一种无线 Mesh 网络中可证明安全的 HMIPv6 路由优化方案

王 刚 郭渊博 刘 伟

(信息工程大学电子技术学院 郑州 450004)

摘 要 HMIPv6 技术能够实现无线 Mesh 网络的无缝切换,针对其绑定更新过程中执行路由优化存在的安全问题,提出了一种适用于无线 Mesh 网络的基于椭圆曲线公钥自认证体制的安全路由优化方案。该方案使用户在执行路由优化的过程中能够实现对绑定更新消息的认证与授权,且通过有效的会话密钥协商机制为绑定更新消息的传输提供了安全保障,具有可证明安全性。最后通过性能分析表明,该方案简化了标准路由优化方案的流程,提高了一般注册过程的效率。

关键词 无线 Mesh 网络,层次化移动 IPv6,绑定更新,路由优化,可证明安全

中图法分类号 TP393.08 **文献标识码** A

Provable Secure Route Optimization Scheme for HMIPv6 in Wireless Mesh Network

WANG Gang GUO Yuan-bo LIU Wei

(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract HMIPv6 technology can implement the seamless handover in wireless mesh network. To address the security issues of route optimization in the mobile handover binding update procedure, a elliptic curve cryptography self-certified public key cryptosystem based secure route optimization scheme was proposed, which is applicable to the wireless mesh network. The proposed scheme not only addresses authentication and authorization of binding update messages in route optimization for mesh clients, but also provides security for the binding update messages by effective session-key negotiation mechanism, which affords provable security. Furthermore, the performance analysis shows that the proposed scheme can simplify the procedure of standard routing optimization scheme and improve the efficiency of the general registration procedure.

Keywords Wireless mesh network, HMIPv6, Binding update, Routing optimization, Provable security

1 引言

无线 Mesh 网络(Wireless Mesh Network, WMN)旨在为无线用户提供更加快速、稳定、随时随地的通信服务[1]。移动 IPv6 技术(Mobile IPv6, MIPv6)能够为无线 Mesh 网络中漫游的无线用户提供无缝的 Internet 访问[2],其支持的路由优化机制是解决网络切换过程中"三角路由"问题的关键技术,能够在一定程度上提高用户一般注册过程的效率。层次化移动 IPv6(Hierarchical Mobile IPv6, HMIPv6)是 MIPv6 的一种扩展技术,无线 Mesh 网络利用 HMIPv6 的层次化移动管理技术能够增强对网络层的移动支持能力,解决对切换用户的移动管理问题,并能够减少当用户远离家乡网络时因频繁发生切换向家乡代理进行地址更新而造成的网络延迟。

然而,WMN 的多跳、自组织及接入灵活等特性在带来高通信覆盖率和接入便利的同时,使其在安全性方面具有天然的缺陷,HMIPv6 技术的实施面临着巨大的安全威胁。如何解决基于 HMIPv6 的无线 Mesh 网络(HMIPv6-WMN)切换过程中路由优化阶段存在的安全问题,对于保证 HMIPv6-WMN 网络切换一般注册过程的安全性是至关重要的。

针对 HMIPv6-WMN 网络切换一般注册过程中执行路由优化存在的安全问题,主要有以下可借鉴的研究成果:RFC3775 中提出利用返回可路由协议(Return Routability Procedure, RRP)[3]来实现路由优化过程的认证及安全防护,RRP 并非是绝对安全的,RRP 只能提供对用户转交地址可达性的验证,而无法验证用户地址的所有权且不能提供保障数据传输的安全机制。为了增强路由优化的安全性,相关研究人员提出了一些针对 RRP 的改进方案[4-6],这些方案一定程度上增强了路由优化过程的安全性,但并不完全满足无线 Mesh 网络的安全需求。文献[7,8]分别提出了两种基于身份密码公钥体制(Identity-based Cryptography, IBC)的安全路由优化方案,然而,IBC 存在着密钥托管且计算开销较大等问题,有着巨大的安全隐患。文献[9]提出了针对 IBC 的改进方案来实现安全切换,但没有提出针对路由优化过程的安全有效的解决方案。现有的安全方案在解决 HMIPv6-WMN 网

到稿日期:2011-04-30 返修日期:2011-06-30 本文受国家 863 计划项目(2007AA01Z405),河南省科技创新杰出青年计划项目(104100510025)资助。

