doi:10.3969/j.issn.1000-436x.2014.z1.005

基于 IPv6 源地址验证的一种可信身份系统

周端奇[1,2,3]，毕军[1,2,3]，姚广[1,2,3]

（1. 清华大学 信息网络科学与网络空间研究院，北京 100084；
2. 清华大学 计算机科学与技术系，北京 100084；3. 清华信息技术国家实验室，北京 100084）

摘 要：当前互联网中，并不对分组发送者的身份进行验证，带来了大量的伪造身份的攻击。为了解决这一安全问题，提出了真实可信身份通信系统。基于源地址验证，通过将用户的身份映射为 IPv6 地址的后 64 位，实现了在分组中携带用户身份，从而确保了用户身份的隐私性、可验证性和真实性，并对其安全性能进行了实验。

关键词：IPv6；SAVI；真实身份；网络安全

中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2014)Z1-0020-07

Trustworthy identity system based on IPv6 source address validation

ZHOU Duan-qi[1,2,3], BI Jun[1,2,3], YAO Guang[1,2,3]

(1. Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China;
2. Department of Computer Science, Tsinghua University, Beijing 100084, China;
3. Tsinghua National Laboratory for Information Science and Technology (TNList) , Beijing 100084, China)

Abstract: In the Internet, there are no mechanisms to verify the identity of a message sender, resulting in a large number of forged identity attacks, such as phishing websites. By mapping the user identity into the rightmost 64 bit of the IPv6 address, this paper tries to make every message embedded with an identity, which lay a credible foundation for communications on the Internet. We design and realize a true identity communication system based on source address validation improvement, which can protect the privacy of the users, and ensure the verifiability and authenticity of the user identities.

Key words: IPv6; SAVI; network security; true identity

1 引言

互联网自诞生之日起发展十分迅速，近年来更是成为了人类社会重要的信息基础设施，极大地推动了人类社会政治、经济、文化的发展。但是，传统的互联网缺乏广泛的可信基础，带来了一系列安全问题严重桎梏了互联网的进一步发展，比如钓鱼网站、DNS 劫持等欺诈行为均给社会带来了巨大的损失。据中网统计显示，钓鱼网站每年给网民带来的经济损失超过 300 亿元。尤其是在安全性要求较高的军事、金融等网络中，伪造的军事指示或者金融交易命令，往往会造成严重后果，带来重大的经济损失。而当前的网络中，缺乏对分组发送者的身份验证，导致容易发生伪造分组的攻击。因此，保证互联网上通信双方的身份真实可信十分重要。

另外，网络监管机构往往需要对可疑的行为进行身份确认，从而尽快定位分组的发送者，但是，当前的网络中，缺乏快捷的身份获取和确认的方

收稿日期：2014-10-15
基金项目：国家高技术研究发展计划(“863”计划)(2013AA013505)；国家自然科学基金资助项目(61140454)；国家科技支撑计划基金资助项目(2012BAH01B01)
Foundation Items: The National High Technology Research and Development Program of China (863 Program) (2013AA013505); The National Natural Science Foundation of China (61161140454); National Science & Technology Pillar Program of China (2012BAH01B01)

法，从而为监管机构实施有效监管增加了难度。因此，在身份真实性的基础上，需要一个能够快捷地进行身份的跨域验证的系统。

2　问题分析

互联网中伪造分组的攻击可以分为两种：第一种是将分组的源地址伪造成合法的源地址，第二种是将分组的发送者身份伪造成合法的发送者身份。这种伪造攻击的根本原因在于传统的互联网缺乏广泛的可信基础。缺乏可信基础的主要原因有以下几点。

1) 互联网缺乏身份认证机制。目前 IPv6 地址分发协议中，DHCPv6 协议（dynamic host configuration protocol for IPv6）[1]和 SLAAC 协议（IPv6 stateless address autoconfiguration）[2]给主机分配 IPv6 地址或主机自行产生 IPv6 地址都是随机生成的，IP 地址并不与用户的真实社会身份相对应，因此只是主机标识，而不是用户的身份标识，导致无法对互联网上的用户进行身份辨别。并且，随着位置的改变，IP 地址也会随之改变，难以作为身份认证。

