一种身份与位置分离环境下基于网络的安全移动性管理协议

唐建强* 刘 颖 周华春 张宏科
(北京交通大学电子信息工程学院 北京 100044)

摘 要：针对身份与位置分离(Locator/Identifier Separation Protocol, LISP)环境下的移动性管理问题，提出一种基于网络的安全移动性管理协议—LISP-SMCP(Secure Mobility Control Protocol)。以接入网为移动管理区域，LISP-SMCP 有效地支持移动节点在区域内切换和区域间切换，并实现本地认证和双向认证。安全性和性能分析结果表明，LISP-SMCP 可以防止中间人、重放和消息篡改等网络攻击，且具有较小的认证时延、切换时延和切换阻塞率。

关键词：身份与位置分离；移动性管理；安全切换；本地认证
中图分类号：TN915.07 **文献标识码**：A **文章编号**：1009-5896(2013)01-0151-08
DOI: 10.3724/SP.J.1146.2012.00782

A Network-based Secure Mobility Control Protocol in Locator/Identifier Separation Networks

Tang Jian-qiang Liu Ying Zhou Hua-chun Zhang Hong-ke
(*School of Electronic and Information Engineering*, *Beijing Jiaotong University*, *Beijing* 100044, *China*)

Abstract: For the mobility issue in Locator/Identifier Separation Protocol (LISP) networks, a network-based Secure Mobility Control Protocol (LISP-SMCP) is proposed. Taking access networks as different mobile domains, LISP SMCP supports mobile nodes intra-domain handoff and inter-domain handoff efficiently, and achieves local authentication and mutual authentication. The security and performance analysis results show that, LISP-SMCP can resist man-in-the-middle attacks, replay attacks and modified attacks. And it outperforms existing schemes in terms of authentication latency, handoff latency and handoff blocking probability.

Key words: Locator/identifier separation; Mobility management; Secure handoff; Local authentication

1 引言

当前互联网面临严重的路由可扩展性问题[1]。为此，互联网工程任务组(IETF)提出了基于网络的未来互联网络体系方案—LISP(Locator/Identifier Separation Protocol)[2]，它将传统 IP 地址的双重属性分离，分别使用终端标识(Endpoint IDentifier, EID)和路由标识(Routing LOCator, RLOC)表示终端身份信息和位置信息。终端的映射信息(EID-to-RLOC)使用映射系统(mapping system)管理。LISP 符合未来互联网在路由可扩展性、移动性和多家乡等方面的要求，是当前最成熟的未来互联网络体系备选方案之一[3]。然而，传统互联网的移动性方案(MIP, MIPv6, PMIPv6, FPMIPv6)不能直接应用在 LISP 网络中，主要原因是这些移动性方案没有考虑路由可扩展性问题和映射信息更新问题。

目前出现了一些 LISP 环境下的移动性管理方案，根据移动范围可以分为区域移动性(localized mobility)，如 LISP-MN-LOCAL[4], MobileID[5], LISP-AR-DMC[6]，和全局移动性(global mobility)管理方案，如 LISP-MN[7], MMILS[8], IM[9]。根据实现方式可以分为基于主机和基于网络的移动性管理方案。基于主机的移动性管理方案，如 LISP-MN 和其改进方案 LISP-MN-LOCAL，需要修改移动节点，违背了 LISP 不修改主机协议的初衷。基于网络的移动性管理方案，如 MobileID, LISP-AR-DMC, MMILS, IM，减少移动节点参与移动性管理，具有较好的切换性能。LISP 环境下的移动性管理方案集中致力于减少移动节点在不同网络移动时的切换时延，并未考虑安全性。当节点移动到新网络时，移动节点需要遵守新网络的接入过程，尤其是需要访问域 AAA 服务器与家乡域 AAA 服务器的交互才能确认移动节点身份，由此可能造成过大的认证时延，从而影响切换时延。

2012-06-21 收到，2012-09-27 改回
国家自然科学基金(61202428, 60903150)，国家 863 计划项目(2011AA010701)，北京市自然科学基金(4122060)和中央高校基本科研业务费专项资金(2012YJS019)资助课题
*通信作者：唐建强 tangjianqiang@bjtu.edu.cn

本文提出一种 LISP 环境下基于网络的安全移动性管理协议(Secure Mobility Control Protocol, LISP-SMCP)。该协议以接入网为移动管理区域，给出接入路由器、隧道路由器与 AAA 服务器的交互过程，移动节点初始安全接入过程，移动节点在区域内和区域间移动安全切换过程。LISP-SMCP 支持移动节点与网络的双向认证；支持移动节点在访问域的本地认证，即访问域 AAA 服务器不需与家乡域 AAA 服务器进行交互，移动节点就可以完成安全切换。该协议可以防止中间人攻击、重放攻击和消息篡改攻击等。此外，给出性能分析模型，与 LISP 环境下的其他移动性管理方案比较结果表明 LISP-SMCP 具有较小的认证时延，切换时延和切换阻塞率。

2 LISP 协议

LISP[2]是一种基于网络的未来互联网体系方案，使核心网与接入网分离来减少接入网路由信息对核心网路由系统的影响，可解决当前网络面临的路由扩展性问题。LISP 的部署不需要对终端进行任何修改，只需将连接接入网与核心网的部分路由器升级为隧道路由器(Tunnel Router, TR)。隧道路由器向映射服务器注册和查询终端的映射信息，根据映射信息完成数据包隧道封装和解封装处理。映射信息由映射系统来存储和维护，已出现一些映射系统方案，例如 LISP-ALT(LISP ALternative Topology)[10]等。为减少映射信息查询时延，隧道路由器在本地映射缓存存储最近使用的映射信息。数据包在核心网中使用路由标识进行寻路转发。LISP 网络中接入网(Access Network, AN)间终端通信过程如图 1 所示。终端 CN(Correspond Node, CN)向终端 MN(Mobile Node, MN)发送普通数据包(步骤 1)，TR_1 向映射服务器(Mapping Server, MS)查询映射信息(步骤 2)，TR_1 在本地映射缓存中缓存 MS 返回的映射信息 (步骤 3)，TR_1 根据映射信息为原始数据包封装一个新的数据包头并转发给 TR_2(步骤 4)，TR_2 剥去数据包外部包头，将原始数据包转发到 MN(步骤 5)。