王 刚 硕士生,主要研究方向为无线网络安全、移动 IPv6,E-mail:wangg911@126.com;郭渊博 博士后,副教授,硕士生导师,主要研究方向为无线网络安全、信息安全;刘 伟 副教授,硕士生导师,主要研究方向为数据库、信息管理系统。

络切换路由优化过程的安全问题时存在各种各样的问题，研究适用于 HMIPv6-WMN 网络的安全路由优化方案成为亟待解决的问题。

2 相关工作

通过对现有各种密码体制进行综合分析考虑，我们认为椭圆曲线公钥自认证密码体制(ECC-based Self-certified Public Key Cryptosystems，ECCSCPKC)[10]是一种能够有效解决上述问题的安全机制。本文提出了一种基于 ECCSCPKC 的安全路由优化方案，其原理是：将运用 ECCSCPKC 签名机制生成的用户身份签名信息加入统计学唯一且加密可验证地址生成方案(Statistically Unique and Cryptographically Verifiable，SUCV)[11]，提出改进的 SUCV(Improved SUCV，ISUCV)安全地址生成算法，并结合 RRP 中路由可达性测试的思想，运用 ECCSCPKC 安全体系来保障路由优化过程的可认证性及数据传输的安全性。其优势体现在以下几个方面：

(1)该方案具有 RRP 中对路由可达性验证的功能，并利用 ISUCV 生成地址包含签名的可认证性，实现了对可达地址声明所有权的验证，实现了执行路由优化用户间的双向认证，保证了执行路由优化的双方是可信任的；

(2)该方案在进行路由可达性验证的同时实现了用户间的安全会话密钥协商过程，并建立了安全隧道来保证随后一般注册过程消息传输的安全性；

(3)该方案结合了 ECC 与自认证公钥两种密码体制的特点，具有简单的密钥分发及维护和轻量级运算等优势，能够有效解决 IBC 存在的用户私钥泄漏等安全隐患；

(4)该方案利用生成地址的可认证性，简化了基于 RRP 路由优化中对转交地址可达性的验证过程，减少了路由优化过程中的“握手”次数，提高了一般注册的效率，优化了网络的切换性能。

3 ECCSCPKC 安全路由优化方案

3.1 路由优化执行策略

HMIPv6-WMN 网络切换拓扑结构如图 1 所示。Operator 是 WMN 网络中一个离线公钥生成器(Public Key Generator，PKG)。网络中通信对端用户 CN 与 Mesh 用户 MC 的通信都是经过移动锚节点 MAP 转发的，这样能够减少 MC 在同一 MAP 域内频繁移动时发送绑定更新消息的数量，减少切换延时。

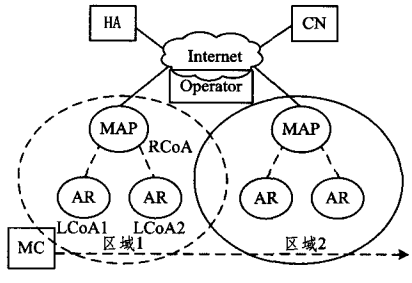

图 1 HMIPv6-WMN 网络切换拓扑结构

HMIPv6-WMN 路由优化执行策略如图 2 所示。当 MC 移动到新的 MAP 域时，首先生成一个安全的转交地址，在完成与接入域的认证与家乡注册，并收到来自家乡代理转发的对端用户发送的数据包时，MC 决策是否进行路由优化来实现一般注册过程，路由优化过程运用了 ECCSCPKC 的签名、密钥协商和加密解密机制。

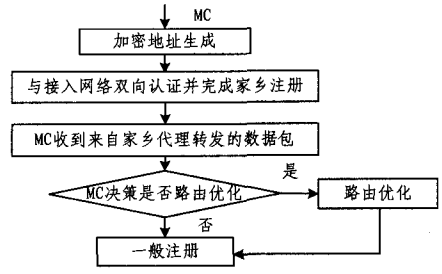

图 2 HMIPv6-WMN 路由优化执行策略

3.2 椭圆曲线公钥自认证密码体制

ECCSCPKC 需要可信的 Operator 为用户生成公钥，用户利用公开信息生成自身私钥，因此 Operator 不知道用户的私钥。

其操作过程分为两个阶段，原理如下：

1. 参数生成阶段(由 Operator 执行)

