# 基于本地安全关联的移动网络接入认证机制*

陈 龙, 汤红波, 葛国栋, 杨 森
(国家数字交换系统工程技术研究中心, 郑州 450002)

**摘 要**: 为减少网络移动中身份认证对性能的影响,提出了一种基于本地安全关联的接入认证机制。该机制通过认证消息携带地址注册信息,整合认证和绑定更新过程,采用本地移动性管理策略,通过建立本地安全关联,实现了域内切换流程本地化,保护了地址注册信息,避免了隧道嵌套。性能分析表明,该机制在实现双向认证的同时能够抵抗重放等多种攻击,相比其他方案,该机制减小了计算开销,缩短了切换时延。

**关键词**: 网络移动性; 认证、授权、计费; 本地认证; 快速切换
**中图分类号**: TP393 **文献标志码**: A **文章编号**: 1001-3695(2012)05-1896-05
doi:10.3969/j.issn.1001-3695.2012.05.079

# Authentication mechanism for network mobility based on local security associations

CHEN Long, TANG Hong-bo, GE Guo-dong, YANG Sen
(*National Digital Switching System Engineering & Technological Research Center, Zhengzhou* 450002, *China*)

**Abstract**: In order to reduce the impact of identity authentication on performance of network mobility, this paper introduced an authentication mechanism. In the mechanism, integrated the authentication and binding update procedures by adding address registration information into authentication messages. With the help of local mobility management strategy and local security associations, the mechanism localized the message flow of the intra-domain handoff, protected the address registration information and eliminated the tunnel-in-tunnel problem. Analysis shows that, the mechanism not only implements the mutual authentication but also resists various attacks such as modified attack. The proposed solution outperforms the counterparts in terms of the computation cost and handoff latency.

**Key words**: network mobility(NEMO); authentication、authorization、accounting(AAA); local authentication; fast handoff

随着移动自组织网络、无线传感器网络和移动热点等技术的发展,越来越多的无线设备形成一个相对稳定的整体进行移动,如部署在汽车、火车、飞机等交通工具上的车载网络,由人体周围无线设备组成的个域网络等。上述应用需求的出现使得 IP 的移动性不仅需要支持单个终端,更需要支持网络移动性(NEMO)。为此,IETF 提出了 NEMO 基本支持协议(NEMO basic support protocol,NBSP)[1]。

为实际部署运营 NEMO,认证、授权、计费(AAA)技术必不可少。目前结合移动 IPv6 的 AAA 技术,设计了若干针对 NEMO 的解决方案[2~5],但是,认证过程产生的开销和时延影响了 NEMO 性能。本文提出了基于本地移动性管理的 NEMO AAA 网络架构,设计了一种基于本地安全关联的认证机制(authentication mechanism based on local security associations,AMLSA)。该机制具有以下主要优点:a)较高的安全性,在实现双向认证的同时保护了地址注册信息的真实性和完整性,有效地提升了 NEMO 的安全性;b)较低的切换时延,域内切换过程能够在本地执行,无须家乡网络参与,改善了 NEMO 的切换性能;c)较小的计算开销,采用对称密钥加解密,计算复杂度低,适用于计算能力较弱的 NEMO 环境;d)较少的隧道封装,在认证过程中采集路径信息,避免了数据包被两层封装。

## 1 基于本地移动性管理的 NEMO AAA 网络

切换流程的本地化是减少切换时延的有效手段,涉及身份认证和地址注册两个方面。为实现域内切换地址注册过程本地化,提出基于本地移动性管理的 NEMO AAA 网络架构。

NEMO 内的节点称为移动网络节点(mobile network node,MNN),MNN 由本地固定节点、本地移动节点、访问移动节点(visiting mobile node,VMN)组成,即移动路由器(mobile router,MR)可以为其他域中的节点服务。因此,NEMO 中存在着 MR 对 MNN 的鉴别和信任问题,由于本地节点可以与 MR 预先配置信任关系,身份认证方式相对简单。下面主要讨论 VMN。