3 LISP 环境下的安全移动性管理协议

本节给出基于 AAA(Authentication, Authorization, Accounting)模型的 LISP 环境下安全移动性管理协议。本文假定 IEEE 802.21 定义的链路层信息可在 LISP-SMCP 中使用。

3.1 LISP 移动网络拓扑结构

图 2 描述部署 AAA 服务器的 LISP 移动网络拓扑结构，每个接入网内至少有一个 AAA 服务器。

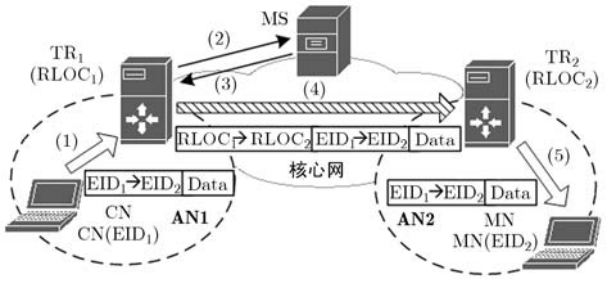

图 1 LISP 结构和终端通信流程示意图

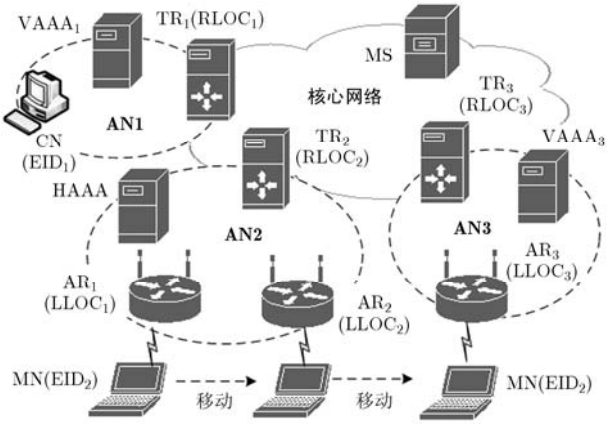

图 2 LISP 移动网络拓扑结构示意图

引入接入路由器(AR, Access Router)作为移动节点的移动接入网关，其地址为本地路由标识(Local LOCator, LLOC)。一个接入网是一个移动管理区域，一个接入路由器控制一个子网，每个接入网可由若干子网组成。接入网内移动节点的数据通过隧道传输，隧道数据包采用本地路由标识寻路转发。隧道路由器作为区域内移动节点的移动锚点，管理并存储区域内移动节点的位置信息(EID-LLOC)。接入网内 AAA 服务器与隧道路由器和接入路由器预先建立安全联盟(security association)。AAA 服务器与接入网内所有接入路由器预先共享相同的组密钥。移动节点与 HAAA(Home AAA)服务器预先协商共享密钥，移动节点在家乡域完成初始安全接入。访问域的 VAAA(Visited AAA)与移动节点的 HAAA 预共享密钥和移动节点的终端标识等信息，否则移动节点不能在访问域完成接入过程。

3.2 移动节点初始安全接入

移动节点在家乡域的初始安全接入过程如图 3 所示，具体过程如下：

(1)MN 发送路由请求(Router Solicitation, RS)消息到 AR_1。

(2)AR_1 返回包含挑战值 CV 的路由通告(Router Advertisement, RA)消息。

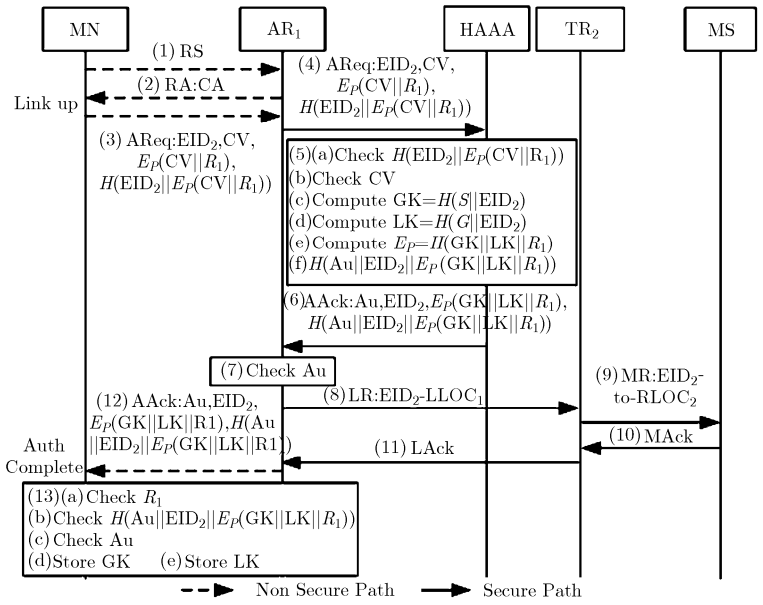

图 3 移动节点初始安全接入过程

(3)MN 向 AR_1 发送接入请求(AReq)消息，内容包括：MN 的终端标识 EID_2，挑战值 CV，使用预共享密钥 P 计算的加密信息 $E_P(CV||R_1)$和哈希值 $H(EID_2||CV||E_P(CV||R_1))$，其中“||”是字符串连接符，$R_1$ 是 MN 生成的随机数，用于防止重放攻击。