2) 源地址缺乏可信性。由于网络转发设备并不对源 IP 地址进行检查，因而无法保证源 IP 地址与发送者身份的一致性，导致众多伪造身份的假冒攻击和重放攻击。

3) 缺乏有效的身份验证回溯机制。当前互联网中，IP 地址分配由各自治域，根据用户需求独立分配，并在用户使用完之后回收 IP 地址并重新分配，导致查证攻击者十分困难，尤其是难以进行跨域的跟踪回溯。

因此，为了防范伪造攻击，互联网体系结构中需要一个广泛的可信基础，并基于该可信基础，设计真实身份。通信双方在具有可信的真实身份的前提下完成通信。

在真实可信身份通信系统中，选择了 IP 地址作为真实可信身份的载体，主要是因为当前的 IP 地址系统中已经存在了 SAVA[3]、uRPF[4]、SAVE[5]等地址检查机制，确保 IP 地址的基本可信，同时，IP 地址天然带有的主机标识含义与用户身份标识有一定的重叠，在不加入新层次的前提下，作为真实可信身份的载体成本最小。

由于 IP 地址是直接可见的，如果直接将用户的真实社会身份放入 IP 地址中，会存在隐私泄露的问题。因此，必须对用户的真实社会身份进行编码加密，将加密结果放入 IP 地址中。同时，还必须保证拥有一定合法权限的网络监管机构可以基于 IP 地址对用户的真实社会身份进行验证和回溯。验证是指系统可以对 IP 地址进行检查，确认该 IP 地址是否有对应的真实社会身份，即该用户身份是否是伪造的；回溯是指系统可以查找出 IP 地址所对应的用户真实社会身份。

这就明确提出了一个问题：是否可以在保护用户隐私的同时，建立一个可以有效地追溯分组发送者真实身份的机制，以供特殊情况下使用？

为了解决上述问题，提出了解决互联网身份认证安全问题的 3 个原则。

1) 隐私性：用户的真实身份不会随意泄露。即在没有获得授权的情况下，无法通过分组确认分组发送者的真实身份。

2) 可验证性：在获得授权的情况下，可以通过分组确认分组发送者的真实身份。

3) 真实性：分组发送者难以伪造其身份，从而确保身份的真实性。

以这 3 个原则为出发点，设计并实现了真实可信身份通信系统。在真实可信身份通信系统中，选择了源 IPv6 地址作为真实可信身份的载体。

3　相关工作

清华大学提出了五元组的设计方案，通过部署 SAVI[6]交换机，对 SAVI 交换机进行实时监控，来收集用户的上网记录。但是，该设计方案依旧采取了自治域本地认证的方式，用户必须先获取 IPv6 地址之后，再进行身份验证，致使 IPv6 地址没有携带身份信息。并且，五元组方案无法支持跨域身份管理和溯源，如果要确认分组发送者的真实身份，需要多方网络管理者的共同合作，逐步回溯，很难仅仅根据所收到的分组对发送者的身份进行回溯。

目前，关于 DHCP 安全性的文献方案[7,8]，主要集中在 DHCPv4 协议的增强上，主要目的是提高 DHCP 分组的安全性，防止伪造 DHCP server 的分配地址。

