

# 支持安全性和移动性的主机身份协议研究

毛燕琴

(南京邮电大学 计算机学院, 江苏 南京 210003)

**摘要:**安全性、移动性和服务质量构成了当前互联网研究的三类关键问题。文中研究探讨了可以支持安全性和移动性的主机身份协议(HIP),论述了该协议对安全性和移动性支持能力,其将公钥体系中的公钥作为主机身份标识(HI),使得主机身份标识具备了验证主机身份真伪的能力,以及通过会话绑定主机身份而非 IP 地址来提供主机移动管理能力。但是 HIP 体系结构及其协议缺乏管理基础设施以及完整的协议簇,尚无法在现有互联网中直接部署和应用。针对此问题,提出了采用联邦制身份体系实现各个管理域之间的主机身份验证以解决 HIP 管理基础设施的不足,以及采用包含主机身份验证协议和主机身份查询协议的主机身份层解决 HIP 完整协议簇的建议。并且说明了改进建议的合理性。

**关键词:**主机身份协议;安全性;移动性;联邦制;管理基础设施

**中图分类号:**TP31

**文献标识码:**A

**文章编号:**1673-629X(2015)08-0161-05

**doi:**10.3969/j.issn.1673-629X.2015.08.034

## Study on Host Identify Protocol Supporting Security and Mobility

MAO Yan-qin

(School of Computer Science & Technology, Nanjing University of Posts and  
Telecommunications, Nanjing 210003, China)

**Abstract:** Security, mobility and QoS (Quality of Service) are three critical issues of current Internet research. The Host Identify Protocol (HIP) supporting security and mobility is discussed which takes a public key of public key cryptography as a Host Identifier (HI). The capability for supporting security and mobility of HIP are discussed which takes the public key in the public key infrastructure as the host identifier to provide the ability to verify the identity of the host, and binds the session through the host identifier instead of IP address to provide the host mobility management capability. However, the lack of management infrastructure and complete protocol stack, HIP architecture and protocol could not be deployed and applied directly in practical network environment. To solve these problems, using federated identify based approach to achieve host identity authentication among multi-management domains to solve the HIP management infrastructure deficiencies, and applying host identity layer containing host authentication protocol and host identity query protocol to solve HIP complete protocol stack are proposed. Besides, the reasonability of these recommendations is explained.

**Key words:** HIP; security; mobility; federalism; management infrastructure

## 1 概述

网络安全性、服务质量和移动性是当今互联网研究领域的三类关键问题。网络安全性是当今互联网研究和开发中最为核心的问题,如果互联网在安全技术的研究和开发方面没有根本的突破,互联网还是无法保证用户敏感数据的保密性、无法保证关键应用数据的完整性、无法保证重要网络应用的可用性,则当今的互联网将无法承担信息社会基础设施的重任。

网络服务质量是当今互联网研究和开发中最为关键的问题之一,如果互联网在网络服务质量保障技术

方面没有根本的突破,则用于语音传递的电话网和用于视频传递的电视网就无法融合到互联网中,三网融合就只能是一个梦想,人类社会依然无法进入到理想的信息社会,无法采用广泛地普及数据、语音和视频类的信息服务设施。

网络移动性是当今互联网研究和开发中的一个热点问题。如果互联网在网络移动技术方面没有根本的突破,则互联网就无法提供随时随地的信息服务,也就无法满足信息化社会对当前信息网络提出的不间断服务的需求。随着第四代移动通信网(4G)在国内的部

收稿日期:2014-09-24

修回日期:2014-12-29

网络出版时间:2015-07-21

基金项目:江苏省“未来网络前瞻性研究”项目课题(BY2013095-1-08);南京邮电大学自然科学基金(NY211115)

作者简介:毛燕琴(1981-),女,讲师,CCF 会员,研究方向为自主计算。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20150721.1448.050.html>