### 1.1 本地移动性管理策略

按照 NBSP 协议,当 NEMO 移动到外地链路时,MR 根据外地网络地址前缀获取或配置转交地址(care of address,CoA),向其家乡代理(home agent,HA)发送绑定更新(binding update,BU)消息注册 CoA,HA 绑定 MR 的家乡地址(home address,HoA)和 CoA。HA 与 MR 之间建立双向隧道,保证了 HoA 的全局可达性。

借鉴层次移动 IPv6 的思想[6],引入移动锚点(mobility anchor point,MAP)负责管理域内所有 MR 和 VMN 的位置更新和

**收稿日期**: 2011-10-09; **修回日期**: 2011-11-16 **基金项目**: 国家科技重大专项资助项目(2009ZX03004-002)

**作者简介**: 陈龙(1988-),男,山东济宁人,硕士研究生,主要研究方向为可移动网络、移动通信(zcyzcl@yahoo.com.cn);汤红波(1968-),男,教授,主要研究方向为可移动网络、移动通信;葛国栋(1985-),男,博士研究生,主要研究方向为可移动网络、移动通信;杨森(1985-),男,助教,硕士,主要研究方向为移动通信.

数据包转发,如图 1 所示。为描述方便,将 MR 和 VMN 统称为移动节点(mobile node,MN)。MAP 将 MN 的 CoA 记为本地转交地址(local CoA,LCoA);当 MN 初次进入某个域中时,MAP 为它们额外分配一个区域转交地址(regional CoA,RCoA),并代替 MN 向 HA 注册 RCoA。当 MN 在域内移动时,RCoA 保持不变,通过更新 LCoA 完成位置管理。VMN 是具有移动能力的节点,其 LCoA 是根据 MR 网络地址前缀配置的,不能标志当前 VMN 的正确拓扑位置,MAP 使用源路由转发以 VMN LCoA 为目的地址的数据包。

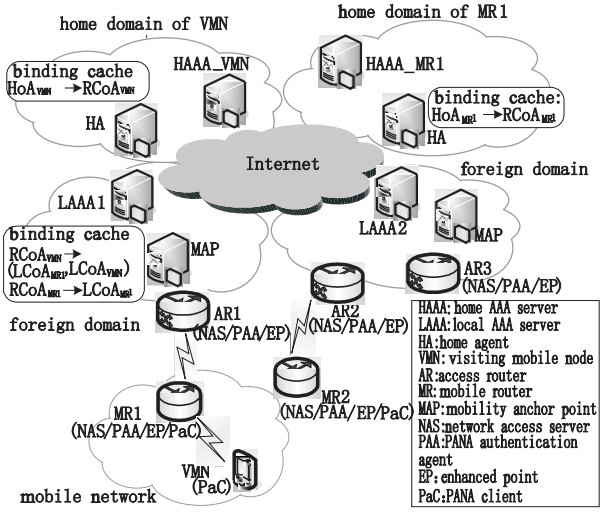



**图1　基于本地移动性管理的NEMO AAA网络**

### 1.2　认证协议与信任模型

在该架构中,用户和服务提供者之间的身份认证采用 PANA(protocol for carrying authentication for network access)协议[7],网络接入服务器(network access server,NAS)与 AAA 服务器之间交互采用 Diameter 协议[8]。PANA 由 PANA 客户端(PANA client,PaC)、PANA 认证代理(PANA authentication agent,PAA)、增强点(enforcement point,EP)、认证服务器(authentication server,AS)等四个功能实体组成,如图 2 所示。MR 和接入路由器(access router,AR)作为 NAS,部署有 PAA、EP,EP 使用加密或者非加密的过滤器对数据包进行选择,实现接入控制功能。

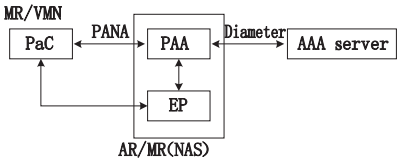



**图2　PANA框架在NEMO中的应用**

基于本地移动性管理的 NEMO AAA 网络信任模型如图 3 所示。AAA 服务器之间、AAA 服务器与域内的接入路由器、MAP 和 HA 之间存在预配置的安全关联(pre-established security associations,PSA)。MN 与其 HAAA 之间存在的 PSA 是身份认证的基础,使得 MN 能够与 LAAA 建立本地安全关联(local SAs,LSA),并与上层路由器建立移动安全关联(mobility SAs,MSA)。