(4)AR_1 收到 AReq 消息后，将其发送到 HAAA。

(5)HAAA 首先检查 $H(EID_2||CV||E_P(CV||R_1))$，确认消息的完整性。然后使用共享密钥 P 解密 $E_P(CV||R_1)$得到 CV 和 R_1，并与未加密的 CV 比较。如果两个值相等，则确认 MN 的身份。计算域间切换密钥值 $GK=H(S||EID_2)$和域内切换密钥值 $LK=H(G||EID_2)$，其中 S 是 HAAA 与 VAAA 的预共享密钥，G 是 HAAA 与区域内 AR 共享的组密钥。然后计算 $E_P(GK||LK||R_1)$和 $H(Au||EID_2||E_P(GK||LK||R_1))$，其中 Au 是 MN 的认证成功标志。

(6)HAAA 向 AR_1 发送接入确认(AAck)消息，内容包括认证成功标志 Au, MN 的终端标识 EID_2，加密信息 $E_P(GK||LK||R_1)$和哈希值 $H(Au||EID_2||E_P(GK||LK||R_1))$。

(7)AR_1 检查 Au 标志，确认 MN 认证成功，允许 MN 接入。

(8)AR_1 向 TR_2 发送位置注册(LR)消息，注册 MN 的位置信息 EID_2-$LLOC_1$。

(9)TR_2 向 MS 发送映射注册(MR)消息，注册 MN 的映射信息 EID_2-to-$RLOC_2$。

(10)MS 返回映射注册确认(MAck)消息，确认 MN 映射信息注册完成。

(11)TR_2 向 AR_1 返回位置确认(LAck)消息，确认 MN 位置信息注册完成。

(12)AR_1 将接入确认消息(AAck)发送给 MN。

(13)MN 收到 AAck 消息后，检查哈希值 $H(Au||EID_2||E_P(GK||LK||R_1))$，核对解密得到的 R_1，防止消息篡改攻击和重放攻击，确认网络的真实性，存储 GK 和 LK，完成双向认证。

3.3 移动节点区域内安全移动切换过程

移动节点在区域内切换时，不需要 HAAA 与 MS 的参与。移动节点在域内的安全切换过程如图 4 所示，其中第 1–第 8 步进行移动切换，第 9–第 10 步优化数据传输路径。图 4 与图 3 的不同过程解释如下：

图 4 中，(3)MN 向 AR_2 发送切换请求(HReq)消息，其中 $E_{LK}(CV||R_1)$是用域内切换密钥 LK 计算的加密信息。(4)AR_2 收到 HReq 消息后，检查

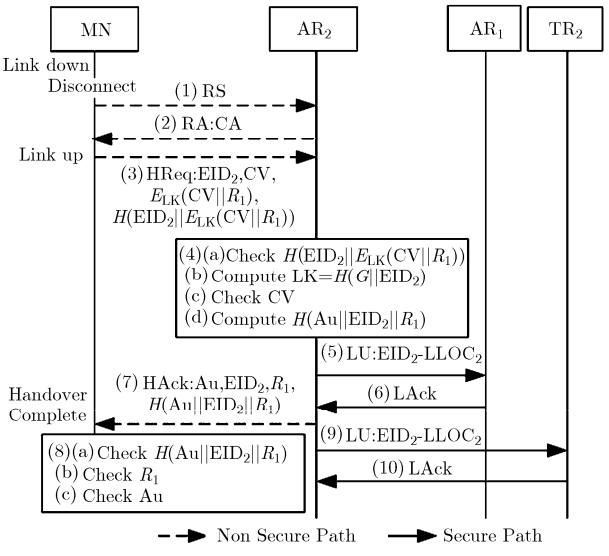

图 4 移动节点区域内安全移动切换过程

$H(\mathrm{EID}_2||\mathrm{CV}\ ||E_{\mathrm{LK}}(\mathrm{CV}||R_1))$，使用预共享组密钥 G 计算 LK= $H(G||\mathrm{EID}_2)$，用 LK 解密得到 CV 并核对 CV 值，确认 MN 的身份。然后计算 $H(\mathrm{Au}||\mathrm{EID}_2||R_1)$。(5)$\mathrm{AR}_2$ 向 AR_1 发送位置更新(LU)消息，更新 AR_1 中 MN 的位置信息为 EID_2-LLOC_2。(9)AR_2 向 TR_2 发送位置更新(LU)消息，优化数据传输路径。

3.4 移动节点区域间安全移动切换过程

移动节点在区域间的安全切换过程中，不需要与 HAAA 交互即可确认移动节点身份。移动节点在区域间的安全切换过程如图 5 所示，其中第 1–第 13 步进行移动切换，第 14–第 17 步优化数据传输路径。图 5 和图 3 的不同过程解释如下：

图中，(3)MN 向 AR_3 发送 HReq 消息，其中 $E_{\mathrm{GK}}(\mathrm{CV}||\ R_1)$是域间切换密钥 GK 计算的加密信息。(5)VAAA 检查 $H(\mathrm{EID}_2||\mathrm{CV}||E_{\mathrm{GK}}(\mathrm{CV}||R_1))$，确认消息的完整性。使用预共享密钥 S 计算 GK=$H(S||\mathrm{EID}_2)$，用 GK 解密得到 CV 并核对 CV 值，确认 MN 的身份。VAAA 使用共享组密钥 G 计算域内切换密钥值 LK=$H(G||\mathrm{EID}_2)$。(9)TR_3 向 TR_2 发送映射更新(MU)消息，更新 MN 的新映射信息 EID_2-to-RLOC_3。(16)TR_3 向通信对端的 TR_1 发送映射更新(MU)消息，优化数据传输路径。