选取参数$(E(F_p),p,G,n,h)$。其中 E 为有限域 F_p 上的椭圆曲线，p 为一个 160bit 的大素数或等于 2^m，G 为选择的基点，n 为 G 的阶，Hash 函数 h 将任意长的字符串映射到固定长度的字符串 r，$r\in[2,n-2]$。

选取一个随机整数 $s\in[2,n-2]$作为 Operator 的密钥，计算公钥 $Q=s\cdot G$。

公开系统参数$(E(F_p),p,G,n,h)$，s 保密。Operator 下的用户使用相同的系统参数。

2. 密钥生成阶段(由用户执行)

MC 选取形如 *username@domain.com* 的网络接口标识 NAI 作为身份 ID_{MC}，并选取一个随机整数 $x_{MC}\in[2,n-2]$作为主密钥，计算 $V_{MC}=Hash(x_{MC}\parallel ID_{MC})\cdot G$ 并发送(ID_{MC},V_{MC})至 Operator。Operator 选取一个随机整数 $k\in[2,n-2]$，并计算 MC 的公钥 Q_{MC} 和证明值 ω_{MC}。

$$Q_{MC}=V_{MC}+(k-Hash(ID_{MC}))\cdot G=(Q_x^{MC},Q_y^{MC})$$

$$\omega_{MC}=k+s\cdot(Q_x^{MC}+Hash(ID_{MC}))\bmod n$$

Operator 发送(Q_{MC},ω_{MC})给 MC。MC 生成私钥 $s_{MC}=\omega_{MC}+Hash(x_{MC}\parallel ID_{MC})\bmod n$，并验证：

$$s_{MC}\cdot G=Q_{MC}+Hash(ID_{MC})\cdot G+[(Q_x^{MC}+Hash(ID_{MC}))\bmod n]\cdot Q$$

若验证有效，则(Q_{MC},s_{MC})为 MC 的公私钥对。

本文涉及到的基于 ECCSCPKC 的相关机制有：

1. 签名机制

(1)签名生成过程

①MC 随机选择时间变量整数 $k_{MC}\in[2,n-2]$，计算 $k_{MC}\cdot G=(X_{MC},Y_{MC})$。

②MC 计算：$X_{MC}\equiv R \bmod p$，若 $R=0$，重选 k_{MC}。

$S=k_{MC}+s_{MC}\cdot Hash(M\parallel R)(\bmod n)$，若 $S=0$，重选 k_{MC}。

③MC 发送签名消息(R,S)及 M 给 MC′。

(2)签名验证过程

①验证 R,S 是否为[2,$n-2$]间的整数。

②MC′计算：

$V_{MC}=Q_{MC}+Hash(ID_{MC})\cdot G+[(Q_x^{MC}+Hash(ID_{MC}))\ \mathrm{mod}\ n]\cdot Q$

$S\cdot G-V_{MC}\cdot Hash(M\|R)$

$=k_{MC}\cdot G+(s_{MC}\cdot Hash(M\|R)\ \mathrm{mod}\ n)\cdot G-(s_{MC}\cdot G)\cdot Hash(M\|R)$

$=k_{MC}\cdot G=(X_{MC},Y_{MC})$

③如果 $X_{MC}\equiv R\ \mathrm{mod}\ p$ 成立，则签名有效。

2. 会话密钥协商机制

注册过的用户 MC 与 MC′间基于时间变量的会话密钥协商过程如下：

①MC 用主密钥 $x_{MC}\in[2,n-2]$，计算

$T_{MC}=x_{MC}\cdot G\ \mathrm{mod}\ n$，发送($ID_{MC}$,$Q_{MC}$,$T_{MC}$)给 MC′。

②MC′计算 $K_{(MC'-MC)}$ 如下：

$V_{MC}=Q_{MC}+Hash(ID_{MC})\cdot G+[(Q_x^{MC}+Hash(ID_{MC}))\ \mathrm{mod}\ n]\cdot Q$

$K_{(MC'-MC)}=x_{MC'}\cdot V_{MC}+s_{MC'}\cdot T_{MC}$

$=(x_{MC'}s_{MC}\ \mathrm{mod}\ n)\cdot G+(s_{MC'}x_{MC}\ \mathrm{mod}\ n)\cdot G$

③反之

$K_{(MC-MC')}=x_{MC}\cdot V_{MC'}+s_{MC}\cdot T_{MC'}$

$=(x_{MC}s_{MC'}\ \mathrm{mod}\ n)\cdot G+(s_{MC}x_{MC'}\ \mathrm{mod}\ n)\cdot G$