## 2　基于本地安全关联的认证机制

文献[2]实现了对 MR 的本地认证,降低了切换时延,但接入权限容易被伪造,缺乏对 VMN 的支持。文献[5]统一了 NEMO 的身份认证和移动注册过程,减少了信令数量和认证时延,但是切换过程需要与家乡网络交互,时延依然较大,且该方案没有给出具体的认证方法。在整合上述两种思路的基础上加以改进,MN 第一次进入某个域时,与 LAAA 建立起 LSA,MAP 建立 RCoA 和 LCoA 的绑定关系;之后当 MN 在域内移动时,切换过程能够在本地执行,无须家乡网络参与。

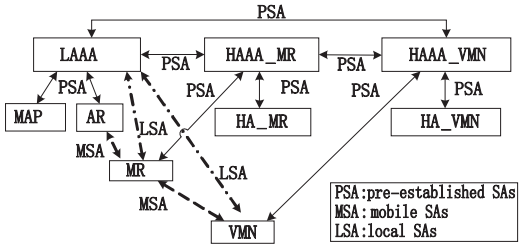



**图3　基于本地移动性管理的NEMO AAA网络信任模型**

### 2.1　认证结构

假定 MN 用全球唯一网络访问标志符(network access identifier,NAI)来标志身份,每个域拥有唯一的域名;AAA 服务器与 NAS 间信任关系通过 Diameter 协议维护,NAS 及其 AAA 服务器之间的链路是安全的;AAA 服务器拥有 MN 的配置文件,这些配置文件包含 MN 拥有的接入权限和服务能力;AAA 服务器与 MN 共享一个长期密钥 $K_{AAA}$,并假设该长期密钥不会被第三方获知;路由器通告消息或其他二层消息含有域名信息,MR 同时通告家乡网络的域名和当前服务网络域名,MN 在检测到切换时可以据此判断当前是域内切换还是域间切换。

### 2.2　域间切换认证过程

#### 2.2.1　MR 域间切换认证过程

当 NEMO 进入一个新的服务域时,MR 发起域间切换认证过程。MR 作为 PaC 向拥有 NAS 功能的 AR 请求接入。MR 域间切换认证过程的信息流如图 4 所示。

1)MR 检测到切换后,发出包含 $M_1$、$NAI_{MR}$、RPI、BU 以及域间切换标志的服务请求消息(AReq)到服务提供者 AR。其中

$$M_1 = E_{K_{AAA}}(R_1) \parallel H(R_1 \parallel NAI_{MR} \parallel RPI \parallel BU) \qquad (1)$$

其中:$E_K(\ )$是使用密钥 $K$ 的加密函数;$R_1$ 是 MR 生成的随机数;RPI 是重放保护指示(replay protection indicator);$H(\ )$是单向 hash 函数(如 SHA-512[9]);BU 为绑定更新消息,包含 MR 的 LCoA;RPI 为时间戳或序列号。

2)AR 收到 AReq 消息后,检查 BU 消息中的 CoA 是否合法,并将其转换为 Diameter 协议中的认证请求(ARR)消息,发送到 LAAA。

3)LAAA 接收到 ARR 消息后,将 BU、$NAI_{MR}$、域间切换认证标志转发至 MAP。

4)MAP 将 BU 中的 CoA 存储为 MR 的 LCoA,为 MR 分配一个 RCoA,然后以 RCoA 为 CoA 生成 $BU_{MAP}$ 消息,将 $BU_{MAP}$ 和对 BU 的响应 BA 一起发回至 LAAA,建立 $NAI_{MR}$、RCoA 与 LCoA 三者的对应关系。

5)LAAA 将 $BU_{MAP}$ 添加到 2)中的 ARR 消息,向 MR 的 HAAA 转发该消息。

6)HAAA 使用 $K_{AAA}$ 解密 $M_1$,比较 $H(R_1 \parallel NAI_{MR} \parallel RPI \parallel BU)$是否与消息中的值一致。如果一致,MR 就被成功认证。

