doi:10.3969/j.issn.1000-436x.2012.z2.039

HIPSCS：基于 HIP 的安全 IP 通信系统

周敏，陈鸣，邢长友，蒋培成
(中国人民解放军理工大学 指挥信息系统学院，江苏 南京 210007)

摘 要：针对主机标识协议(HIP, host identity protocol)实际部署应用的相关问题，设计实现了一种基于 HIP 的安全 IP 通信系统(HIPSCS, HIP based secure communication system)。该系统通过将主机标识(HI, host identifier)和用户身份证书唯一关联，实现了主机身份的实名化，以保障网络报文的源地址真实可信，并通过 IPsec 技术加密所有通信数据以达到安全通信目的。实现并在实验室环境中部署了 HIPSCS 原型系统。实验表明此通信系统可用性强，并能很好地支持移动通信。

关键词：主机标识协议；安全；通信系统；原型系统
中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2012)Z2-0270-06

HIPSCS: secure IP communication system based on HIP

ZHOU Min, CHEN Ming, XING Chang-you, JIANG Pei-cheng
(Institute of Command Information System, PLA University of Science and Technology, Nanjing 210007, China)

Abstract: To make the host identity protocol(HIP) into practical use, a secure communication system basd on HIP named HIPSCS was designed and implemented. HIPSCS achieved the real-name identification of communications hosts by binding the HI with user's certificates, thus made the source of packets trustworthy from network. IPsec was used to encrypt communication data, so that the goal of secure IP communication was accomplished. The HIPSCS prototype was implemented in the laboratory environment, and experimental results show that HIPSCS has good usability and can support mobile communication well.

Key words: host identity protocol; secure; communication system; prototype

1 引言

在因特网设计之初假设网络节点是固定可信的，IP 地址即作为节点的身份标识符，又作为定位寻址符。然而，将 IP 地址作为标识符对网络实体身份进行鉴别并没有实际意义，因为 IP 分组中几乎所有字段都可以被入侵者伪造[1]。为此，由 IETF 提出的主机标识协议(HIP, host identity protocol)通过引入主机标识符，使 IP 地址仅具有节点定位寻址符的作用，从根本上解决了主机标识动态变化的问题[2]。具体而言，HIP 通过引入一个主机标识符(HI, host identifier)命名空间与通信节点一一对应，而将 IP 地址只作为定位寻址符使用。在实现中通过引入 128bit 的主机标识标签(HIT, host identity tag)在具体报文交互中代表 HI 作为主机的标识符。由于 HIP 使用公钥密码体制中的公钥作为可信用户的 HI，这样，用户就能方便地鉴别其身份，提高了 IP 通信的安全性。HIP 使得 IP 地址回归到节点定位符的地位，

收稿日期：2012-10-24
基金项目：国家重点基础研究发展计划(“973”计划)基金资助项目(2012CB315806)；国家自然科学基金资助项目(61070173, 61103225)
Foundation Items: The National Basic Research Program of China (973 Program) (2012CB315806); The National Natural Science Foundation of China (61070173, 61103225)

这对于 IP 通信特别是移动通信非常有益。保持节点的身份标识符不变，而节点的 IP 地址随着节点漫游的需要发生相应变化，能够在保证安全性的前提下降低移动通信的实现难度[3]。近年来，世界上各相关组织和机构持续进行了 HIP 协议的完善工作，HIP 的设计与开发取得了长足的进步。

然而，将 HIP 协议付诸实施，还有一些技术问题需要研究解决。首先，HI 命名空间需要管理机制，以保证通信节点身份来源可靠。文献[4]提出为用户分配用户标识符(UI)作为用户身份标识并与主机标识相关联。这种机制便于实现，但是扩展性不强，只适用于在小规模局域网。文献[5]提出了采用 HIP 协议实现网络层实名认证机制，但是其证书认证机制的引入破坏了 HIP 协议抵抗 DoS 攻击的能力。IETF 于 2011 年 3 月发布的草案指出了在 HIP 中实现网络实名认证需要注意的问题，规范了在 HIP 协议中的证书格式，但是实名认证实现方案的细节仍需讨论[6]。