3. 加密解密机制

会话密钥协商过的 MC 向 MC′发送加密消息 M 的加密解密过程如下：

(1)加密过程

MC 将消息 M 转化为椭圆曲线上的一点(m_x,m_y)。

②MC 随机选择整数 $\omega_{MC}\in[2,n-2]$，并计算 $V_{MC'}$、C_1 和 C_2 如下：

$V_{MC'}=Q_{MC'}+Hash(ID_{MC'})\cdot G+[(Q_x^{MC'}+Hash(ID_{MC'}))\ \mathrm{mod}\ n]\cdot Q$

$C_1=\omega_{MC}\cdot G$

$C_2=M+\omega_{MC}\cdot V_{MC'}$

③MC 把密文 C_1 和 C_2 发送给 MC′。

(2)解密过程

MC′通过如下计算恢复消息 M：

$C_2-s_{MC'}\cdot C_1=M+\omega_{MC}\cdot V_{MC'}-(\omega_{MC}\cdot s_{MC'}\ \mathrm{mod}\ n)\cdot G=M$

3.3 改进的 SUCV 安全地址生成算法

ISUCV 安全地址生成算法采用 ECCSCPKC 签名机制生成用户 IPv6 地址的后 64 位接口标识，即生成新的 64 位 isucvHID，isucvHID 中包含对 MC 身份 ID_{MC} 的签名信息，具有不可伪造性；通过对 ISUCV 地址中签名进行验证，能够实现对生成地址所有权的验证，使得 ISUCV 地址具有可认证性。ISUCV 地址的生成与验证过程如下：

1. ISUCV 地址生成过程

Operator 为 MC 生成 Q_{MC}，MC 自己生成私钥 s_{MC}，构成公私钥对(Q_{MC},s_{MC})，设 MC 接入网络的子网前缀是长度为 64bit 的 $pre\_addr\in\{0,1\}^*$，令：

$M\leftarrow\{pre\_addr\|Q_{MC}\}\in\{0,1\}^*$

(1)随机选择时间变量整数 $k_{MC}\in[2,n-2]$，计算 $k_{MC}\cdot G=(X_{MC},Y_{MC})$。

(2)计算：$X_{MC}\equiv R\ \mathrm{mod}\ p$，若 $R=0$，重选 k_{MC}。

$S=k_{MC}+s_{MC}\cdot Hash(M\|R)(\mathrm{mod}\ n)$，若 $S=0$，重选 k_{MC}。

设 $\sigma=(R,S)$为针对 M 的签名。

(3)将签名 σ 映射到椭圆曲线 $E(Fp)$ 上的一点(σ_x,σ_y)，σ_x 长度为 160bit，取 σ_x 最左端的 64bit 作为输出，将 σ 作为 ISUCV 参数。

(4)将输出字段的第 6 位置 1，生成 ISUCV 地址的后 64bit 接口标识 isucvHID，通过与路由宣告消息中包含的子网前缀信息 pre_addr 进行串接，生成完整的 ISUCV 地址。

2. ISUCV 地址验证过程

假设地址验证者在对消息源地址进行验证前已经获得该地址生成者的身份消息(ID_{MC},Q_{MC})，当地址验证者收到使用 ISUCV 地址发送的消息后，执行如下操作对生成的 ISUCV 地址进行验证：

(1)独立计算 ISUCV 参数 σ 生成 σ_x'，取出 σ_x'字段的最左端 64bit，将第 6 位置 1，将得到的结果与 ISUCV 地址的后 64bit 进行比对，如果不一致，验证失败，结束验证过程；否则执行如下验证操作：

(2)计算：$M\leftarrow\{pre\_addr\|Q_{MC}\}$

(3)计算：

$V_{MC}=Q_{MC}+Hash(ID_{MC})\cdot G+[(Q_x^{MC}+Hash(ID_{MC}))\ \mathrm{mod}\ n]\cdot Q$

$S\cdot G-V_{MC}\cdot Hash(M\|R)$

$=k_{MC}\cdot G+(s_{MC}\cdot Hash(M\|R)\ \mathrm{mod}\ n)\cdot G-(s_{MC}\cdot G)\cdot Hash(M\|R)=k_{MC}\cdot G=(X_{MC},Y_{MC})$