4 安全性分析

表 1 给出了几种移动性管理方案的比较。PMIPv6 只关注于移动性，不能改善路由可扩展性问题。IETF 已经提出扩展 PMIPv6 后支持区域间移动性的方案[11]和移动节点认证的方案[12]。其他的移动性管理方案基于 LISP 设计，支持路由可扩展性，但都未考虑安全性。本文提出的 LISP-SMCP 协议支持区域内和区域间的移动性，并且支持安全性。

表 1 移动性管理方案比较

移动性管理方案	路由可扩展性	修改移动节点	域内移动性	区域间移动性	安全性
PMIPv6	不支持	否	支持	扩展支持	扩展支持
LISP-MN	支持	是	支持	支持	无
MobileID	支持	否	支持	不支持	无
LISP-AR-DMC	支持	否	支持	不支持	无
MMILS	支持	否	支持	支持	无
IM	支持	否	支持	支持	无
LISP-SMCP	支持	否	支持	支持	支持

LISP-SMCP 具有如下安全特性：

(1)双向认证　MN 和网络侧通过加密和解密过程完成挑战值 CV，随机数 R_1 的核对，确认双方拥有相同的密钥(如图 3 的第 5，第 13 步确认共享密钥 P；图 4 中的第 4，第 8 步确认共享密钥 LK；图 5 中的第 5，第 13 步确认共享密钥 GK)，完成身份的双向确认。

(2)防止中间人攻击　MN 与 AR 之间的敏感信息，都加密后传输(如密钥 GK 和 LK，随机数 R_1)，中间人并不能获得敏感信息，可以防止中间人攻击。

(3)防止消息篡改攻击　MN 与 AR 之间传输的消息使用哈希函数 $H(\bullet)$检查其完整性(如图 3 中的第 5，第 13 步；图 4 中的第 4，第 8 步；图 5 中的

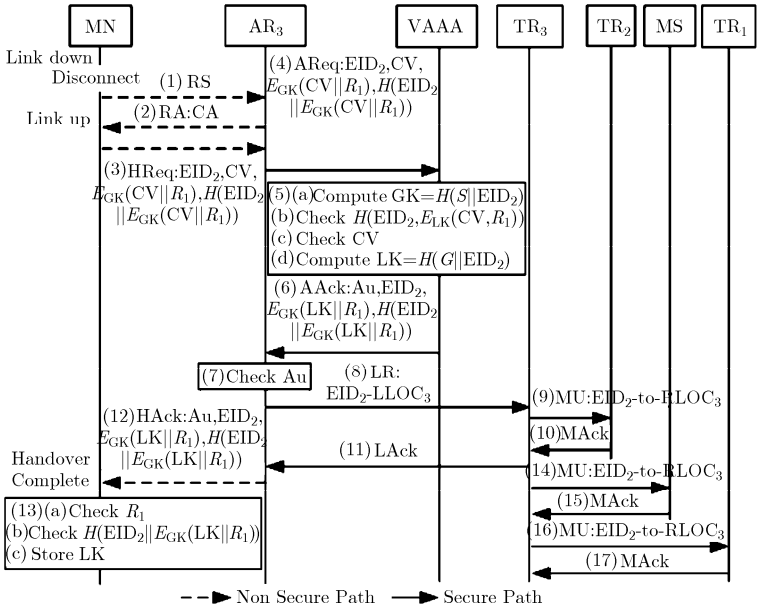

图 5 移动节点区域间安全移动切换过程

第 5, 13 步)，第 3 方对消息的任何篡改都会被发现，可以防止消息篡改攻击。

(4)抗重放攻击　MN 与 AR 之间消息的新鲜性通过 MN 的随机数和 AR 的挑战值来保持(图 3，图 4 和图 5 中的随机数 R_1 和 CV)，攻击者很难事先猜中，因此可以抵抗重放攻击。

(5)本地认证　当 MN 在区域内移动时，只需 AR 的参与(如图 4 中的 AR_2)，即可完成 MN 的认证，不需要与 AAA 服务器交互；当 MN 在区域间移动时，只需访问域内的 AR 和 VAAA 服务器参与(如图 5 中 AR_3 和 VAAA)，即可完成移动节点身份确认，不需要与 HAAA 服务器交互。本地认证可以降低 MN 切换时的认证时延。

(6)切换密钥动态生成　MN 的区域内和区域间切换密钥都通过哈希计算得到(如图 2 中第 5 步和图 3 中第 4 步，LK=$H(G||\text{EID})$, GK=$H(S||\text{EID})$)，且密钥与 MN 的终端标识 EID 绑定，减少了 AAA 服务器或 AR 管理密钥的代价。

5　性能分析

本节给出性能分析模型，分析 LISP-SMCP 协议的认证时延，切换时延和切换阻塞率，并与 LISP-MN-LOCAL, MobileID, LISP-AR-DMC, LISP-MN, MMILS 和 IM 进行比较。

5.1 分析模型

为分析移动性管理方案的性能，给出性能分析模型[5,13]，如图 6 所示。表 2 列出了主要参数的意义。

性能分析模型中，MobileID 的本地映射服务器(Local Mapping-Server, LMS)、MMILS 的代理隧道路由器(Agent Tunnel Router, ATR), IM 的汇聚点(Rendezvous Point, RP)和 LISP-SMCP 的 TR 都处于同一个位置，因为它们都完成相似的功能。对于 LISP-MN-LOCAL，假定 LMS 管理 MN 的映射信息。由于对称加密计算和哈希计算处理时延较低，因此性能分析忽略了消息处理时延、队列时延和映射系统处理时延等。LISP-MN, MobileID, LISP-AR-DMC, MMILS, IM 都没有提及 MN 切换时的安全考虑，为客观比较移动性管理方案的性能，考虑一般情况，认为 MN 在移动切换时，需要向 HAAA 服务器完成认证。即当 MN 在家乡域，则向 HAAA 确认 MN 身份；当 MN 在外地域，则通过外地域的 VAAA 服务器与 HAAA 服务器交互确认 MN 的身份。