针对 HIP 实际部署应用的问题，本文提出了基于公钥架构(PKI, public key infrastructure)[6]管理 HI 的方案，设计实现了一种基于 HIP 的安全通信系统(HIPSCS, HIP based secure communication system)。HIPSCS 先将主机的网络标识与用户身份唯一关联，实现了主机身份的实名化和全局性管理，然后基于 HIP 保证了 IP 报文的安全通信。为了验证 HIPSCS 的设计，本文编制了程序，并搭建了无线实验环境对原型系统进行了测试。

2　基于 HIP 的安全 IP 通信系统 HIPSCS

2.1　HIPSCS 的基本工作过程

PKI 是一种基于公钥密码体制的安全基础设施。它是用来实现证书的产生、管理、存储、发行和撤销等功能的安全平台，使用户可以在多种应用环境下方便地使用加密和数字签名技术，从而保证网上数据的机密性、完整性和不可抵赖性。本文引入 PKI 机制，对主机 HI 进行管理，便于实现 HIP 协议在大规模网络中应用。首先，在 HIP 协议中，没有建立 HI 和主机直接的真实对应关系。通信双方的认证过程只能验证对方是特定 HI 相对应私钥的持有者，而对方具体身份仍然不明确。引入 PKI 机制后，可通过证书绑定 HI 和主机的真实信息，真正达到实名访问的目的。其次，PKI 系统可有效处理主机密钥对的产生、发放、管理、查询、废止和更改等问题。通过在 PKI 中生成并注册 HI 公钥，确保主体唯一性和防止重名。因此，PKI 机制的引入实现了全网范围主机通信过程中身份的认证，使得 HIP 协议适用于大规模网络。图 1 给出了在大规模网络环境下一种基于 HIP 的安全通信系统的工作过程。

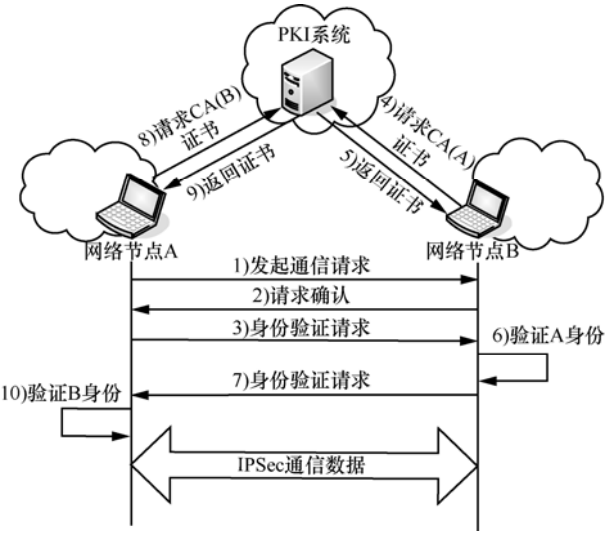

图 1　HIPSCS 移动通信流程

图 1 中 PKI 系统主要包括了用户证书发放机构(CA)以及证书和用户信息的管理机构。未获得 PKI 系统颁发证书的主机，无法接入网络。PKI 系统的实现方式将在第 3.1 节中具体描述。图 1 中若节点 A 试图向节点 B 发起通话，首先要根据 HIP 协议发送通信请求报文，并等待节点 B 的请求确认报文。之后，将自己的证书信息发送给节点 B，请求 B 对其进行身份验证。节点 B 从收到的证书中获取为节点 A 颁布证书的 CA(A)信息，并利用此 CA 的公钥对网络节点 A 的证书进行验证。验证通过后节点 B 向节点 A 发送自己的证书信息，节点 A 通过类似的步骤对节点 B 的身份进行验证。图中第 2)、3)步中节点 A 和 B 之间的交互还包括密钥协商等过程，具体细节见第 3.3 节中描述。双方验证通过后，创建安全连接，记录对方 HI 和 IP 的映射信息，之后便能采用 IPSec 方式开始通信[8]。