署以及相关业务在国内的开通,对于高效率网络移动技术的研究和开发逐步成为互联网中的关键问题之一。

1988 年因特网首次爆发网络蠕虫病毒,莫里斯蠕虫病毒<sup>[1]</sup>,使得计算机网络界的研究和开发人员才开始放弃了网络乌托邦的思想,逐步重视网络安全技术的研究和开发,才真正诞生了一批网络安全技术,例如网络防火墙技术。现在,网络防火墙已经成为构建计算机网络系统必不可少的部件,网络安全已成为计算机网络中的核心技术。虽然现在已经研究和开发了不同层次的网络防火墙,但是,网络蠕虫和网络攻击还是可以绕过防火墙袭击网络系统,网络安全问题并没有得到根本解决。网络安全的根本问题在于传统因特网的设计并没有把网络安全作为主要需求考虑<sup>[2]</sup>,本身造成了基于 TCP/IP 协议栈的互联网安全能力的缺失。

身份验证、访问控制和攻击检测构成了现代网络安全基本技术体系<sup>[3]</sup>,但是,基于 TCP/IP 协议栈的互联网本身缺少身份验证的功能。例如传统互联网主要通过 IP 地址标识和定位网络主机,而 IP 地址可以随意设置并且难以验证每个网络主机真实的 IP 地址。从当前互联网设计和实现机制看,网络主机是无法验证其身份真伪的,所以,所有基于网络主机的安全机制都是无法真正实施的。这也是目前网络安全无法得到突破性进展的关键难题之一。

网络服务质量也一直是计算机网络界十分热门的研究课题,这里涉及到网络的资源分配和调度问题,特别涉及到针对每个网络主机的网络资源分配和调度问题。虽然目前在专用的商业互联网上可以通过“区分服务+多协议标签交换(MPLS)”<sup>[4]</sup>获得服务质量保证,但是,在公共互联网上还是难以提供服务质量保证,因为在无法识别网络主机身份的公共互联网环境下,试图提供有区分的服务没有任何实用价值。

网络中的移动性问题包括主机移动性、会话移动性和用户移动性<sup>[5]</sup>。主机移动性是指到主机 IP 地址发生变化时,主机还可以被寻址和进行数据传递;会话移动性表示在不同端系统装置之间传递正在进行会话连接;而用户移动性表示无论用户处于什么位置,只要采用相同的用户标识符就可以获得相同的网络服务。随着无线局域网技术的发展,互联网中应用最广泛的是主机移动性管理技术。传统的网络主机缺乏移动能力的原因在于网络主机身份标识和网络主机位置标识的合一,即采用单一的 IP 地址同时标识网络主机身份和网络主机的位置。一旦网络主机移动,则 IP 地址必须变化,否则无法保持与网络的连通。但是,IP 地址的变化使得网络主机的标识也发生了变化,难以保持

网络主机标识的唯一性。这是当前互联网中影响网络主机移动性的根本原因。

计算机网络界针对网络的安全性和移动性提出了许多解决方案,其中具有一定代表性的是主机身份协议(HIP)<sup>[6-7]</sup>。它试图增加一个主机的身份标识,用于分离网络主机的身份标识(新建立的主机标识)和位置标识(原来主机的 IP 地址),从根本上解决网络的安全性和移动性问题。

## 2 HIP 协议基本特性

### 2.1 HIP 基本思路和组成

HIP 提出了一个新的名字空间“主机身份(Host Identify, HI)”用于标识主机,其具有全球唯一性,目前采用公私密钥对中的公钥作为主机身份。HIP 将主机的身份标识和位置标识(IP 地址)分离,便于提供移动性支持。同时,将公钥作为主机标识,易于解决相关的安全问题。