4　系统设计

基于上述目标，设计了真实可信的身份通信系统，在保证用户隐私不被泄露的同时，确保用户必须使用其真实身份进行通信，并实现用户身份可验证和可溯源。

在真实可信身份通信系统中，定义了 3 种 ID。

NID(network ID)：用户进行身份认证时所使用的用户名，即用户的真实社会身份。

EID(encrypted ID)：使用加密算法对 NID 进行加密后的结果。

GID(general ID)：根据 EID 生成的 64 bit，作为 IPv6 地址的后 64 bit 地址，用以在分组中携带用户身份。

真实可信身份通信系统主要由 4 个部分组成：身份认证系统、地址分配系统、身份溯源系统、分组过滤系统（如图 1 所示）。

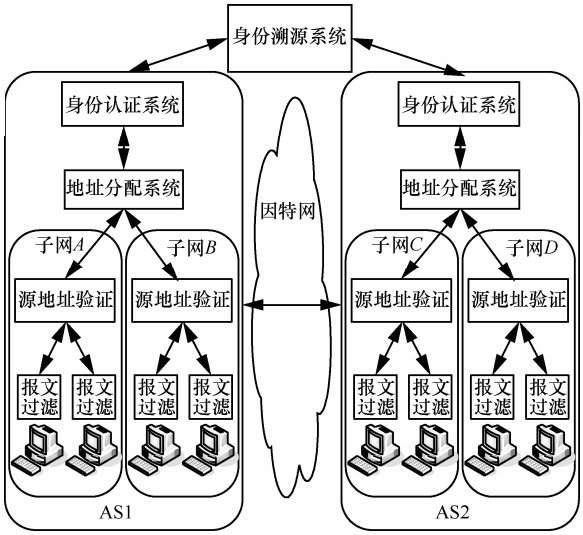

图 1　真实可信身份通信系统

身份认证系统，是对用户的真实社会身份 NID 及其密码进行检验，如果验证通过，将用户的真实社会身份 NID 加密产生 64 bit 的 GID，并将 GID 发送到地址分配系统；如果验证不通过，则返回错误信息，使用户无法使用网络服务。另外，身份认证系统需要将经过其认证的身份，所分配的 IPv6 地址和分配时间发送到身份溯源系统，以供记录。

地址分配系统，在获取身份认证系统发送的 GID 后，将 GID 与子网前缀等信息相结合，生成 IPv6 地址，分配给用户所使用的主机，并将所分配的地址和地址分配时间发送回身份认证系统。

身份溯源系统，支持用户根据所收到的分组对分组发送者的身份进行验证和回溯，即确认分组发送者是否拥有真实可信的社会身份 NID 以及获取该 NID。

分组过滤系统，部署在主机层面，维护真实身份过滤表，用以记录已经经过验证的真实身份，并使用该过滤表对伪造身份的分组进行过滤。对于首次收到的分组，分组过滤系统会根据分组 IPv6 地址，检查分组发送者是否拥有真实可信的社会身份 NID，如果确认该分组发送者的 NID 真实可信，则将该 NID 记入真实身份过滤表中。

真实可信身份通信系统的设计，满足安全的 3 个原则：“隐私性”、“可验证性”、“真实性”。

隐私性：身份认证系统使用加密算法对 NID 进行加密，保证了在没有密钥的情况下，难以根据分组信息获取用户的真实社会身份。身份溯源系统必须拥有一定的权限才可以使用，保证了用户的真实社会身份不会被随意泄露。

可验证性：身份溯源系统提供 2 个层次的身份验证和溯源，使分组发送者的身份真实性可以得到确认。

真实性：为了确保用户的身份真实，真实身份通信系统是基于源地址验证设计的，由源地址验证保证源 IPv6 地址的真实性。真实身份通信系统将用户的真实社会身份绑定到源 IPv6 地址，进而保证了身份的真实性。

5　系统实现

基于上述设计，实现了真实可信身份通信系统的原型。其中，身份认证系统和地址分配系统是基于 DHCPv6 协议扩展实现的，同时，实现了真实可信身份生成算法；身份溯源系统，设计并实现了协议流程，保证只有拥有足够权限的用户才能对分组身份进行验证和溯源。

5.1　DHCPv6 协议扩展

通过对 DHCPv6 协议进行扩展，使其支持身份认证等，实现了身份认证系统和地址分配系统。Dibbler 是 DHCPv6 的一个 C++开源实现方案，主要是基于 Dibbler 针对四分组交互流程，新增加了 Username、Nonce、Digest 3 个 Option，使之可以携带用户名 NID 和密码，同时，增加了 DHCPv6 服务器与身份认证系统交互的过程。

具体交互流程如下（如图 2 所示）。

1) Solicit：DHCPv6 客户端发送 Solicit 消息，通过新增加 Username Option 选项，携带用户名信息。

2) Advertise：DHCPv6 服务器收到用户名信息后，向认证服务器查询该用户名是否存在。如果该用户名存在，则认证服务器会随机生成一个加密字 Nonce，并将所生成的 Nonce 发送回 DHCPv6 服务器。DHCPv6 服务器将 Nonce 添加