之后,HAAA 转发 $BU_{MAP}$ 至 HA。

7)HA 收到 $BU_{MAP}$ 后按照 NBSP 协议处理。绑定 RCoA 与 MR 的网络前缀,向 HAAA 回送 $BA_{MAP}$。

8)HAAA 生成 MR 与 LAAA 之间的共享密钥 $K_L$:

$$K_L = H(R_1 \parallel \mathrm{NAI_{MR}} \parallel D_L) \tag{2}$$

其中:$D_L$ 为 LAAA 所在网络的域名,$K_L$ 用于建立 LSA。式(2)表明了 LAAA 可以协助 MR 认证 VMN 身份的授权方法。HAAA 向 LAAA 发送包含 $M_2$、$K_L$、$S_{MR}$、$BA_{MAP}$ 的认证应答(ARA)消息,其中:

$$M_2 = E_{K_{AAA}}(R_1 \parallel S_{MR}) \parallel H(R_1 \parallel S_{MR}) \tag{3}$$

$S_{MR}$ 指明了与 MR 存在服务关系的域名列表,以及 MR 的接入权限和服务能力。

9)LAAA 将 $BA_{MAP}$ 转发到 MAP,通知 MAP 认证成功。MAP 开始为 MR 提供数据转发服务。

10)LAAA 存储 $S_{MR}$,根据 $S_{MR}$ 和 AR 的服务能力,鉴权得到 $S_{MR\text{-}L}$,生成随机数 $R_2$ 以及 AR 与 MR 的会话密钥 $K_S$。

$$K_S = H(R_2 \parallel \mathrm{NAI_{MR}} \parallel \mathrm{NAI_{AR}}) \tag{4}$$

将包含 $M_2$、$M_3$、$K_S$、$S_{MR\text{-}L}$、BA 的 ARA 消息发送到 AR,通知 AR 认证结果,其中:

$$M_3 = E_{K_L}(R_2 \parallel S_{MR\text{-}L} \parallel \mathrm{NAI_{AR}}) \parallel H(R_2 \parallel S_{MR\text{-}L} \parallel \mathrm{NAI_{AR}} \parallel BA) \tag{5}$$

11)AR 接收到 ARA 消息后,获知 MR 已被认证。AR 发出包含 $M_2$、$M_3$ 的认证响应(ARep)消息,通知 MR 认证结果。MR 检查 $R_1$ 和消息的完整性,计算 $K_L$、$K_S$。MR 利用 $K_L$ 建立与 LAAA 之间的 Diameter 会话,从而 LAAA 可以协助 MR 认证 VMN 身份。

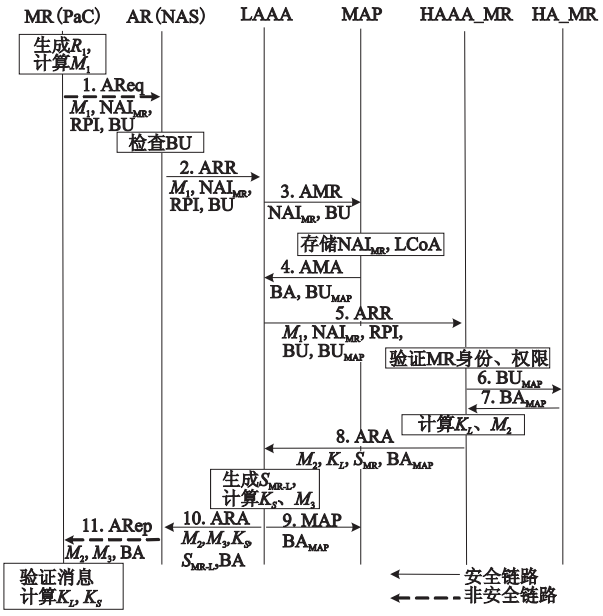



图4 MR域间切换认证过程

### 2.2.2 VMN 域间切换认证过程

VMN 作为 PaC 向拥有 NAS 功能的 MR 请求接入 NEMO,如果这是在该域中的首次认证,则执行域间切换认证过程。认证过程与 MR 不同的部分作如下说明:

a)MR 收到 AReq 消息后,将 ARR 消息直接转发至 LAAA,而非 HAAA_MR。

b)在 LAAA 发往 MAP 的"3. AMR"消息中增加 $NAI_{MR}$。

c)MAP 将 BU 中的 CoA 存储为 VMN 的 LCoA,为 VMN 预分配 RCoA,根据 $NAI_{MR}$ 建立经过 $LCoA_{MR}$ 到 $LCoA_{VMN}$ 的路径(图 1)。

d)LAAA 获知 VMN 身份被 HAAA 验证后,根据 $S_{VMN}$ 和存储的 $S_{MR}$ 鉴权得到 $S_{VMN\text{-}L}$,并存储 $S_{VMN}$。