(4)验证：若 $X_{MC}\equiv R\ \mathrm{mod}\ p$ 成立，接收使用该 ISUCV 地址的 MC 发送的消息，否则放弃消息。

3.4 安全路由优化方案实现过程

提出的安全路由优化方案实现过程如图 3 所示，主要可以分为可返路由测试过程和一般注册过程。在可返路由测试过程中，MC 向需要执行路由优化的 CN 发送家乡地址可达性测试，CN 通过由 HA 转发的测试消息可以验证 HoA 的可达性；在一般注册过程中，CN 能够实现对注册消息中包含的 MC 的 RCoA 进行验证，同时进行绑定注册。假设 MC 与 HA，HA 与 CN 之间已建立共享会话密钥。若 MC 与 CN 间的共享会话密钥过期，需要重新协商。

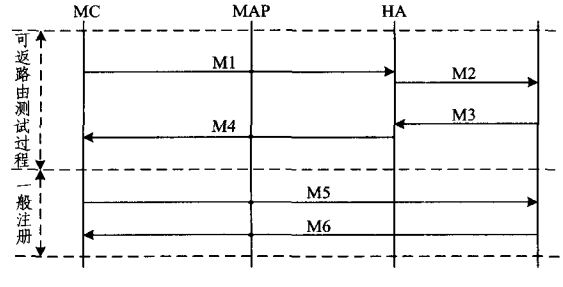

图 3 安全路由优化方案实现过程

M1：$MC\rightarrow HA$：$\{QR\|ID_{MC}\|Q_{MC}\|N_0\|MIC_{MC-HA}\}$

MC 收到来自 HA 转发的 CN 的数据包后，利用 CN 地址的可认证性对 CN 进行身份认证，认证成功后通过 MAP 由

HA 向 CN 发送地址优化请求消息 M1，该消息中包含公钥请求信息 QR，MC 的身份信息（ID_{MC}，Q_{MC}）及安全载荷信息（包括随机数 N_0 和消息完整性验证码 MIC_{MC-HA}）。

M2：$HA \rightarrow CN$：$\{QR \parallel ID_{MC} \parallel Q_{MC} \parallel N_0 \parallel MIC_{HA-CN}\}$

HA 收到消息 M1 后，利用 MIC_{MC-HA} 验证消息的完整性，若验证失败，则丢弃该消息；否则提取 $\{QR \parallel ID_{MC} \parallel Q_{MC} \parallel N_0\}$，用 HA 与 CN 的共享会话密钥封装并生成消息 M2，通过安全隧道将其发送到 CN。

M3：$CN \rightarrow HA$：$\{QA \parallel ID_{CN} \parallel Q_{CN} \parallel N_1 \parallel MIC_{CN-HA}\}$

CN 首先验证消息 M2 的完整性，验证成功后建立列表记录序列值 N_0，并根据收到的公钥请求消息 QR 生成包含身份信息（ID_{CN}，Q_{CN}）的请求应答消息 QA，封装 QA 值与 N_1 生成消息 M3 发送给 HA。

M4：$HA \rightarrow MC$：$\{QA \parallel ID_{CN} \parallel Q_{CN} \parallel N_1 \parallel MIC_{HA-MC}\}$

同理，HA 验证消息 M3 并生成消息 M4，经 MAP 转发给 MC。

M5：$MC \rightarrow CN$：$\{BU \parallel N_2 \parallel MIC_{MC-CN}\}$

MC 得到 QA 值后利用 CN 的身份信息（ID_{CN}，Q_{CN}）计算共享会话密钥 K_{MC-CN}，封装包含转交地址信息（RCoA，HoA）的绑定更新消息 BU 和随机序列值 N_2，生成消息 M5。

M6：$CN \rightarrow MC$：$\{BA \parallel N_3 \parallel MIC_{CN-MC}\}$

CN 收到消息 M5 后，验证消息的完整性和 N_2 的正确性，通过验证 MC 的 RCoA 的所有权来实现对转交地址可达性的验证，若验证成功，则表明 MC 的 HoA 与 RCoA 具有可认证性与可达性；CN 绑定 BU 消息并生成封装的 BA 消息 M6 反馈给 MC，完成一般注册过程，否则丢弃 BU 消息。