PKI 机制的引入，使得网络中的数据分组源地址都真实存在并与物理实体一一对应，能够快速方便地定位网络的任何攻击和入侵行为，为上层应用提供安全保障。另外，由于安全关联由 HI 标识，不随主机的移动而改变，移动终端 IP 改变时只需直接发送 IP 更新报文，告知服务器修改 HI 和 IP

之间的映射即可，极大地降低了传统 IPsec 移动通信模式中重新建立安全关联带来的时间和系统处理开销[9]，带来了较好的移动性能。

2.2　HIPSCS 的功能模块

在 Linux 2.6 操作系统中，基于 HIPL 1.0.6[10] 工作的基础，设计并实现了 HIPSCS 体系结构。具体而言，修改了 HIPL 初始化模块以获取本地网管发布的证书及密钥，并设计了实名证书认证模块完成通信双方的证书认证过程，其功能模块如图 2 所示。

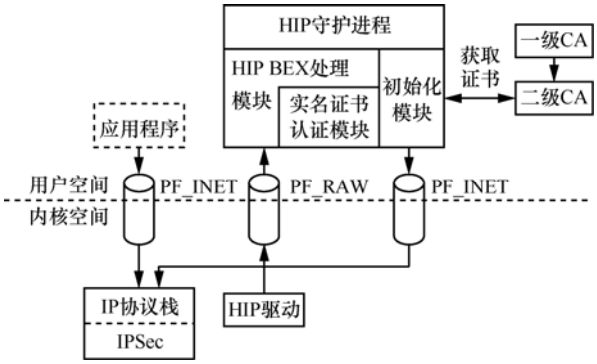

图 2　HIPSCS 体系结构

原 HIPL 协议结构中，用户空间的应用程序通过 PF_INET 选项调用内核空间的 IP 协议栈构造 IP 报文并发送，HIP 守护进程中初始化模块的监听进程将截获此 IP 报文，同时 HIP 驱动模块通过 PF_RAW 选项创建原始套接字构造 HIP 报文，供 HIP BEX 模块完成通信双方 4 次握手的自检验过程。若双方认证成功，便构造 IPsec 报文开始通信，否则丢弃报文不进行通信。

为实现基于 HIP 的网络实名通信，首先对主机 HIT 生成方法进行改进以方便管理，基于 openssl 库函数[11]设计实现了 CA 机制，并在 HIP 初始化模块中读入证书信息和密钥信息。在详细分析 HIP 协议和 HIPL 代码的基础上，在 HIP BEX 处理模块中实现了证书信息携带和证书验证的功能，实现通信双方身份的可信认证。

3　HIPSCS 实现中的关键技术

3.1　便于管理的主机标识标签生成算法

扩展的数字证书发布过程如下：用户将有效身份证件标识等个人身份信息传送至本地网管。本地网管核实用户的身份并为用户生成密钥及身份标识。若该标识未被使用，且验证身份字符串与用户真实身份证件一致，则通过 CA 为用户签发数字证书。证书中附加有主机标识、密钥对、用户基本身份以及该认证中心的标识符等信息。

根据 HIPSCS 需求，为实现网络可管可控目标，本文设计本地网管负责用户的入网申请，实现客户端密钥对、主机标识标签(HIT)的统一生成工作。原始 HIP 协议中采用直接对 HI 进行 hash 产生 HIT[2]，标识空间扁平难以管理。本文对 HIP 协议 HIT 的生成做了改进，使用以下便于管理的层次化 HIT 生成算法[12]。