5.2 认证时延

认证时延(Authentication Latency, AL)为移动

表 2 参数意义

参数	意义
t_r	相邻 TR 或核心网中路由器间的时延
m	家乡域与访问域的核心网中路由器跳数
t_u	MS 与 TR/RP 之间的时延
t_a	区域内移动代理或路由器(LMS/RP/TR 和 AR/TR)与 AAA 的时延
t_{am}	区域内 LMS/TR/RP 与 AR/TR 之间的数据传输时延
t_n	区域内相邻 AR/TR 之间的时延
t_{ra}	AR/TR 与无线接入点间的时延
t_{mr}	MN 与无线接入点间的时延
t_{tc}	CN 与 c-AR/c-TR 之间的时延
t_{ac}	CN 与 AR/TR 之间的数据传输时延
t_{hc}	CN 与 TR 之间的数据传输时延(即 LISP-MN 域间切换时，MN 与 CN 的时延)
$T_{A\text{-}B}$	消息在节点 A 与 B 间的传输时延

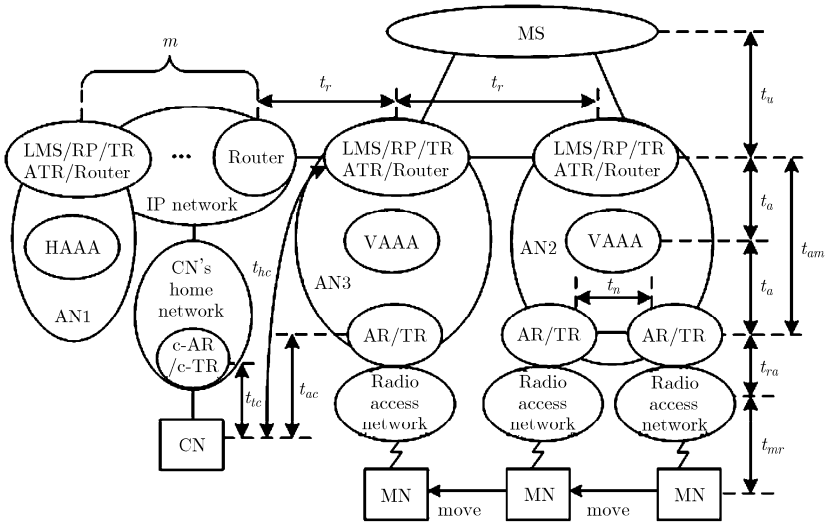

图 6 性能分析模型

节点切换时发出认证请求到完成接入认证的时间间隔。本文分开讨论区域内切换认证时延($\mathrm{AL_{INTRA}}$)和区域间切换认证时延($\mathrm{AL_{INTER}}$)。

对于 LISP-SMCP, MN 在区域内切换时，只需要 AR 的参与就可以完成认证，因此 LISP-SMCP 的区域内切换认证时延为 0, LISP-MN-LOCAL, MobileID, LISP-AR-DMC, MMILS 和 IM 的域内和域间切换认证时延相同。认证时延分别为

$$\begin{aligned}\mathrm{AL}_{\mathrm{INTRA}}^{\mathrm{Other}} &= \mathrm{AL}_{\mathrm{INTER}}^{\mathrm{Other}} = 2T_{\text{AR-VAAA}} + 2T_{\text{VAAA-HAAA}} \\ &= 6t_a + 2(m+2)t_r \end{aligned} \tag{1}$$

$$\mathrm{AL}_{\mathrm{INTRA}}^{\text{LISP-SMCP}} = 0 \tag{2}$$

$$\mathrm{AL}_{\mathrm{INTRA}}^{\text{LISP-SMCP}} = 2T_{\text{AR-VAAA}} = 2t_a \tag{3}$$

5.3 切换时延

切换时延(Handover Latency, HL)为 MN 在移动过程中完成链路层切换到接收到 CN 的数据包的时间间隔。切换时延由移动检测时延(T_{MD})，重复地址检测时延(T_{DAD})，切换认证时延(AL)和位置注册时延(Local Registration Latency, RL)组成。根据文献[14]建议的路由通告消息(Router Advertisement, RA)最大间隔值(MaxRtrAdvInterval, MaxInt)和最小间隔(MinRtrAdvInterval, MinInt)，得到移动检测平均时延为 T_{MD}=(MaxInt+MinInt)/4[13]。根据文献[15]，设定重复地址检测时延为 T_{DAD}=1000 ms。本文分开讨论区域内切换时延($\mathrm{HL_{INTRA}}$)和区域间切换时延($\mathrm{HL_{INTER}}$)。

基于主机的移动性管理方案需要检测 MN 的位置，并分配新的路由标识，切换时延为：$\mathrm{HL}^{(\cdot)}=T_{\mathrm{MD}}+T_{\mathrm{DAD}}+\mathrm{AL}^{(\cdot)}+\mathrm{RL}^{(\cdot)}$，其中$(\cdot)$代表不同移动性管理方案。位置注册时延分别为

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTRA}}^{\text{LISP-MN-LOCAL}} &= 2T_{\text{MN-LMS}} + 2T_{\text{MN-c-TR}} \\ &= 4t_{mr} + 4t_{ra} + 2t_{am} + 2t_{ac} - 2t_{tc} \end{aligned} \tag{4}$$

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTER}}^{\text{LISP-MN}} &= 2T_{\text{MN-MS}} + 2T_{\text{MN-c-TR}} \\ &= 4t_{mr} + 4t_{ra} + 2t_u + 2t_{hc} - 2t_{tc} \end{aligned} \tag{5}$$