4 安全性证明

CK 模型利用模块化方法分析与设计可证明安全的密钥交换协议[12]。CK 模型中攻击者 $\mathcal{A}$ 为概率多项式时间图灵机，$\mathcal{A}$ 能够按照一定的规则控制网络，具有被动攻击和主动攻击能力，主要包括：发送查询；Corrupt 查询；泄露查询（包括临时私钥泄漏查询、长期私钥泄漏查询、会话密钥泄漏查询、系统主密钥泄漏查询）；Expose 查询；测试查询等。

本文提出的安全路由优化方案的会话密钥协商过程在 CK 模型下是 SK 安全的，规定攻击者 $\mathcal{A}$ 只具有被动窃听攻击能力，不具有篡改和伪造能力。定义 Sid 为会话标识符，认证器 C 能够将认证模型 AM 中的协议转化为非认证模型 UM 下一个等价的协议，安全路由优化方案中会话密钥协商流程如图 4 所示。

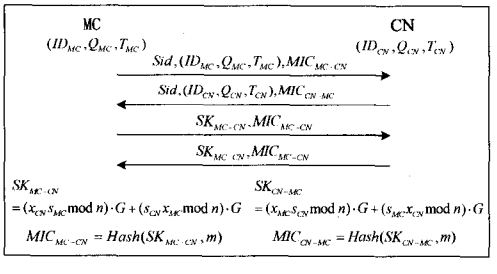

图 4 安全路由优化方案中会话密钥协商流程

定义 1[12] 如果对于 UM（AM）中任何密钥交换协议对手 $\mathcal{A}$，协议能够满足下列性质，称该协议在 UM（AM）中是 SK 安全的。

（1）参与双方实体成功完成了匹配的会话，并且输出相同的会话密钥；

（2）$\mathcal{A}$ 进行 Test 查询，成功的概率不超过 $0.5+\varepsilon$，ε 为安全参数下可忽略的概率。

定义 2[12] 认证器 C 是能够将任何 AM 中的协议 π 转换为 UM 中等价的协议 π' 的转换器。

定义 3[12] 认证器 C 的输入是协议 π，λ 是 MT 认证器，输出是协议 $\pi'=C_\lambda(\pi)$，满足：若 π 在 AM 中是 SK 安全的，则 π' 在 UM 中也是 SK 安全的。

OWHF 假设：h 为单列哈希函数。给定 $h(m)$，m 是计算不可得的。而且，给定 m、$h(m)$ 和 $h(m')$，m' 是计算不可得的，即如果 $m \neq m'$，$h(m)=h(m')$ 是计算不可得的。

ECDL 假设：给定有限域 F_p 上阶为 n 的椭圆曲线 $E(F_p)$ 和两点 $P, Q \in E(F_p)$。假设存在 $l \in [2, n-2]$ 且 $l \cdot P=Q$，若 n，p 足够大，在已知 $E(F_p)$ 与 P 的前提下是无法计算求得 Q 的。

定理 1 消息完整性验证码 MIC 在 OWHF 假设的前提下是安全的。

证明：MC 与 CN 间消息完整性验证码 $MIC_{MC-CN}=Hash(SK_{MC-CN}, m)$，显然，MIC 是 OWHF 安全的。

定理 2 在 ECDL 假设成立且 MIC 安全的前提下，$\pi_{MC,CN}^{ECSCPKC\text{-}HMWMNv6}$ 在 AM 模型中是 SK 安全的。

证明：在协议交互过程中，若挑战者 MC 与 CN 均没被攻击者 $\mathcal{A}$ 攻陷，成功完成了匹配的会话，MN 与 CN 都得到了没有篡改的（ID_{CN}，Q_{CN}，T_{CN}）和（ID_{MC}，Q_{MC}，T_{MC}），则生成的共享会话密钥是一致的，这满足定义 1 的性质 1，其中

$$SK_{MC-CN}=SK_{CN-MC}$$
$$=(x_{CN}s_{MC} \bmod n)\cdot G+(s_{CN}x_{MC} \bmod n)\cdot G$$