算法 1　主机密钥及 HIT 产生算法

输入：用户身份信息

输出：主机实名标识

1)　生成 128 bit 随机数种子。

2)　采用 RSA 算法生成用户公私钥。

3)　连接随机数，地址分配机构 64 bit 前缀、身份号码字符串和公钥，利用 SHA-1 散列算法得到 160 bit 散列值，取最左边 64 bit 为 Hash2。

4)　组合地址分配机构 64 bit 前缀和 64 bit Hash2 成为一个与用户身份对应的有效主机实名标识 HIT。

5)　验证此 HIT 是否已被使用，若被使用，将随机数加 1，转 3),否则该结果即分配为用户的 HIT。

图 3　主机密钥及 HIT 生成算法

该算法将 HIT 划分为 2 级层次化结构，前 64bit 为用户所在域的域标识，后 64bit 代表用户的域内标识。与原始 HIP 协议的 HIT 计算方法相比，采用此算法与现有层次结构的 IP 地址相似，便于对 HIT 的分级管理。由于 HIT 和 IPv6 格式相同，本文将 HIT 的最高 2 位设置为 01 或 10，以和当前 IPv6 地址进行区分。

3.2　用户证书分发方法

CA 按照以上流程生成密钥对和 HIT 之后，调用 openssl 工具使用自己的公钥为用户生成证书。完成之后，USBKey 中存放着主机私钥 host_rsa_key_pub、公钥 host_rsa_key_pub.pub、证书 host-cert.pem 和 CA 证书 ca-cert.pem 文件。在实际应用中，要保护密钥的安全，最好的办法是采用具有处理器的 USBKey 技术[13]，将密钥工作在 USBKey 内部进行，密钥不会被读入到计算机的硬盘或内存中，有效地保护了主机私钥安全。在实验室受限制的环境下，使用普通 U 盘，在 ini.c 中添加代码将信息读入到缓存区中进行通信。另外，为解决大规模网络中证书管理复杂的问题，可采用多级 CA 的方式进行证书的发布[14]。

3.3　可信身份认证的扩展 4 次握手过程

在 HIP BEX 处理模块中进行 HIP 4 次握手的扩展关键在于证书信息在何时机以何种方式携带。文献[6]中在 I1 和 R1 报文中携带证书信息，这样响应方在 R1 阶段就需耗费资源保持通信状态，若发起方频繁发送 I1 报文且不回应对方的 R2 报文，响应方很容易耗尽资源甚至崩溃。为防止以上 DoS 攻击，在 I2 和 R2 阶段携带证书信息。

对 HIP 协议的基本 4 次握手交换过程进行扩展，构建具有可信身份认证功能的扩展 4 次握手认证携带信息如图 4 所示。

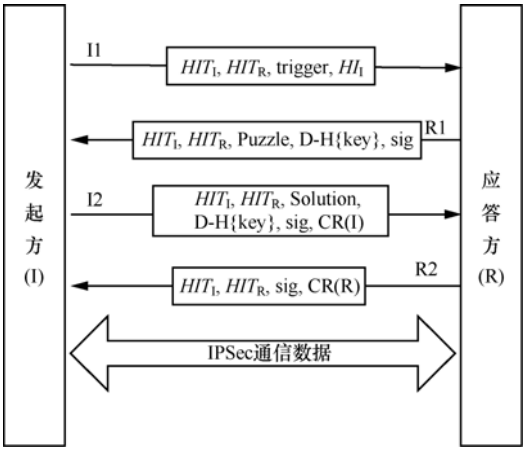

图 4　扩展的 HIP 4 次握手过程

在 PKI 机制管理下，为了互相认证彼此的身份，两者交互过程如下。

1) 发起方发送 I1 报文，请求安全连接建立。

2) 应答方根据发起方的公钥构造谜题要求发起方解答，并附带 DH 半会话密钥构造 R2 发送至发起方。

3) 发起方在 I2 报文中附带自己的实名标识证书信息和谜题答案并发送。

4) 响应方收到 I2 后，首先验证收到的实名证书和数据签名，然后对发起方给出的谜题答案进行验证。如果正确，使用根证书验证对方证书的有效性。若验证未通过，则响应方拒绝和发起方通信。否则，解密发起方的 DH 半会话密钥，计算得出 DH 会话密钥，创建进行 IPsec 通信使用的安全关联 SPI，构造 R2 报文附带自己的证书发送给发起方。