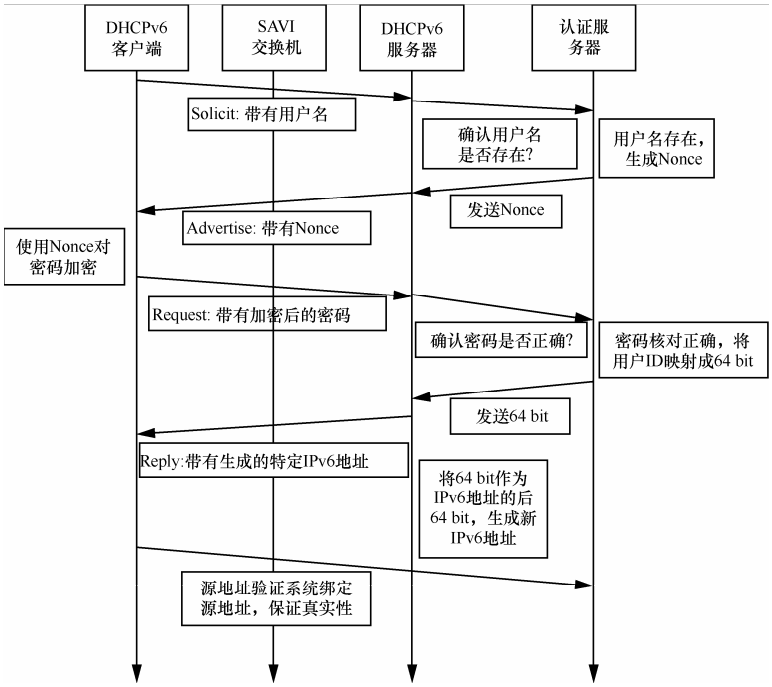

图 2　身份认证系统和地址分配系统交互流程

到新增加的 Nonce Option 选项，并通过 Advertise 消息发送到客户端。

3) Request：DHCPv6 客户端接收到 Advertise 消息后，利用 DHCPv6 服务器传来的加密字，运用对称加密算法对用户密码进行运算，得出加密后的密码。DHCPv6 客户端将所得加密后的密码添加到新增加的 Password Digest Option 选项，并通过 Request 消息发送到 DHCPv6 服务器。

4) 密码比对：DHCPv6 服务器将 Request 中 Password Digest Option 携带的加密后的密码转发到认证服务器。认证服务器将加密后的密码与自己运算出的结果进行比对，如果相同则认为该用户为真实合法用户，并进一步查询该用户名对应的用户身份 ID，并按照身份 ID 映射算法生成 IPv6 地址后 64 bit，发送到 DHCPv6 服务器；如果不同，则将认证失败的消息告知 DHCPv6 服务器。

5) Reply：DHCPv6 服务器如果接收到了后 64 bit，则结合 IPv6 网段的地址前缀和所生成的后 64 bit，生成一个 128 bit 的 IPv6 地址。通过 Reply 消息将 IPv6 地址返回给 DHCPv6 client；否则，不再回复 Reply 消息，不分配 IPv6 地址。

5.2　真实可信身份生成算法

真实可信身份生成算法分为 2 个步骤：第一步，使用不对称加密算法产生公钥 p 和私钥 q，并使用私钥 q 对用户真实社会身份 NID 进行加密，加密结果为 EID；第二步，使用散列函数对 EID 进行运算，得出结果中取 64 bit 作为 GID，如图 3 所示。

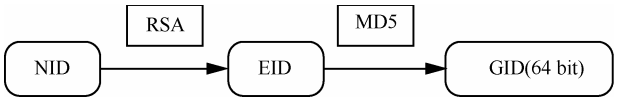

图 3　真实可信身份生成算法

在真实可信身份通信系统中，选择 RSA 算法作为不对称加密算法，选择 MD5 作为散列函数，实现了真实可信身份生成算法。另外，将真实可信身份通信系统与身份生成算法相关的接口公开，使系统可以兼容其他算法。

5.3　身份溯源系统

身份溯源系统，支持身份真实性验证和真实身份获取。

在进行身份真实性验证时，验证者首先需要向身份溯源系统发送用户名和密码，身份溯源系统检查该验证者拥有验证权限之后，将 EID 发送给验证者。验证者对 EID 使用 MD5 算法计算，并将计算结果与 GID 对比，即可确认被验证者的身份真实性。在完成身份真实性验证之后，可以进一步向身份溯源系统申请获取被验证者的真实身份。身份溯源系统检查该验证者拥有获取权限之后，将身份生成算