假设在 AM 中存在一个攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ε 区分测试会话查询中返回的值是真实的会话密钥还是等长随机数。CK 模型中，攻击者 $\mathcal{A}$ 无法对测试会话与匹配的会话进行实体攻陷、泄漏会话状态、查询会话密钥与实体长期私钥等攻击，只能通过攻破用会话密钥加密的消息或者通过获得会话密钥的组成元素来生成会话密钥。针对情况 1，攻击者 $\mathcal{A}$ 能够以不可忽略的优势 ε 攻破对称加密消息，即攻击者 $\mathcal{A}$ 能够从消息验证码中提取加密消息，并从加密消息中恢复加密密钥，这是与定理 1 和 ECDL 假设相矛盾的；针对情况 2，攻击者 $\mathcal{A}$ 能够获得会话中用消息验证码保护的（ID_{CN}，Q_{CN}，T_{CN}）和（ID_{MC}，Q_{MC}，T_{MC}），并通过计算生成会话密钥：

$$V_{MC}=Q_{MC}+Hash(ID_{MC})\cdot G+[(Q_x^{MC}+Hash(ID_{MC}))$$
$$\bmod n]\cdot Q$$
$$SK_{CN-MC}=x_{CN}V_{MC}+s_{CN}T_{MC}$$
$$=(x_{CN}s_{MC} \bmod n)\cdot G+(s_{CN}x_{MC} \bmod n)\cdot G$$

显然这与定理 1 中测试会话无法获得双方实体私钥相矛盾。因此，攻击者 $\mathcal{A}$ 进行 Test 查询，成功区分会话密钥与等长随机数的概率不超过 $0.5+\varepsilon$，ε 为安全参数下可忽略的，满足定义 1 的性质 2。

综上，在 ECDL 假设成立且 MIC 安全的前提下，$\pi_{MC,CN}^{ECSCPKC-HMWMNv6}$ 在 AM 模型中是 SK 安全的。

定理 3 假设 ECCSCPKC 加密算法 $E_{ECCSCPKC}$ 和消息验证码 MIC 能够抵抗选择消息攻击，则 MT 认证器 λ 能够仿真 UM 环境下的 MT 协议。

证明：设 $\mathcal{A}$ 是与 λ 交互的 UM 攻击者，构造一个计算不可区分的 AM 攻击者 $\mathcal{A}$。$\mathcal{A}'$ 在 UM 中与运行 MIC 的 MC′、CN′进行交互，$\mathcal{A}$ 在 AM 中与 MC、MN 进行交互。

α 事件表示：当 MC′未被 $\mathcal{A}'$ 攻陷时，CN′输出“CN′收到 $m_{MC'}$”，且 MC $\xrightarrow{m}$ CN 处于未激活状态。若 α 事件发生，则说明 $\mathcal{A}'$ 成功伪造了一个新的 MIC 值。

假设 α 事件发生的概率为 δ，l 是 $\mathcal{A}'$ 在测试查询中交互消息的次数，UM 中通信双方为 MC′和 CN′，攻击者 $\mathcal{A}'$ 作为一个 MIC 伪造者 $\mathcal{F}$，在允许至多 l 次询问相应 MIC 预言机 M_K 的条件下，$\mathcal{F}$ 成功的概率为 δ/l。

$\mathcal{F}$ 定义：输入 m，$\eta_{MN'}=E^{K}_{CN'}(m,Q_{MN'},ID_{MN'},T_{MN'})$，$\eta_{CN'}=E^{K}_{MN'}(m,Q_{CN'},ID_{CN'},T_{CN'})$，$\eta=M_K((m)_{SK})$。$\mathcal{F}$ 仿真 MN′和 CN′与攻击者 $\mathcal{A}'$ 间的交互过程，m^* 是随机给定的一个激活消息。

(1)当 CN' 被 $\mathcal{A}'$ 用消息 $(m,\eta_{MN'})$ 激活，$\mathcal{F}$ 向 MN′发送 $(m,\eta_{CN'})$；

(2)当 MN′被 $\mathcal{F}$ 用消息 $(m,\eta_{CN'})$ 激活，且 $m\neq m^*$，$\mathcal{F}$ 随机选取 K^*，返回 $\eta=M_{K^*}((m)_{SK})$；

(3)若 $\eta_{MN'}$ 被查询过，则 $\mathcal{F}$ 询问预言机 M_K 输出返回值，若 $m=m^*$，$\mathcal{F}$ 仿真失败，放弃；

(4)若 $\mathcal{A}'$ 用 MN′发送的消息 $(m,\eta_{MN'})$ 激活 CN′，$\mathcal{F}$ 输出 (m,η)。

β 事件表示：在 $\mathcal{F}$ 仿真中，MN′被伪造，对应的伪造消息是 m^*。因为 m^* 伪随机选取，且 β 和放弃事件不会同时发生，所以 β 发生的概率为 δ/l。