5) 发起方收到 R2 后，通过证书验证对方的身份。若验证未通过，则响应方拒绝和发起方通信。否则，创建安全关联开始通信。

由于发起方在 I2 阶段携带证书信息，应答方在发送 R1 阶段不必为发起方分配资源维护通信状态，又因为发起方在 I2 阶段耗费与应答方的 R2 阶段相当的代价，因此发起方频繁发送连接请求报文也不会对应答方造成 DoS 攻击。以上将证书信息携带在 I2 和 R2 报文的方式很好地保持了 HIP 协议的原有优点，优于文献[6]中的方式。

以上过程能有效保障通信节点的安全性，但是可能带来的问题是计算耗费较大，影响手持终端的性能。针对此问题可以通过利用未来网络中智能化的网络设备来解决。例如通过 OpenFlow 的控制器，对节点证书进行一次验证后，才允许其接入网络，之后不再需要节点与每个通信节点进行验证，从而降低了移动节点的开销，并带来更好的移动性能[15]。

为保证协议的可扩展性和避免扩展首部过长带来的麻烦，通过在 I2 或 R2 的数据字段携带证书信息，主要包括证书长度和证书实体 2 个部分。

HIPL 代码中/hipd/output.c 的 hip_create_i2()和 hip_create_r2()函数实现了 I2 和 R2 报文的构造，具体包括调用 hip_build_network_hdr()完成网络层报头和密钥计算等步骤。通过指针 cxt 实现证书信息的写入，构造携带证书信息的 I2 或 R2 报文。

在/hipd/input.c 中 hip_handle_r2()和 hip_handle_i2()函数分别实现了接收到对方发送的 R2 和 I2 报文时的处理。首先调用/lib/core/Builder.c 中的 hip_get_param()函数将报文中的证书信息写入结构体，并调用 d2i_x509()函数将其转换为 x509 的证书格式。最后调用 X509_verify_cert()完成对证书的验证。

4　实验验证

根据以上研究和设计，在实验室环境下部署了基于 HIPSCS 的安全 IP 通信系统原型，如图 5 所示。

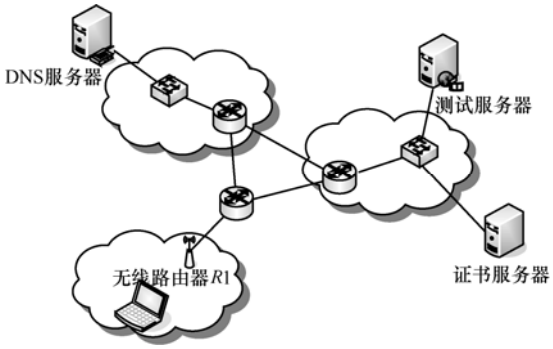

图 5　实验环境

实验环境由 3 台服务器和 1 台移动终端构成。服务器的 CPU 均为主频 2.4GHz 的 Intel Core I5，并运行 Linux(Fedora 16)操作系统，实验便携机的 CPU 为主频 2.4GHz 的 Intel Core I5，运行 Linux(Centos 6)操作系统。其中，证书服务器作为本单位 CA 为主机提供密钥对、HIT 及证书的生成和分配工作；测试服务器作为通信响应方为用户提供各种基于 HIP 的服务；DNS 提供主机域名、HIT 和 IP 地址之间的解析服务；其中移动终端采用 Wi-Fi 协议与测试服务器通信，以对安全 IP 通信机制进行验证，以上各主机均通过在内核编译 HIPSCS 协议将主机标识层加入 TCP/IP 协议栈。各主机的具体配置信息如表 1 所示。