HIP 主要由名字空间(namespace)和 HIP 基本交换协议(HIP Base EXchange protocol, BEX)组成。目前 Internet 定义了两类名字空间,IP 地址和域名系统。HIP 定义了新的名字空间 HI,其具有全球唯一性,代表网络上任意一台主机的身份,替代目前采用 IP 地址标识主机的功能。HI 可以有很多定义形式,但目前使用公私密钥对中的公钥来表示主机身份。由于不同算法产生的公钥长度不一,为标识每个 HI,将 HI 进行 hash 运算得到固定 128 位长度的 HIT(Host Identify Tag),进而可以使用 HIT 标识主机身份。由于采用公钥来表示 HI,那么需要利用公钥基础设施提供密钥分发和管理的服务。虽然公钥是 HIP 协议的一个重要元素,但 HIP 协议本身并未考虑公钥相关的分发和管理问题。

HIP 协议是在数据交互之前,为通信双方主机快速交换 HI 值,建立 IPSec 安全关联(IPSec SA)。可以说 HIP 协议是一种端到端的身份验证和密钥建立协议,它可以与封装安全净荷协议(Encapsulated Security Payload, ESP)或其他端到端的安全协议结合使用。可以视为轻量级的互联网密钥交换协议(Internet Key Exchange, IKE)<sup>[8]</sup>,但不能替代 IKE,因为 HIP 不具备良好的策略控制机制。HIP 基本交换过程包含四个报文,报文交互设计能很好地抵御拒绝服务(Deny of Service, DoS)攻击,并且可提供基于公钥身份验证的密钥建立过程。

### 2.2 HIP 基本交换协议

HIP 通信分成两个阶段, HIP 基本交换和安全的传输。HIP 基本交换协议通过四个报文交互完成 HIP 关联(HIP association)的建立,为通信双方数据交

互建立了安全通道。其协议交互具体过程如图 1 所示。

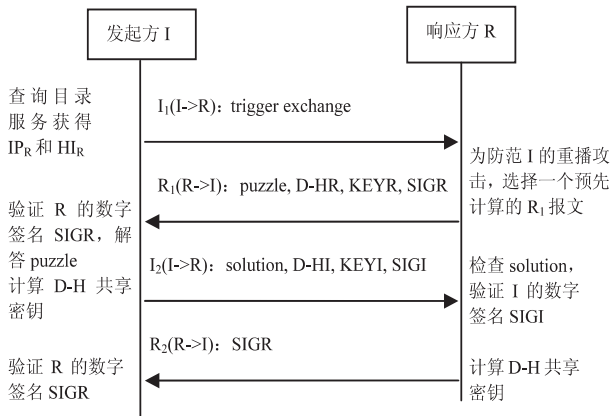


图 1 HIP 基本交换协议(BEX)过程

在 HIP 基本交换协议之前发起方 (Initiator, I) 需要查询目录服务 (如 DNS 或 LDAP), 获得对等响应方 (Response, R) 的 IP 地址 IP<sub>R</sub> 和主机身份 HI<sub>R</sub>。

(1) 发起方 I 首先发送 I<sub>1</sub> 报文, 触发 HIP 通信过程。

(2) 为防范发起方 I 的重播攻击, 选择一个相关参数预先计算好的 R<sub>1</sub> 报文返回给发起方 I。报文中包含了质问参数 puzzle, D-H 算法 R 方参数 D-H<sub>R</sub>, R 的公钥 KEY<sub>R</sub>, 以及相应的数字签名 SIG<sub>R</sub>。

(3) 发起方 I 验证响应方 R 的数字签名 SIG<sub>R</sub> 通过后, 解答难题 puzzle 获得 solution, 选择好 D-H 算法 I 方参数 D-H<sub>I</sub>, 发送 I<sub>2</sub> 报文给响应方 R。报文中包含了解答参数 solution, D-H 算法 I 方参数 D-H<sub>I</sub>, I 的公钥 KEY<sub>I</sub>, 以及相应的数字签名 SIG<sub>I</sub>。最后根据 D-H 算法、D-H<sub>I</sub>、D-H<sub>R</sub> 计算出双方的共享密钥。