当 MT-λ 中对应伪造消息 m^* 的 β 事件发生时，CN′最后接收到的消息是一个合法的 MIC 值，而 MN′从未生成过对应消息的 MIC 值，则 $\mathcal{F}$ 以概率 δ/l 成功伪造了一个新的 MIC 值，δ/l 是概率不可忽略的，这与定理 3 是矛盾的。

综上，在 ECCSCPKC 加密算法 $E_{ECCSCPKC}$ 和消息验证码 MIC 能够抵抗选择消息攻击的前提下，MT 认证器 λ 能够仿真 UM 环境下的 MT 协议。

定理 4 在 ECDL 假设成立且 MIC 安全的前提下，$\pi^{ECSCPKC-HMWMNv6}_{MC,CN}$ 在 UM 模型中是 SK 安全的。

证明：根据定义 1—定义 3 及定理 2 和定理 3 可证。

5 性能分析

表 1 为本文提出的安全路由优化方案与基于 RRP 的路由优化方案[3]的性能分析。

表 1 性能分析

方案名称	握手次数	签名验证次数	Hash 运算次数	会话密钥计算次数	加密次数	解密次数
RRP	4	0	6	2	4	2
OUR	3	2	6	2	6	6

由上表可以看出，本文提出的安全路由优化方案的运算次数略高于基于 RRP 的路由优化方案，而基于 ECCSCPKC 的签名运算、会话密钥计算及加解密算法的运算是轻量级的[10]，且减少了一次交互过程。综合安全性与性能分析，本文提出的安全路由优化方案能够保证 HMIPv6-WMN 切换一般注册过程的安全性并且能够提高绑定更新过程的效率。

结束语 本文提出了无线 Mesh 网络中一种椭圆曲线公钥自认证密码安全体系下的可证明安全的 HMIPv6 路由优化方案。该方案解决了用户在切换过程中执行路由优化的认证、授权和数据安全传输的问题，且仅经过 3 次握手就能够实现路由优化用户间的双向认证与密钥协商。通过安全性证明，该方案在 CK 模型下是 SK 安全的，保证了一般注册过程的安全性；该方案简化了标准路由优化方案的流程，提高了一般注册过程的效率，从而达到了无线 Mesh 网络切换一般注册阶段路由优化过程的安全保障与性能优化。

参 考 文 献

[1] Srivathsan S, Balakrishnan N, Iyengar S S. Scalability in Wireless Mesh Networks [M]. Guide to Wireless Mesh Networks, Computer Communications and Networks, 2009: 325-347

[2] Sultana H P, Pounambal M, Krishna P V. A Fast Handover Scheme for Multicasting in IPv6 based Mobile Ad-hoc Networks [J]. Journal of Computer Science, 2011, 7(1): 90-94

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

[4] Ren Kui, Lou Wen-jing, Zeng Kai, et al. Routing optimization security in mobile IPv6 [J]. Computer Networks, 2006, 50: 2401-2419

[5] Song Seh-wa, Choi H-K, Kim J-Y. A Secure and Lightweight Approach for Routing Optimization in Mobile IPv6 [J]. EURASIP Journal on Wireless Communications and Networking, 2009(7)

[6] 黄志彬，洪佩琳. 移动 IPv6 路由优化安全方案[J]. 计算机工程与应用，2009，45(6)：120-123

[7] Kandikattu R, Jacob L. A Secure IPv6-based Urban Wireless Mesh Network (SUMNv6) [J]. Computer Communications, 2008, 31: 3707-3718

[8] 侯雅毅，钱焕延，王晓喃. MIPv6 中基于身份的安全路由优化[J]. 计算机工程，2009，35(9)：127-129

[9] 张志，崔国华. 移动 IPv6 网络安全接入认证方案[J]. 计算机科学，2009，36(12)：26-31

[10] Tsaur W J. Several security schemes constructed using ECC-based self-certified public key cryptosystems [J]. Applied Mathematics and Computation, 2005, 168(1): 447-464

[11] Montenegro G, Castelluccia C. SUCV Identifiers and Addresses [Z]. Internet Draft, 2001

[12] Canetti R, Krawczyk H. Analysis of Key-exchange Protocol and Their Use for Building Secure Channel [C]// Proceedings of the Euro-crypt 01. Berlin: Springer-Verlag, 2001: 453-474