## 2.3 域内切换认证过程

### 2.3.1 MR 域内切换认证过程

当 MEMO 在域内整体切换时,MR 执行域内切换认证过程,信息流如图 5 所示。

1)MR 发出包含 $M_1$、$NAI_{MR}$、RPI、BU 以及域内切换标志的 AReq 消息,其中:

$$M_1 = E_{K_L}(R_1) \parallel H(R_1 \parallel \mathrm{NAI_{MR}} \parallel \mathrm{RPI} \parallel \mathrm{BU}) \tag{6}$$

2)同 2.2.1 节中的第 2)步。

3)LAAA 接收到 ARR 消息后,使用 $K_L$ 解密 $M_1$,认证 MR 身份。之后,LAAA 将 BU、$NAI_{MR}$、本地更新标志转发至 MAP。

4)MAP 根据 $NAI_{MR}$ 使用 BU 中的 CoA 更新 MR 的 LCoA 以及 MR 下 VMN 的路径,完成 NEMO 拓扑位置的整体更新,之后 MAP 回送 BA。

5)LAAA 根据存储的 $S_{MR}$ 和 AR 的服务能力鉴权得到 $S_{MR\text{-}L}$,生成 AR 与 MR 的会话密钥 $K_S$。

$$K_S = H(R_1 \parallel \mathrm{NAI_{MR}} \parallel \mathrm{NAI_{AR}}) \tag{7}$$

将包含 $M_2$ 和 $K_S$ 的 ARA 消息发送到 AR,通知 AR 认证结果。其中:

$$M_2 = E_{K_L}(R_1 \parallel S_{MR\text{-}L} \parallel \mathrm{NAI_{AR}}) \parallel H(R_1 \parallel S_{MR\text{-}L} \parallel \mathrm{NAI_{AR}} \parallel BA) \tag{8}$$

6)AR 接收到 ARA 消息后,获知 MR 已被认证,授权 MR 接入。AR 发出包含等参数的 ARep 消息,通知 MR 认证结果。MR 检查 $R_1$ 和消息的完整性,计算 $K_S$。

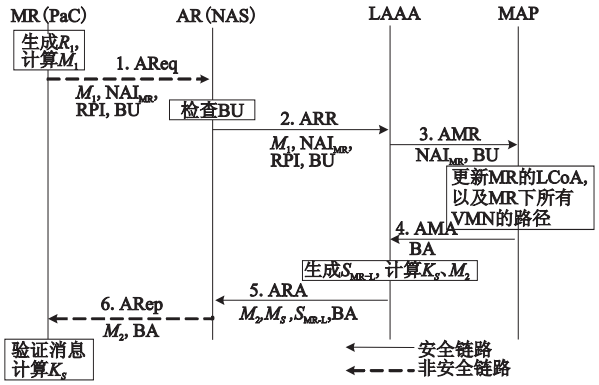



图5 MR域内切换认证过程

### 2.3.2 VMN 域内切换认证过程

VMN 的域内切换认证过程与 MR 类似,不同的部分作如下说明:

a)MAP 收到"3. AMR"消息后,根据 $NAI_{MR}$、$NAI_{VMN}$、BU 更新到 VMN 的路径信息。

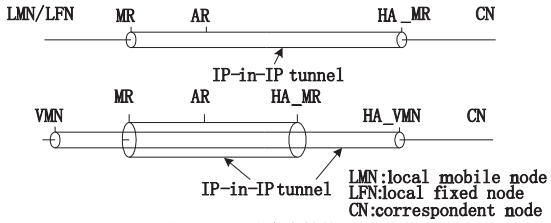
b)LAAA 依靠 LSA 验证 VMN 身份后,根据存储的 $S_{VMN}$ 和 $S_{MR}$ 鉴权得到 $S_{VMN\text{-}L}$。