基于网络的移动性管理方案切换时延为：$\mathrm{HL}^{(\cdot)}=\mathrm{AL}^{(\cdot)}+\mathrm{RL}^{(\cdot)}$，位置注册时延分别为

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTRA}}^{\text{MobileID}} &= 2T_{\mathrm{TR_{old}\text{-}LMS}} + 2T_{\mathrm{TR_{new}\text{-}LMS}} + T_{\mathrm{TR_{old}\text{-}MN}} \\ &= 4t_{am} + t_n + t_{mr} + t_{ra} \end{aligned} \tag{6}$$

$$\mathrm{RL}_{\mathrm{INTRA}}^{\text{LISP-AR-DMC}} = 3T_{\text{AR-AR}} + T_{\text{AR-MN}} = 3t_n + t_{mr} + t_{ra} \tag{7}$$

$$\mathrm{RL}_{\mathrm{INTRA}}^{\text{MMILS}} = 2T_{\mathrm{TR_{old}\text{-}TR_{new}}} + T_{\mathrm{TR_{old}\text{-}MN}} = 3t_n + t_{mr} + t_{ra} \tag{8}$$

$$\mathrm{RL}_{\mathrm{INTRA}}^{\mathrm{IM}} = 2T_{\text{TR-RP}} + T_{\text{RP-MN}} = 3t_{am} + t_{mr} + t_{ra} \tag{9}$$

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTRA}}^{\text{LISP-SMCP}} &= 2T_{\mathrm{AR_{old}\text{-}AR_{new}}} + T_{\mathrm{AR_{old}\text{-}MN}} \\ &= 3t_n + t_{mr} + t_{ra} \end{aligned} \tag{10}$$

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTER}}^{\text{MMILS}} &= 2T_{\mathrm{TR_{new}\text{-}MS}} + 2T_{\mathrm{TR_{new}\text{-}ATR}} \\ &= 2t_u + 2(m+2)t_r \end{aligned} \tag{11}$$

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTER}}^{\mathrm{IM}} &= 2T_{\mathrm{TR_{new}\text{-}RP_{new}}} + 2T_{\mathrm{RP_{new}\text{-}MS}} + 2T_{\mathrm{RR_{new}\text{-}RP_{old}}} \\ &\quad + T_{\mathrm{RP_{old}\text{-}MN}} = 2t_{am} + 2t_u + 3t_r + t_{mr} + t_{ra} \end{aligned} \tag{12}$$

$$\begin{aligned}\mathrm{RL}_{\mathrm{INTER}}^{\text{LISP-SMCP}} &= 2T_{\mathrm{AR_{new}\text{-}TR_{new}}} + 2T_{\mathrm{TR_{old}\text{-}TR_{new}}} + T_{\mathrm{TR_{old}\text{-}MN}} \\ &= 2t_{am} + 3t_r + t_{mr} + t_{ra} \end{aligned} \tag{13}$$

5.4 切换阻塞率

切换阻塞率(Handoff Blocking Probability, BP)是指切换请求被阻塞的概率。切换阻塞率由一段时间内被阻塞的切换请求数与总切换请求数的比例表示。切换阻塞率通常用于反映 MN 在移动切换过程中，因切换故障造成 MN 的会话突然中断的可能性。导致切换阻塞的因素很多，本文只考虑切换时延因素。当 MN 在子网中的滞留时间小于切换时延时，则 MN 的会话将中断。

使用 μ_c 表示 MN 在子网间的穿越速率，μ_d 表示 MN 在接入网间的穿越速率，P_d 表示 MN 在接入网之间移动切换的概率，P_l 表示 MN 在接入网内的移动切换概率。假定 N 个子网组成一个圆形的接入网，每个子网的覆盖范围是半径为 R 的圆，MN 的平均移动速率为 v, MN 的会话到达率服从速率为 λ_s 的泊松分布。则可得到穿越速率和切换概率分别为[16]

$$\left.\begin{aligned}&\mu_c = 2v/\pi R,\ \mu_d = \mu_c/\sqrt{N} \\ &P_d = \mu_d/(\mu_d + \lambda_s),\ P_l = 1 - P_d\end{aligned}\right\} \tag{14}$$

假设 $E(\mathrm{HL}^{(\cdot)})$为 $\mathrm{HL}^{(\cdot)}$的期望，则 MN 的切换时延期望为

$$E(\mathrm{HL}^{(\cdot)}) = P_d \times E(\mathrm{HL}_{\mathrm{INTER}}^{(\cdot)}) + P_l \times E(\mathrm{HL}_{\mathrm{INTRA}}^{(\cdot)}) \tag{15}$$

假设 $E(\mathrm{HL}^{(\cdot)})$服从指数分布，其累积分布函数为 $F_T(t)$, MN 在一个子网中的滞留时间为 T_R，其概率密度函数为 $f_R(u)$，则可得到 MN 的切换阻塞率$(\mathrm{BP}^{(\cdot)})$为[17]

$$\begin{aligned}\mathrm{BP}^{(\cdot)} &= \Pr(\mathrm{HL}^{(\cdot)} > T_R) = \int_0^{\infty} [1 - F_T(u)]\, f_R(u) \mathrm{d}u \\ &= \mu_c E(\mathrm{HL}^{(\cdot)}) / (\mu_c E(\mathrm{HL}^{(\cdot)}) + 1) \end{aligned} \tag{16}$$