(4) 响应方 R 检查 solution, 验证 I 的数字签名 SIG<sub>I</sub> 通过后发送 R<sub>2</sub> 报文给发起方 I。报文中包含 R 方的数字签名 SIG<sub>R</sub>。最后根据 D-H 算法、D-H<sub>I</sub>、D-H<sub>R</sub> 计算出双方的共享密钥。

分析 HIP 基本交换协议, 可以看出四轮握手和报文交互提供了 puzzle 机制、基于身份验证的 Diffie-Hellman 协议、HIP 重播保护机制等安全功能, 可以防范拒绝服务、身份假冒和重播等攻击。

HIP 协议位于传输层和网络层之间<sup>[8]</sup>, IANA (Internet Assigned Numbers Authority) 分配 139 作为 HIP 协议。HIP 报文格式如图 2 所示。

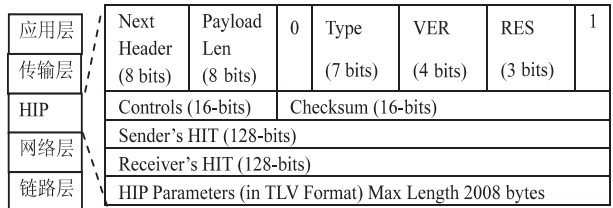


图 2 HIP 报文格式

### 3 HIP 在安全中的应用

HIP 协议的设计可以较好地抵御服务拒绝攻击、重播报文攻击和身份假冒攻击。借助基于公钥密码表示的主机标识符所提供的自验证能力, 可以基于 HIT 建立一对 IPsec 安全关联 (IPsec SA), 结合安全传输协议 (如 ESP 协议<sup>[9]</sup>), 提供端到端的安全服务。由于 SA 通过安全策略索引 (SPI) 和 HIT 进行检索, 而不再关联 IP 地址。因而, 主机可自由地通过 MIP 和 DHCP 等协议更改 IP 地址, 但安全关联 SA 不受影响。

此外, 为了满足受限网络 (如传感网) 环境对安全的需要, 针对计算能力和存储能力有限的传感设备之间的安全通信, 文献[10]提出了基本交换协议 BEX 的改进协议—节能交换协议 (HIP Diet EXchange, DEX), 通过省略公钥数字签名和哈希签名来降低加密数据负荷。在此基础上, 文献[11]提出了压缩 DEX 协议数据的压缩层以适应于物联网环境, 降低网络数据传输负荷。

除了结合端到端的安全协议, 提供安全关联的建立功能外, HIP 还可以在 P2P 网络环境下为多媒体通信系统提供强安全性和良好的连接性<sup>[12]</sup>。

### 4 HIP 在移动性管理中的应用

目前存在三类移动性问题<sup>[5]</sup>, 即用户移动、会话移动、主机移动。用户移动是指无论用户的位置何在, 都可以通过相同的用户标识访问到该用户。会话移动是指当前会话在不同的设备间切换。主机移动发生在主机更换 IP 地址。

针对不同类别的移动, 目前存在很多移动管理协议来提供相应的移动管理服务。现有的移动管理协议可以分为三类<sup>[13]</sup>: 高层协议、中间层协议、低层协议。其协议层次结构如图 3 所示。

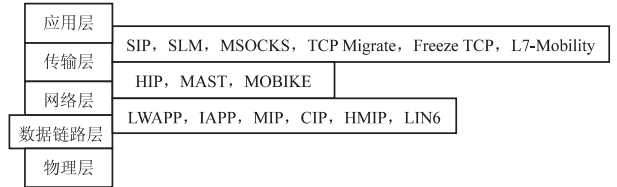


图 3 移动性管理协议分类

高层移动管理协议主要解决会话移动管理, 低层移动管理协议解决设备移动管理, 中间层移动管理协议解决高层协议和低层协议的松耦合性问题, 将会话的切换和设备的移动之间的关联透明化, 保证下层的移动不影响上层应用会话的服务质量。不同层次的移动管理协议各有所长, 为提供一套完整的松耦合的移动使能协议栈。文献[13]提出跨层的移动管理协议联合, 通过绑定不同层次的移动管理协议所涉及的对象标识, 满足自下而上的移动服务需求。