## 2.4 数据传输机制

数据包传输过程如图 6(b)所示。按照上述认证过程,HA 建立了 HoA 和 RCoA 的绑定关系,MAP 建立了 LCoA 和 RCoA 的绑定关系。MAP 与 HA 之间建立双向隧道,MAP 与 MN 建立双向隧道。以 MN 的 HoA 为目的地址的数据包被 HA 封装,

转发至 RCoA。MAP 解封装,并隧道至 LCoA。由于 VMN 的 LCoA 被直接路由,MAP 对以 VMN LCoA 为目的地址的数据包执行源路由。

反方向的数据包被 MN 封装后,源地址为 LCoA,目的地址为 HA,MAP 接收到数据包后,解封装,并以对应的 RCoA 为源地址,目的地址不变,重新封装并转发数据包。为确保 MAP 可以接收到以 HA 地址为目的的数据包,MR 和 AR 都将目的地址不在本子网内的数据包向 MAP 方向转发。由图 6 可以看出,AMLSA 与 NBSP 相比,VMN 数据包不需要两层嵌套封装,且不必通过 HA_MR 转发。




(a)NEMO基本支持协议　(b)基于本地安全关联的认证机制

**图6　数据包传输过程**

## 3　性能分析

### 3.1　安全性能

下面分析 AMLSA 拥有的安全特性。

1)双向认证　任何第三方都无法获得密钥 $K_{AAA}$,只有 MN 和 HAAA 能够解密 $M_1$ 和 $M_2$,因此 MN 和 HAAA 能够相互认证。进而通过 HAAA 与 LAAA 之间的 PSA,MN 与访问网络之间可以完成双向认证。

2)抗窜改攻击　由于 $H(\ )$ 函数具有单向性,给出值 $x$,容易计算出 $H(x)$,而给出 $H(x)$ 很难计算出 $x$,MN 和 HAAA 通过检查 $M_1$、$M_2$、$M_3$ 中的 $H(\ )$ 函数值,可以检测出消息是否被窜改。

3)抗重放攻击　认证消息中 RPI 仅能使用一次,攻击者使用合适的 RPI 无法得到合法的 $H(\ )$ 函数值。

4)避免密钥暴露　不在不安全的链路上传递密钥,防止密钥被窃听者截获,且 $K_{AAA}$ 密钥仅在首次进入域内时使用,被破解的风险较低。

5)会话密钥生成　能够生成会话密钥,可以用于保护用户数据和接入控制的实施。

6)保护地址注册消息　AAA 服务器通过检查 $H(\ )$ 函数值验证 BU,在认证 MN 身份的同时保证了 BU 的真实性和完整性。

7)验证接入权限　接入权限得到 AAA 服务器验证,防止用户伪造权限。初始认证过程中,MR 的服务权限和 VMN 的接入权限加载到了 LAAA,LAAA 可以在代替 HAAA 完成接入权限的授权。

表 1 给出了 AMLSA 与 LMAM[2] 安全特征的比较。从表中可以看出,AMLSA 在保护地址注册消息、验证接入权限方面优于 LMAM。文献[9]指出 NEMO 大多数安全威胁来源于未经保护的地址注册消息,因此 AMLSA 在一定程度上提升了 NEMO 的安全性。

表 1　安全特征比较

| 比较项 | AMLSA | LMAM |
|---|---|---|
| 双向认证 | 是 | 是 |
| 抗窜改攻击 | 是 | 是 |
| 抗重放攻击 | 是 | 是 |
| 避免密钥暴露 | 是 | 是 |
| 会话密钥生成 | 是 | 是 |
| 保护地址注册消息 | 是 | 否 |
| 验证接入权限 | 是 | 否 |

### 3.2　计算开销

定义计算开销为每次认证过程中所有实体的计算总开销。相关参数定义如表 2 所示。

表 2　计算开销相关符号定义

| 符号 | 意义 |
|---|---|
| $C_h$ | 计算一次单向 hash 函数的开销 |
| $C_{\text{sym}}$ | 使用对称密钥加密或解密一次的开销 |
| $C_{\text{rand}}$ | 生成一次随机数的开销 |
| $C_{\text{asym}}$ | 使用非对称密钥加密或解密一次的开销 |