表 1　　主机地址配置信息

主机	主机标识符 HIT	IP
DNS 服务器	2001:0012:e2a4:41b9:eb7d:87f7:44c4:58a7	10.2.0.8/24
测试服务器	2001:0015:e035:1818:4aca:5e0c:b368:079e	10.3.0.8/24
移动主机	2001:0019:1573:e04e:c683:3177:3562:7c55	10.1.0.8/24

本实验环境中，引入证书服务器集中产生主机密钥对、HIT 和证书，并通过 USBKey 形式保证密钥信息由本人所持有。因此真实主机身份与 HI 之间唯一对应，网络攻击者若想冒充通信双方中某一方的身份，需同时伪造其 HIT 值、公私钥、CA 颁发的证书和当前通信 IP 地址才可能完成一次网络攻击，在现有密码算法机制下，要实现这些假冒过程几乎是不可能的，从而有效地避免了假冒攻击、中间人攻击等多种网络攻击。

为测试本系统对网络通信时延产生的影响，笔者对安全 IP 通信中安全连接建立过程产生的时延进行统计计算，各阶段所需时间以及在整个安全连接建立过程中所占比例如表 2 所示。其中，发送 I1 开销为发起方构造一个 I1 报文并发送出去所需的时间，响应开销为响应端收到某个握手报文后，进行解析并构造相应响应报文直至发送出去所需时间。总开销包含了在主机对报文的处理以及报文在网络中传输 2 部分开销，因此比 4 部分之和要大。从统计结果可见，总开销为毫秒级，不会影响网络性能。

进一步，从测试服务器向便携机发送不同长度的文件，并计算从文件发送到正确接收的时延。图 6 中实线表示本文实现的 HIPSCS 通信协议下的文件传输时延开销，其中不包含通信双方 4 次握手的安全连接过程，虚线表示相同情况下传统 IP 网络的时延开销，图 6 中是执行了 10 次实验的平均情况。

表 2　　4 次握手时延性能

项目	发送 I1 开销	发送 R1 开销	发送 I2 开销	发送 R2 开销	总开销
时间/ms	<0.35	<0.75	<21	<20	<50
所占比例	0.7%	1.5%	42%	40%	100%

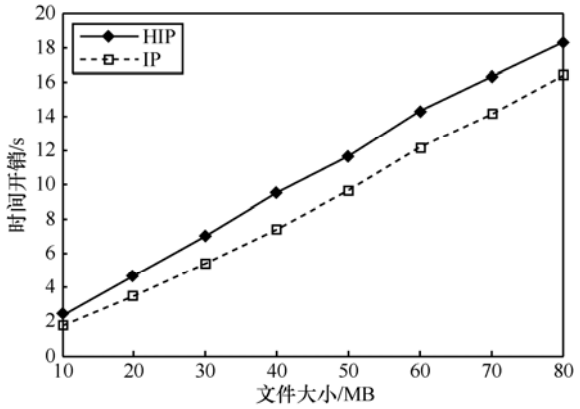

图 6　文件传输时延

可以看出，HIPSCS 的时延随着传输文件的大小基本呈线性增加。例如，当文件长度为 10MB 时，HIP 传输的时间约为 2.35s，传统 IP 传输时间约为 1.74s；当文件长度为 80MB 时，HIP 的传输时间约为 18.32s，传统 IP 的传输时间约为 16.31s。HIPSCS 比传统 IP 网络消耗的时间要长，主要是由于 HIP 通信要对数据进行 ESP 封装，由以上统计数据可以看出这部分时间不会对网络性能产生较大影响。因此，HIPSCS 协议适合在现有网络中部署。

