模型、子系统规模的数量与体积等都取决于具体的任务特性。

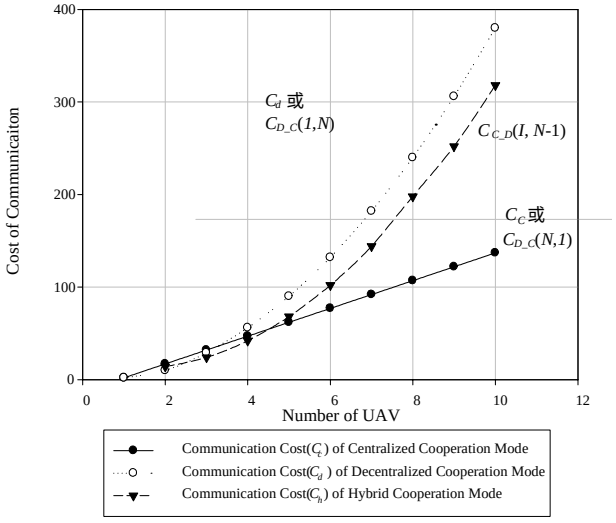

图 6 样不同协作模式中的通信成本

5 结束语

网络组织模型是多 UAV 系统实现高效、可靠组织与管理的关键，这对于大规模 UAV 系统更是如此。本文研究并探讨了几种新的分级混合组织模型以及具有自适应能力的动态组织模型，对于进一步研究 MUAVs 的动态可变结构协作控制、任务规划与协同等机制具有重要意义。

参考文献

[1] Rabbath C A, Gagnon E, Lauzon M. On the Cooperative Control of Multiple Unmanned Aerial Vehicles[J]. IEEE Canadian Review. 2004, 46(1): 15-19.

[2] McDowell, Smith. R. Agent-based Hierarchical Architecture for Autonomous Control of Lethal Unmanned Vehicles[J]. AFRL Technology Horizons. 2002, 3(2): 33-35.

[3] Gaudiano P, Shargel B, Bonabeau E, et al. Swarm Intelligence: A New C2 Paradigm with an Application to Control of Swarms of UAVs[C]//Proc. of the 8th ICCRTS Command and Control Research and Technology Symposium. Washington, D. C., USA: [s. n.], 2003.

[4] Chalmers R, Scheidt D, Neighoff T, et al. Cooperating Unmanned Vehicles[C]//Proc. of the 1st Intelligent Systems Technical Conference. Chicago, USA: [s. n.], 2004.

[5] Zelinski S, Koo T J, Sastry S. Hybrid System Design for Formations of Autonomous Vehicles[C]//Proc. of IEEE Conference on Decision and Control. Hawaii, USA: [s. n.], 2003-11.