6 数值分析结果

表 3 给出了参数默认值，一些参数取值来源于文献[13]和文献[16]。

6.1 时延分析

图 7 给出了访问域与家乡域之间的距离(即路由器跳数)对认证时延的影响。图 7 表明 LISP-SMCP 认证时延不随访问域与家乡域的距离增加而改变。这是由于 LISP-SMCP 支持本地认证，即当 MN 在域内移动时，只需 $\mathrm{AR_{new}}$ 即可完成身份确认；MN 在域间移动时，只需 VAAA 和 $\mathrm{AR_{new}}$ 即可完成身份确认，其认证时延远低于其他方案。

图 8 和图 9 给出了移动检测时延对域内和域间位置注册时延的影响。图 8 和图 9 表明基于主机的

表 3 参数默认值

t_r	t_u	t_a	t_{am}	t_n	t_{ra}	t_{tc}	t_{ac}
5 ms	20 ms	3 ms	10 ms	5 ms	2 ms	2 ms	20 ms
t_{hc}	MinInt	MaxInt	m	N	R	v	λ_s
15 ms	30 ms	70 ms	0	5	500 m	20 m/s	10 sessions/s

移动性管理方案位置注册时延随移动检测时延 T_{MD} 增加而增加，基于网络的移动性管理方案位置注册时延不受 T_{MD} 的影响。从图 8 可以看出 LISP-SMCP, LISP-AR-DMC 和 MMILS 具有相同的域内位置注册时延，从图 9 可以看出 LISP-SMCP 具有较小的域间位置注册时延。

图 10 和图 11 给出了访问域与家乡域的距离对域内和域间切换时延的影响。图 10 和图 11 表明 LISP-SMCP 具有较小域内和域间切换时延，且不随访问域与家乡域的距离增加而改变。这是由于 LISP-SMCP 支持本地认证，具有较小的认证时延和位置注册时延。

6.2 切换阻塞率

由于 MobileID 和 LISP-AR-DMC 没有区域间的移动性管理，为了比较切换阻塞率，假定 MobileID 和 LISP-AR-DMC 方案中的 MN 的切换时延期望即为域内切换时延的期望。