5　结束语

为研究 HIP 协议的实名认证机制和在现实中对移动 IP 的支持能力，对在 HIP 中添加 PKI 机制的方法做了深入研究，设计并实现了一种基于 HIP 的双向认证机制。在实验室条件下，设计了一个网络层的实名认证通信系统原型，证明 HIP 协议在未来网络中应用的可能性。实验结果证明 HIP 协议能够有效保证网络层的安全可信通信，尤其是较好地解决了移动通信的问题，并有较高的可用性。下一步将在 HIPSCS 实现网络实名认证的基础上，探讨利用实名 IP 机制更有效地保护网络资源，保证上层通信安全的方法。

参考文献：

[1] LEINER B M, CERF V G, CLARK D D, *et al.* A brief history of the Internet[J]. ACM SIGCOMM Computer Communication Review, 2009, 39(5):22-31.

[2] RFC 4423.Host Identity Protocol(HIP)Architecture[S].IETF,2006.

[3] NIKANDER P. The host identity protocol (HIP): bringing mobility, multi- homing, and baseline security together[A]. Security and Privacy in Communications Networks and the Workshops[C]. Nice, France, 2007. 518-519.

[4] BARISCH M, MATOS A. Integrating user identity management systems with the host identity protocol[J]. Computers and Communications, 2009, 830-836.

[5] KARVONEN K， KOMU M. Usable security management with host identity protocol[J]. Computer Systems and Applications, 2009, 830-836.

[6] BARBER R. Implementing public key infraseructures in a dynamic business environment[J]. Computers & Security, 2000, 19(20):230-233.

[7] RFC 6253. Host Identity Protocol Certificates[S]. IETF,2011.

[8] RFC 5202.Using the Encapsulating Security Payload(ESP) Transport Format with the Host Identity Rotocol(HIP)[S]. IETF, 2008.

[9] RFC 4303. IP Encapsulating Security Payload (ESP)[S]. IETF, 2005.

[10] KOMU M, Application programming interfaces for the host identity protocol[EB/OL]. http://infrahip.hiit.fi/hip-native-api-final.pdf, 2004.

[11] 王志海,童新海,沈寒辉. OpenSSL 与网络信息安全—基础、结构和指令[M].北京:清华大学出版社,2009.
WANG Z H, TONG X H, SHEN H H. OpenSSL and Network Information Security-Basis, Structure and Structure[M]. Beijing:Tsinghua University Press,2009.

[12] 陈涛, 罗万明, 阎保平. 基于 IPv6 实名地址的可信通信机制[J]. 计算机工程, 2010, 36(19):11-14.
CHEN T, LUO W M, YAN B P. Trustworthy communication mechanism based on IPv6 real-name address[J]. Computer Engineering, 2010, 36(19):11-14.

[13] SHEN J J, LIN C W, HWANG M S. A modified remote user authentication scheme using smart cards[J]. IEEE Trans on Consumer Electron, 2003,49(2):414-416.

[14] NIELSEN R, HAMILTON B. Observations from the deployment of a large scale PKI[A]. Proceedings of 4th Annual PKI Researeh Workshop[C]. Gaithersburg, USA, 2005.

[15] MCKEOWN N, ANDERSON T, BALAKRISHNAN H, *et al.* Openflow: enabling innovation in cam campus networks[EB/OL]. http:// www. openflow.org/documents/openflow-wp-latest.pdf, 2012.

作者简介：

周敏（1988-），女，湖北宜城人，中国人民解放军理工大学硕士生，主要研究方向为未来网络、网络性能分析与建模。

陈鸣（1956-），男，江苏无锡人，中国人民解放军理工大学教授，主要研究方向为网络测量、网络性能分析与建模。

邢长友（1982-），男，河南杞县人，博士，中国人民解放军理工大学讲师，主要研究方向为网络与分布式计算、未来网络、网络流媒体。

蒋培成（1988-），男，山东泰安人，中国人民解放军理工大学硕士生，主要研究方向为 SDN 网络、网络测量与建模。