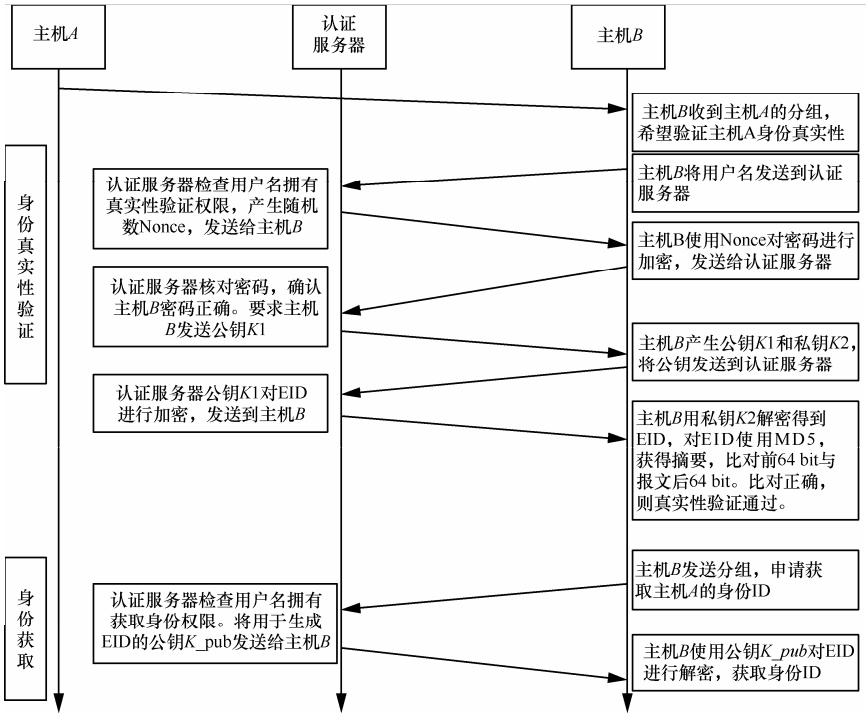

图 4　身份溯源系统交互流程

法中公钥 p 发送给验证者，验证者使用公钥 p 对 EID 进行解密，解密所得结果为被验证者的真实社会身份 NID，如图 4 所示。

身份真实性验证的具体交互流程如下：

1) 主机 *B* 将用户名发送到认证服务器，申请验证主机 *A* 身份真实性；

2) 认证服务器检查主机 *B* 用户名是否拥有身份真实性验证的权限。如果确认拥有，则产生随机数 Nonce，发送给主机 *B*；

3) 主机 *B* 使用 Nonce 对密码进行加密，发送给认证服务器；

4) 认证服务器核对密码，检查主机 *B* 密码正确，如果密码核对通过，则要求主机 *B* 发送公钥；

5) 主机 *B* 使用 RSA-1 024 算法产生公钥 *K*1 和私钥 *K*2，并将公钥发送到认证服务器；

6) 认证服务器使用公钥 *K*1 对 EID 进行加密后，发送到主机 *B*；

7) 主机 B 使用私钥 *K*2 解密得到 EID，对 EID 使用 MD5，获得摘要，对比摘要的前 64 bit 和分组后 64 bit IPv6 地址，如果对比通过，则真实性验证通过。

身份获取的具体交互流程如下：

1) 主机 *B* 发送分组，申请获取主机 *A* 的身份 ID；

2) 认证服务器检查用户名是否拥有获取身份的权限，如果确认拥有，则将用于生成 EID 的公钥 *K_pub* 发送到主机 *B*；

3) 主机 *B* 使用公钥 *K_pub* 对 EID 进行解密，获取身份 ID。

6　系统评价

6.1　性能评估

相比传统的 DHCPv6 地址分配流程，真实可信身份通信系统中地址分配流程添加了身份认证环节，带来了一定的延时。为了分析身份认证环节所引入的延时影响，搭建了一个简单的实验拓扑进行实验测试（如图 5 所示）。