除提供安全应用外,HIP 协议扩展<sup>[14]</sup>可以提供主机移动管理能力。目前应用会话由二元组<IP,socket>标识,当主机发生移动,其位置标识(IP 地址)发生改变,因为 IP 地址作为会话的一个标识参数,那么节点的跨网移动必然会对上层应用产生影响。如果会话绑定的是 HI 而非 IP,无论节点进行跨网的移动还是多归属主机更换网络通信接口,都不会影响上层会话的通信。主机所对应的 IP 地址如发生变化,HIP 协议通过发送 update 报文及时通告通信对方,以实现主机移动管理功能。在 IP 网络环境下,MIP、Migrate 和 HIP 协议都支持主机移动管理,在文献[15]对它们的性能、安全性、部署、可伸缩性和鲁棒性进行了比较。

但 HIP 协议自身并不能区分上层会话标识,无法实现会话在不同主机上的迁移<sup>[5]</sup>以提供会话移动管理能力。在文献[13]中提出,为解决会话在不同主机上的切换,结合会话层移动(SLM)协议以及 HIP 协议,定义新的三元组<EPID,HI,IP>分别标识会话、主机、位置,完成会话的移动性管理。

此外,HIP 协议自身也不能提供用户移动管理能力。而 SIP 协议具有良好的会话移动管理和用户移动管理能力,可以将 SIP 协议和 HIP 协议组合,提出一种全面的移动管理框架<sup>[5]</sup>。充分利用 HIP 协议的安全、移动、多归属等特性,将其作为一种传输机制,为基于 SIP 的应用服务提供安全等扩展能力,并且为 P2P SIP 系统提供标识和安全方面的便利。

## 5 部署和应用方面的不足

HIP 协议提出了一个很好的思路,把公钥加密体系中的公钥作为主机的身份,使得主机的身份标识具备了验证主机身份真伪的能力。建立这种具有验证真伪能力的主机身份标识符确实是解决当今网络安全问题的关键环节。

同时,HIP 分离了网络主机身份标识和位置标识,使得上层应用建立的应用连接(例如 TCP 连接)或者应用会话(例如 SIP 会话)只需要采用“主机身份标识+端口号”绑定主机身份标识,而不需要采用传统“IP 地址+端口号”的传送层地址绑定 IP 地址。这样,使得上层应用可以直接依赖于主机标识进行应用层交互,主机位置的变化将不再影响应用层数据传递,使得网络主机移动处理可以仅仅局限在网络层处理,这将提高主机移动性处理的效率,可以设计更加有效的网络主机移动技术方案。

目前 IETF 发布的有关 HIP 体系结构的定义<sup>[6]</sup>和 HIP 协议的规范<sup>[7]</sup>,仅仅作为一类参考信息或实验协议。这说明 HIP 虽然提供了一个很好地解决网络安全和移动性的设计思路,但是,HIP 本身的研究和开发尚

未完善。IRTF(互联网指导工作组)针对 HIP 提出了一系列问题<sup>[6]</sup>,例如 HIP 放在协议栈的哪里?HI 的生命期?如何在端点上应用?是否需要建立管理的基础设施?什么是 HI 的解答机制?这些问题都是 HIP 协议目前尚未充分和完整研究的问题。从实际 HIP 的部署和应用角度看,HIP 的管理基础设施的构建以及 HIP 完整协议簇的构建将是两个致命的不足。