如图 12 所示，图 12(a)表明切换阻塞率随 MN 移动速率增加而增加，图 12(b)表明切换阻塞率随着子网覆盖范围的增大而减小。图 12(c)显示会话到达

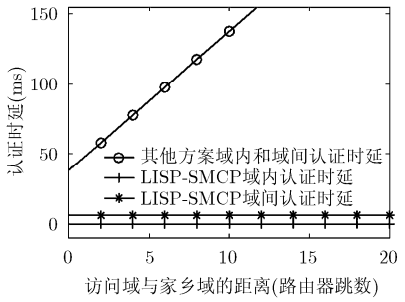

图 7 认证延迟与核心网路由器跳数

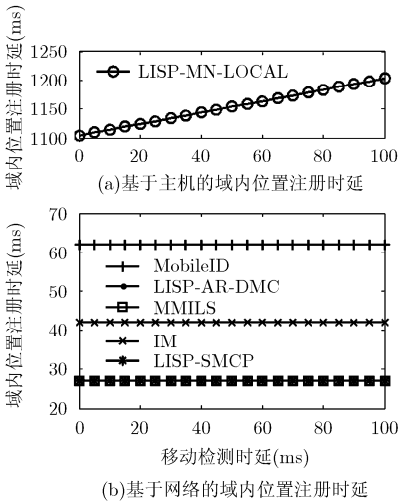

图 8 域内位置注册时延与移动检测时延

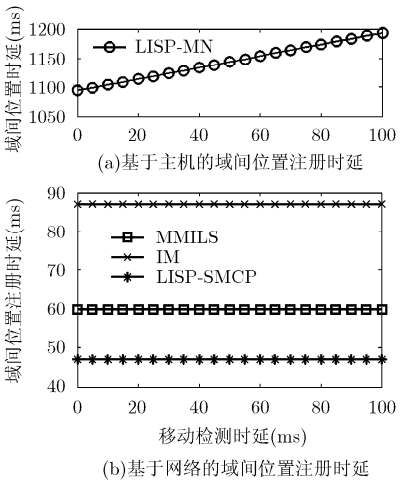

图 9 域间位置注册时延与移动检测时延

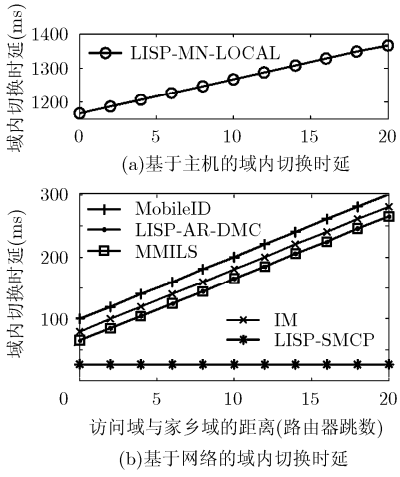

图 10 域内切换时延与路由器跳数

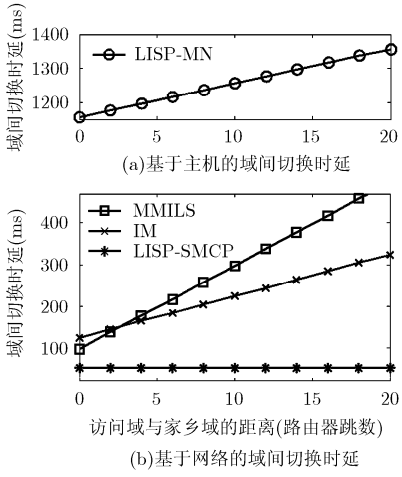

图 11 域间切换时延与路由器跳数

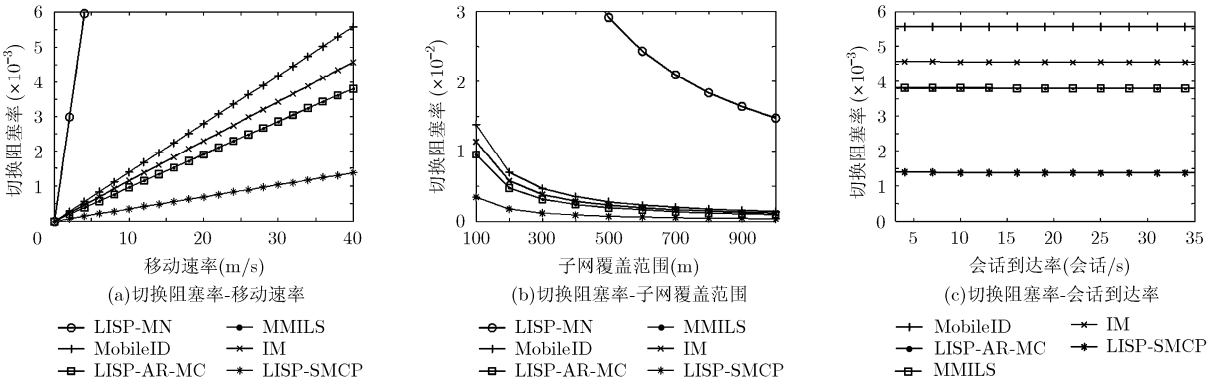

图 12 切换阻塞率的变化情况

率对切换阻塞率几乎没有影响。由于 LISP-MN 的切换阻塞率远大于其他方案，图 12(c)中未画出 LISP-MN 的切换阻塞率。图 12 表明 LISP-AR-DMC 和 MMILS 的切换阻塞率变化情况相同，LISP-SMCP 具有较小的切换阻塞率。

7 结束语

本文提出一种 LISP 环境下基于网络的安全移动性管理协议。该协议给出了基于 AAA 服务器的移动节点初始安全接入过程，区域内和区域间移动切换过程。该协议不需要对移动节点做修改，当移动节点在网络中漫游时，不需要向家乡域 HAAA 服务器询问其身份信息，支持本地认证和双向认证。此外，该协议可以防止中间人攻击、重放攻击和消息篡改攻击等。给出了性能分析模型，并与 LISP 环境下的其他移动性管理方案比较，结果表明提出的 LISP-SMCP 具有较小的认证时延、切换时延和切换阻塞率。

参 考 文 献

[1] Meyer D, Zhang L, and Fall K. Report from the IAB workshop on routing and addressing[S]. RFC 4984, Sept. 2007.

[2] Farinacci D, Fuller V, Meyer D, *et al.*. Locator/ID separation protocol (LISP)[OL]. http://tools.ietf.org/id/ draft-ietf-lisp-23.txt, May 4, 2012.

[3] Li T. Recommendation for a routing architecture[S]. RFC 6115, February 2011.

[4] Menth M, Klein D, and Hartmann M. Improvements to LISP mobile node[C]. 22nd International Teletraffic Congress (ITC), Amsterdam, Netherlands, 2010: 1–8.

[5] Dong P, Chen J, and Zhang H. A network-based localized mobility approach for locator/ID separation protocol[J]. *IEICE Transactions on Communications*, 2011, E94.B(6): 1536–1545.

[6] Gohar M and Seok Joo K. Network-based distributed mobility control in localized mobile LISP networks[J]. *IEEE Communications Letters*, 2012, 16(1): 104–107.

[7] Farinacci D, Lewis D, Meyer D, *et al.*. LISP mobile node[OL]. http://tools.ietf.org/id/draft-meyer-lisp-mn-07.txt, April 23, 2012.

[8] Qiu F, Li X, and Zhang H. Mobility management in identifier/locator split networks[J]. *Wireless Personal Communications*, 2012, 65(3): 489–514.

[9] Luo H, Zhang H, and Qiao C. Efficient mobility support by indirect mapping in networks with locator/identifier separation[J]. *IEEE Transactions on Vehicular Technology*, 2011, 60(5): 2265–2279.

[10] Fuller V, Farinacci D, Meyer D, *et al.*. LISP alternative topology (LISP+ALT)[OL]. http://tools.ietf.org/id/draft-ietf-lisp-alt-10.txt, December 6, 2011.

[11] Ma Z, Wang K, and Zhang F. Network-based inter-domain handover support for proxy mobile IPv6[OL]. http://www.ietf.org/id/draft-ma-netext-pmip-handover-02.txt, January 4, 2012.

[12] Korhonen J, Bournelle J, Chowdhury K, *et al.*. Diameter proxy mobile IPv6: mobile access gateway and local mobility anchor interaction with diameter server[S]. RFC 5779, February 2010.

[13] Ki-Sik K, Wonjun L, Youn-Hee H, *et al.*. Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6[J]. *IEEE Wireless Communications*, 2008, 15(2): 36–45.

[14] Johnson D, Perkins C, and Arkko J. Mobility support in IPv6[S]. RFC 3775, June 2004.

[15] Thomson S and Narten T. IPv6 stateless address autoconfiguration[S]. RFC 2462, December 1998.

[16] Makaya C and Pierre S. An analytical framework for performance evaluation of IPv6-based mobility management protocols[J]. *IEEE Transactions on Wireless Communications*, 2008, 7(3): 972–983.

[17] Yang S, Zhou H, Qin Y, *et al.*. SHIP: cross-layer mobility management scheme based on session initiation protocol and host identity protocol[J]. *Telecommunication Systems*, 2009, 42(1): 5–15.

唐建强： 男，1987 年生，博士生，研究方向为网络路由交换技术、网络安全.

刘 颖： 女，1978 年生，博士，讲师，研究方向为下一代互联网、网络安全.

张宏科： 男，1957 年生，博士，教授，研究方向为网络路由交换技术、普适服务理论技术.