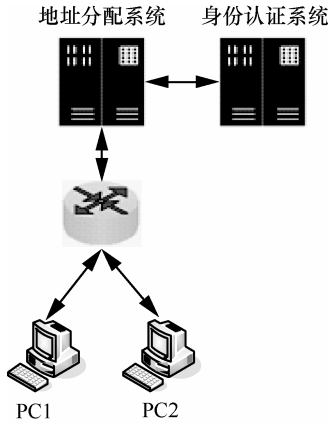

图 5　DHCPv6 分配地址耗时占比分析

其中，PC1 运行未更改的 DHCPv6 协议作为对照组，PC2 运行扩展后的 DHCPv6 协议作为实验组。当对照组进行测试实验时，身份认证系统不接入网络拓扑中。

实验组和对照组分别进行了 100 次实验，记录主机获取地址所用延时，并以 0.05 s 为区间进行分组分析（如表 1 所示）。

可以看出，实验组平均比对照组需要多耗时 0.047 s，比对照组增加耗时 2.63%，是身份认证系统所带来的延时效果（如图 6 所示）。

表 1　性能评估：实验组、对照组统计

统计指标	实验组	对照组
均值	1.831 s	1.784 s
方差	0.099 s^2	0.122 s^2
标准差	0.315 s	0.349 s
中位数	1.903 s	1.870 s
最大值	2.214 s	2.207 s
最小值	0.699 s	0.663 s

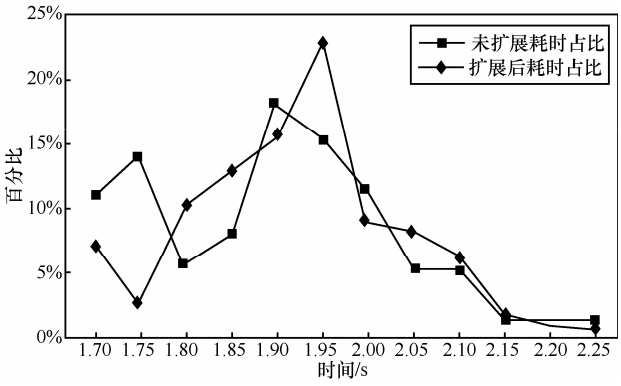

图 6　性能评估耗时占比分析

为了说明引入身份认证系统后，地址分配流程的耗时是否显著增加，进行假设检验。

原假设 H_0：实验组均值 E_1=对照组均值 E_2

进行双样本等方差 t 检验，得出：

P-value = 0.345 > 0.05，无法拒绝原假设。

进行双样本异方差 t 检验，得出：

P-value = 0.356 > 0.05，无法拒绝原假设。

2 次 t 检验结果说明：引入身份认证系统后，并没有显著增加地址分配流程的耗时，所引入耗时在统计上可以忽略不计。

但是，值得注意的是，本次实验环境中，地址分配系统和身份认证系统是在同一物理机器，2 台不同的虚拟机上运行的，因此，二者之间的网络传输耗时可能被低估。

6.2　安全性

安全性主要是指系统需要能够有效地防范假冒攻击和重放攻击。对于真实可信身份通信系统，假冒攻击主要是指攻击者已知用户的身份 NID，企图通过假冒用户身份，获取相应的 IPv6 地址进行通信；重放攻击主要是攻击者直接重放用户的 IPv6 地址进行通信。

在假冒攻击中，由于攻击者仅知道用户的 NID 而不知道用户密码，所以无法按正常途径通过身份认证系统获取 GID，进而无法使地址分配系统通过 DHCPv6 协议向其分配合法地址。

如果攻击者通过随机伪造密码，试图获取特定 NID 对应的 GID。由于密码的二进制长度为 128 bit，随机产生密码需要尝试 2^{128} 次，以每次地址分配耗时 1.831 s 计算，则攻击者需要 4.7×10^{32} 年才能攻击成功一次。

由于 SAVI 是通过监听 DHCPv6 协议分组实现源地址与交换机端口的绑定，直接假冒源地址发送的分组将会被 SAVI 交换机过滤，从而防止了假冒攻击。另外，即使攻击者通过非 SAVI 部署区发送出攻击分组，由于其 GID 是随意伪造的，在到达目的端时，依旧会被分组过滤系统过滤，从而使假冒攻击失效。