### 5.1 缺乏管理基础设施

目前定义的 HIP 是基于公钥密码体系产生的身份标识,而公钥密码体系需要一个公钥基础设施(PKI)<sup>[16]</sup>的支撑。PKI 又是一种构建成本极高的基础设施,它可以作为现代信息社会信用管理体系的一种具体实现,一般由值得信赖的、由政府管理的权威机构建设和运行。

HIP 体系结构及其协议定义中没有提到专门用于 HIP 的 PKI 设施的构建和管理,建议采用通用的 PKI 基础设施,或者通过域名服务器(DNS)实现 HIP 的基础设施管理。通用的 PKI 构建成本太高,而 DNS 并不具备 PKI 的安全特征,如果需要提升 DNS 的安全能力,则 DNS 构建的成本也会快速增长,这是需要在定义和规范 HIP 中仔细考虑而又没有考虑的内容,这是 HIP 研究和开发不完善的具体表现。

因为 HIP 是解决网络安全性和移动性的一种重要技术,它应该在全网部署和运行。从理论上讲,这种部署和运行需要伴随着 PKI 的部署和运行,其部署和运行的成本不是一般规模网络运营商或者一般规模的机构能够承受的,这样会极大地限制 HIP 技术的部署和应用。文中将在第 6 节提出一个解决方案,使得 HIP 摆脱全网 PKI 的制约。

### 5.2 缺乏完整的协议簇

HIP 协议重新定义了主机身份标识,这种主机身份标识需要与主机的位置标识(IP 地址)、主机全局资源标识(URI)等已有的主机标识相互绑定,才能真正投入应用。目前 HIP 试图通过 DNS 解析主机对应的主机标识和 IP 地址,这是一个理想化的处理方式。目前互联网上的绝大多数主机并没有在 DNS 上注册,仅仅利用 DNS 完成 HIP 相关信息的解析,这是难以满足应用需要的。

从实际网络部署和应用角度看,HIP 应该提供一个完整的 HI 层,其中包括一个完整的 HIP 协议簇,实现 HI 与主机相关标识信息的绑定和查询的管理。下一节将提出一个解决方案,使得 HIP 具备一个完整的协议簇。

## 6 改进建议

为了弥补目前 IETF 发布的 HIP 体系结构及其协

议的不足,有两类改进方案:采用联邦制身份体系解决 HIP 管理基础设施方面的不足,采用一个主机身份层解决 HIP 完整协议簇方面的不足。

### 6.1 基于联邦制身份体系的 HIP

为了弥补 HIP 在管理基础设施方面的不足,建议采用联邦制身份体系建立 HIP 协议。这种联邦制身份体系与目前因特网互连结构类似,首先是各个管理域内部依赖于主机特征值建立一个可验证的标识符,由各个管理域负责主机标识的验证;各个管理域之间通过信任管理的交互,实现跨管理域的主机身份验证。

### 6.2 主机身份层的完整协议簇

为了弥补 HIP 在完整协议簇方面的不足,建议 HIP 必须构成一个协议簇,形成一个 HI 层。在 HI 层必须包括主机身份验证协议(HIA),可以用于传递主机标识、验证主机身份真伪;主机身份查询协议(HIQ),用于通过主机特征参数查询主机身份,通过主机标识符查询 IP 地址;主机标识管理协议(HIM),用于建立主机标识空间,添加、删除和更改主机标识符,建立主机标识符与主机接口 IP 地址的对应关系。

## 7 结束语

IETF 发布的 HIP 体系结构和协议为互联网协议增加了两个主要特色功能<sup>[6]</sup>:其一是耦合网络互连层与传送层;其二是主机身份验证。第一个特色功能使得互联网协议栈可以支持主机移动性;第二个特色功能使得互联网协议栈可以支持主机身份验证,便于建立一个可信网络。这两个特色功能还可以结合起来,提供移动网络环境下的安全功能。所以,HIP 是一个有可能从根本上解决网络安全性和移动性问题的解决方案。