AMLSA 机制域间切换认证过程计算了 10 次单向 hash 函数,使用对称密钥加解密六次,两次生成随机数,该过程的计算开销为

$$C_{\text{AMLSA-I}} = 10C_h + 6C_{\text{sym}} + 2C_{\text{rand}} \tag{9}$$

AMLSA 机制域内切换认证过程的计算开销为

$$C_{\text{AMLSA-H}} = 8C_h + 4C_{\text{sym}} + 2C_{\text{rand}} \tag{10}$$

LMAM、LR-AKE[4]、LIM[3] 机制的计算开销分别为

$$C_{\text{LMAM}} = 8C_h + 6C_{\text{sym}} + 2C_{\text{rand}} \tag{11}$$

$$C_{\text{LR-AKA}} = 12C_h + 5C_{\text{asym}} + 2C_{\text{rand}} \tag{12}$$

$$C_{\text{LIM}} = 8C_h + 2C_{\text{asym}} \tag{13}$$

其中:$C_{\text{asym}}$ 是 $C_{\text{sym}}$ 的 100 ~ 1000 倍[2],则从式(9) ~ (13)可以看出,LR-AKE 和 LIM 机制计算开销远大于 AMLSA 和 LMAM。AMLSA 域间切换认证过程的计算开销比 LMAM 稍大,而域内切换认证过程的计算开销较小。

### 3.3　切换时延

定义切换时延为 MN 发出认证请求到完成认证的时间间隔。

AMLSA 机制下 MR 域间切换时延为

$$T_{\text{MR-I}} = 2t_1 + 6t_0 + 2t_{\text{LR}} + t_{\text{proc}} \tag{14}$$

VMN 域间切换时延为

$$T_{\text{VMN-I}} = 4t_1 + 6t_0 + 2t_{\text{LV}} + t_{\text{proc}} \tag{15}$$

MR 域内切换时延为

$$T_{\text{MR-H}} = 2t_1 + 4t_0 + t_{\text{proc}} \tag{16}$$

VMN 域内切换时延为

$$T_{\text{VMN-H}} = 4t_1 + 4t_0 + t_{\text{proc}} \tag{17}$$

其中:$t_{\text{proc}}$ 为认证处理时延,其他参数为传输时延,如图 7 所示。

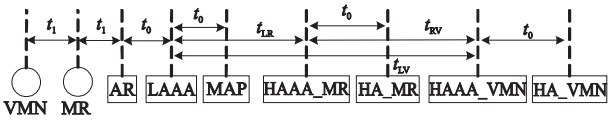



**图7　用于分析切换时延的网络模型**

使用 NS-2 进行实验仿真。网络模型如图 7 所示。参数设置如下[2,3]:传输时延服从指数分布,无线链路单跳时延 $t_1$ 均值为 50 ms,有线链路单跳时延 $t_0$ 均值为 10 ms。MN 在路由器

内的驻留时间服从 Gamma 分布,LAAA 与 MAP 之间、LAAA 与 AR 之间、HAAA 与 HA 之间的距离设为 1 跳。结果是十次运行后得到的平均值。记 LAAA 与 HAAA_MR 之间的距离为 $d_{LR}$,LAAA 与 HAAA_VMN 之间的距离为 $d_{LV}$,HAAA_MR 与 HAAA_VMN 之间的距离为 $d_{RV}$。

图 8 给出了 AMLSA、LE-HMIPv6[2]、DNA[5]、LR-AKE、LIM 五种机制下 MR 的切换时延。其中:AMLSA-H 表示域内切换,AMLSA-I 表示域间切换,虚线表示的是用数学计算得出的切换时延。实验仿真得出的结果和数学计算得出的数据基本一致。AMLSA 域内切换时延不随 $d_{LR}$ 的增加而增大,但比 LE-HMIPv6 稍大,需要说明的是 LE-HMIPv6 要求数据链路层提供切换触发子以实现预切换,而 AMLSA 不需要。