实验模拟攻击者进行假冒攻击。攻击者知道 NID，通过随机产生密码希望获取 GID。经过 200 次攻击，没有成功获取 GID。

在重放攻击中，攻击者直接重放合法用户的 IPv6 地址发送分组。当攻击者与合法用户位于同一子网时，由于 SAVI 将 IP 地址与交换机端口号绑定，攻击分组会被 SAVI 过滤。当攻击者与合法用户位于不同子网时，由于子网前缀不同，攻击者的攻击分组会被域间源地址过滤，从而使重放攻击失效。

6.3　隐私性

隐私性主要是指攻击者通过 GID 或者 EID 获取用户身份 NID。隐私性主要是通过加密算法保障。考虑到随着运算能力的提升和加密算法逐步被破解，将系统设计与加密算法独立，即系统为加密算法提供相应接口，加密算法可以随时升级或更改，从而保证系统隐私性不会因为加密算法的过时而失去作用。

在真实可信身份通信系统中，选择实现了 RSA

算法作为 NID 的加密算法。在 RSA 算法中，有 3 个关键的参数：n、p 和 q。其中，n 为密钥长度，p 和 q 为 2 个质数。

$$n=pq$$

p 和 q 的长度决定了算法的安全性，只有当 p 和 q 为足够大的素数时，攻击者才无法在多项式时间内将 n 分解。

随着 n 的长度增加，对 RSA 算法进行暴力破解的时间复杂度也随之增加。根据估算（如表 2 所示），在密钥长度 n 达到 2 048 bit 时，破解所需时间为 3×10^{20} MIPS 年（MIPS 年：每秒钟执行一百万条指令的计算机计算一年时间的计算量）。按照当前 CPU 性能约为 3 GHz，则需要一台计算机运行 10^{17} 年才能破解。在真实可信身份通信系统中，采取了 RSA 2 048 作为加密算法，保证了用户的隐私不被泄露。

表 2 RSA 算法安全性估算

密钥长度 n/bit	MIPS 年
512	3×10^{4}
768	2×10^{8}
1 024	3×10^{11}
2 048	3×10^{20}

7 结束语

针对互联网缺乏可信基础而常常发生伪造攻击，设计了真实可信身份通信系统，通过将用户身份嵌入到 IPv6 地址中，能够有效地防止用户身份被假冒。在有效地保证用户身份隐私不泄露的同时，系统支持经过授权的用户验证分组发送者的身份，查询分组发送者的真实身份。系统扩展了 DHCPv6 协议，使其能够支持用户身份认证过程，设计了开放的用户身份映射接口，并在原型中实现了一种用户身份映射算法，设计并实现了用户身份溯源系统。

参考文献：

[1] RALPH D, *et al*. Dynamic Host Configuration Protocol for IPv6 (DHCPv6)[S]. RFC 3315, 2003.

[2] THOMAS N, THOMSON S, *et al*. IPv6 Stateless Address Autoconfiguration[S]. 2007.

[3] BI J, *et al*. A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience[S]. 2008.

[4] WARREN K, MCPHERSON D. Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)[S]. RFC 5635, 2009.

[5] LI J, *et al*. SAVE: source address validity enforcement protocol[A]. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies[C]. 2002.

[6] BI J, *et al*. Source Address Validation Improvement (SAVI) Framework[S]. 2013.

[7] RALPH D, ARBAUGH W. Authentication for DHCP Messages[S]. RFC 3118, 2001.

[8] KEN H, , *et al*. DHCP authentication for DHCP Messages[S]. 2000.

作者简介：

周端奇（1989-），男，湖北随州人，清华大学硕士生，主要研究方向为 IPv6 安全。

毕军[通信作者]（1972-），男，北京人，博士，清华大学信息网络科学与网络空间研究院网络体系结构和 IPv6 研究室主任、教授、博士生导师，主要研究方向为新型互联网协议（IPv6 协议、互联网源地址验证、互联网路由等）和新型网络体系结构（软件定义网和内容中心网等）。E-mail: junbi@tsinghua.edu.cn。

姚广（1984-），男，湖北宜昌人，清华大学博士后，主要研究方向为 SDN。