但是,目前 IETF 发布的 HIP 体系结构及其协议既缺乏管理基础设施,又缺乏完整的协议簇,尚无法在现有的互联网直接部署和应用。文中提出了一个 HIP 的改进建议,试图采用联邦制身份体系解决 HIP 管理基础设施方面的不足,采用一个主机身份层解决 HIP 完整协议簇方面的不足。

互联网中的安全性、服务质量和移动性问题都是涉及到网络体系结构的问题,根本上解决这些问题必然会涉及到网络体系结构的变动。同样,进一步完善 HIP 的研究和开发必然会涉及到互联网体系结构的更改,所以,HIP 可以作为未来互联网研究和开发的一个关键技术,值得深入研究和探索。

## 参考文献:

- [1] Orman H. The Morris worm: a fifteen-year perspective[J]. IEEE Security & Privacy, 2003, 1(5): 35-43.
- [2] Clark D C. The design philosophy of the DARPA Internet protocols[J]. Computer Communications Review, 1988, 18(4): 106-114.
- [3] 沈苏彬. 网络安全原理与应用[M]. 北京:人民邮电出版社, 2005.
- [4] Faucheur F L, Wu L, Davie B, et al. Multi-Protocol Label Switching (MPLS) support of differentiated services[S]. [s. l.]: IETF, 2002.
- [5] Camarillo G, Mas I, Nikander P. A framework to combine the session initiation protocol and the host identity protocol[C]//Proc of IEEE wireless communications and networking conference. [s. l.]: [s. n.], 2008: 3051-3056.
- [6] Moskowitz R, Nikander P. Host Identity Protocol (HIP) architecture[S]. [s. l.]: IETF, 2006.
- [7] Moskowitz R, Heer T, Jokela P, et al. Host Identity Protocol Version 2 (HIPv2)[S]. [s. l.]: IETF, 2014.
- [8] Al-Shraideh F. Host identity protocol[C]//Proc of international conference on systems and mobile communications and learning technologies, and networking. [s. l.]: [s. n.], 2006: 203-203.
- [9] Jokela P, Moskowitz R, Nikander P. Using the Encapsulating Security Payload (ESP) transport format with the Host Identity Protocol (HIP)[S]. [s. l.]: IETF, 2008.
- [10] Moskowitz R, Hummen R. HIP Diet EXchange (DEX)[S]. [s. l.]: IETF, 2014.
- [11] Hummen R, Hiller J, Henze M, et al. Slimfit—a HIP DEX compression layer for the IP-based Internet of things[C]//Proc of IEEE 9th international conference on wireless and mobile computing, networking and communications. [s. l.]: IEEE, 2013: 259-266.
- [12] Koskela J. A HIP-based peer-to-peer communication system [C]//Proc of international conference on telecommunications. [s. l.]: [s. n.], 2008: 1-7.
- [13] Nazir F, Boreli R, Herborn S, et al. A case study for mobility management protocol co-existence[C]//Proc of IWCLD'07. [s. l.]: [s. n.], 2007: 141-151.
- [14] Nikander P, Henderson T, Vogt C, et al. End-host mobility and multihoming with the host identity protocol[S]. [s. l.]: IETF, 2008.
- [15] Henderson T R. Host mobility for IP networks: a comparison [J]. IEEE Network, 2003, 17(6): 18-26.
- [16] Gutmann P. PKI: it's not dead, just resting[J]. Computer, 2002, 35(8): 41-49.

# 支持安全性和移动性的主机身份协议研究

作者：[毛燕琴](#)，[MAO Yan-qin](#)  
作者单位：[南京邮电大学 计算机学院, 江苏 南京, 210003](#)  
刊名：[计算机技术与发展](#)  
英文刊名：[Computer Technology and Development](#)  
年，卷(期)：2015(8)

引用本文格式：[毛燕琴](#), [MAO Yan-qin](#) [支持安全性和移动性的主机身份协议研究](#)[期刊论文]-[计算机技术与发展](#)  
2015(8)