图 9 给出了 AMLSA、DNA、LR-AKE、LIM 四种机制下 VMN 的切换时延(LE-HMIPv6 不支持 VMN 的切换)。其中 AMLSA 机制下 VMN 的切换时延最小,且不随 $d_{LV}$ 和 $d_{RV}$ 增加而增大。在 MR 数量较多的环境下,VMN 在 MR 之间切换的次数较多,AMLSA 的性能优势更为明显。

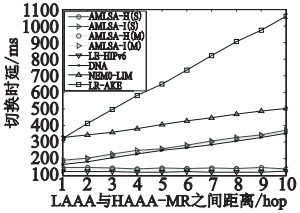



图8 MR切换时延随$d_{LR}$的变化

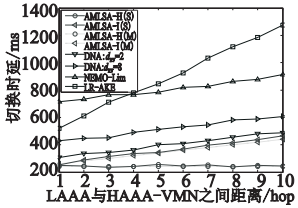



图9 VMN切换时延随$d_{LV}$的变化

## 4 结束语

本文提出了基于本地移动性管理的 NEMO AAA 网络,设计了一种基于本地安全关联的 NEMO 认证机制,给出了网络实体间的交互流程、身份认证以及接入权限的授权方法。该机制整合身份认证和地址注册过程,利用本地移动性管理策略和本地安全关联,实现了 MN 域内切换时认证—注册过程的本地化,避免了 VMN 数据包嵌套封装。性能分析表明,该机制能够实现用户和网络之间的双向认证、抗重放攻击等,保护了地址注册信息,提升了 NEMO 的安全性;与其他方案相比,该机制在计算开销和切换时延方面更优。

**参考文献:**


[1] DEVARAPALLI V, WAKIKAWA R, PETRESCU A, *et al*. RFC 3963, network moblity (NEMO) basic support protocol[S]. [S. l.]: IETF, 2005.

[2] CHUANG M C, LEE J F. A lightweight mutual authentication mechanism for network mobility in IEEE 802.16e wireless networks[J]. Computer Networks, 2011, 55(16): 3796-3809.

[3] LIM H J, KIM M, LEE J H, *et al*. Reducing communication overhead for nested NEMO networks: roaming authentication and access control structure[J]. IEEE Trans on Vehicular Technology, 2011, 60(7): 3408-3423.

[4] FATHI H, SHIN S, KOBARA K. R-AKE-based AAA for network mobility (NEMO) over wireless links[J]. IEEE Journal on Selected Areas in Communications, 2006, 24(9): 1725-1737.

[5] AHN Y, LEE T J, CHOO H, *et al*. DNA Diameter NEMO applications based on binding update integration[C]//Proc of Frontiers of High Performance Computing and Networking. Berlin: Springer-Verlag, 2006: 1-6.

[6] SOLIMAN H, CASTELLUCCIA C, ELMALKI K, *et al*. RFC 5380, hierarchical mobile IPv6 (HMIPv6) mobility management[S]. [S. l.]: IETF, 2008.

[7] JAYARAMAN P, LOPEZ R, OHBA Y, *et al*. RFC 5193, protocol for carrying authentication for network access (PANA) framework [S]. [S. l.]: IETF, 2008.

[8] KORHONEN J, BOURNELLE J, TSCHOFENIG H, *et al*. RFC 5447, Diameter mobile IPv6: support for network access server to diameter server interaction[S]. [S. l.]: IETF, 2009.

[9] NIST. Department of Commerce. Federal Information Processing Standard (FIPS), secure hash standard[S]. 2002.

[10] PETRESCU A, OLIVEREAU A, JANNETEAU C, *et al*. Draft-petrescu-nemo-threats-01, threats for basic network mobility support (NEMO threats)[S]. [S. l.]: IETF, 2004.

[11] 葛国栋, 汤红波, 王晓雷. 嵌套移动网络中基于代价函数的自适应路由优化机制[J]. 电子与信息学报, 2011, 33(8): 2018-1022.

[12] 周华春, 张宏科, 秦雅娟. 一种代理移动 IPv6 认证协议[J]. 电子学报, 2008, 36(10): 1873-1880.

[13] 杨君, 郭伟, 刘军. 基于可信区域的移动 IPv6 切换优化[J]. 计算机应用研究, 2010, 27(3): 1106-1109.