doi:10.3969/j.issn.1000-436x.2013.01.019

基于流认证的 IPv6 接入子网主机源地址验证

陈越，贾洪勇，谭鹏许，邵婧
(解放军信息工程大学 网络空间安全学院，河南 郑州 450004)

摘 要：提出了一种以密码学方法实现的 IPv6 接入子网主机高速源地址验证方案。把主机 MAC 地址作为身份同主机公钥相绑定，利用密码生成地址算法从主机公钥衍生出 IPv6 接入子网地址，通过数字签名提供主机真实性的验证，以消息认证码和流认证技术实现接入网关对数据分组流 IPv6 地址的快速安全的验证。原型系统实验表明，该方案能够以低开销实现数据分组源地址验证，是一种安全、可行的方案。
关键词：源地址验证；基于身份的密码；密码生成地址；消息认证码；流认证
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1000-436X(2013)01-0171-07

Host's source address verification based on stream authentication in the IPv6 access subnet

CHEN Yue, JIA Hong-yong, TAN Peng-xu, SHAO Jing
(Institute of Cyberspace Security, PLA Information Engineering University, Zhengzhou 450004, China)

Abstract: A cryptographically-implemented high-speed source address verification scheme for the hosts in the IPv6 access subnet was proposed. The MAC address was used as the identity of the host machine and bounded with the host's public key. Then the IPv6 address was derived from the host machine's public key using the cryptographically generated address algorithm. The address authenticity was guaranteed by the digital signature and the fast and secure source address verification for packet stream was achieved through message authentication code algorithm and stream authentication. The experimental system show that the scheme could ver fy the source addresses of data packets at a loss cost. Thus, it is a secure and feasible scheme.
Key words: source addresses verification; identity based cryptography; cryptographically generated address; message authentication codes; stream authentication

1 引言

由于互联网在设计之初并没有考虑到可能会出现的恶意攻击，对报文的转发只是基于报文的目的地址，对源地址不做检查，所以使得现在的互联网中的伪造源地址攻击轻易而频繁。针对该问题，研究者们提出了一些源地址验证方案[1~4]，依据所能实现的验证粒度，现有方案大致分成 3 类，包括自治系统间源地址验证、自治系统内源地址验证和接入子网内源地址验证。其中，前 2 类方案只能实现前缀级别的源地址验证，不能实现主机粒度的源地址验证和遏制自治系统内主机发起的源地址攻击。

接入子网源地址验证方案，主要依据所有相关网络设备在同一个网络管理机构管理控制下，解决方案与接入子网的地址管理分配和控制策略以及端系统的接入方式密切相关。现有接入子网源地址验证方案在安全性方面仍存在一定的不足。例如，

收稿日期：2011-08-22；修回日期：2011-12-20
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（2012CB315901）；国家科技支撑计划基金资助项目（2008BAH37B03）
Foundation Items: The National Basic Research Program of China (973 Program) (2012CB315901); The National Key Technology R&D Program of China (2008BAH37B03)

文献[4]提出的真实源地址验证方案 SAVA 采用了在交换机的端口和真实有效的 IP 地址之间实现动态绑定的方法。但是 SAVA 中的签名并不是密码学意义上的签名，只是一种标识，不具有数字签名所具有的认证性和不可否认性。因此，需要提出一个更加安全高效的接入子网内源地址验证方案。

流认证技术为高速 IP 分组源认证提供了重要思路[5~8]。其主要方法是通过对称密钥、伪随机函数密钥链和密钥延迟发送方法来获得快速的数据分组的源认证。例如，PERRIG A 和 SONG D 提出的 TESLA[7,8]是一个高效的多播源验证协议，它可以对收到的多播数据进行验证，确保数据来自声明的多播源。

本文针对 IPv6 网络，以身份公钥密码[9]和消息认证码[6]为技术基础，采用流认证的思想，提出了一种新的 IPv6 接入子网源地址验证方案——SASAV (stream-authentication-based source address verification)。在 SASAV 中，主机利用自身的 MAC 地址为身份申请私钥，然后再利用身份私钥对应的公钥衍生出接入子网内的 IPv6 地址，通过数字签名和消息认证码实现了数据分组流的源地址验证。 SASAV 采用了身份公钥密码体制，因而可以实现 TESLA 等流认证协议所不具备的不可否认性服务。

2 基于流认证的源地址验证方案——SASAV

SASAV 验证流程如图 1 所示，包括基于身份密码系统的构建、IPv6 真实地址产生和源地址验证信息的产生与验证 3 个阶段。

2.1 基于身份密码系统的构建

该阶段分为 2 步进行，主机注册和主机密钥产生。其中，主机注册实现了合法主机向私钥生成中心 PKG 的安全注册，保证每个主机都必须以真实的 MAC 地址作为身份进行注册，同时，为注册成功的主机对应分配一个随机数，为下一步做准备。这一步是整个系统运行安全的前提，可以结合实际应用场景采用一些人工手段来保证注册的安全性。

主机密钥产生过程主要为各主机安全产生并分发私钥，而主机公钥是由主机自己根据其 MAC 地址和系统公开参数生成的。通过 PKG 的主私钥和主机在上一步得到的随机数，可以保证只有拥有合法身份的主机才能获得对应的私钥，同时保证主机获得的私钥是 PKG 产生的，不是伪造的且没有被恶意篡改。

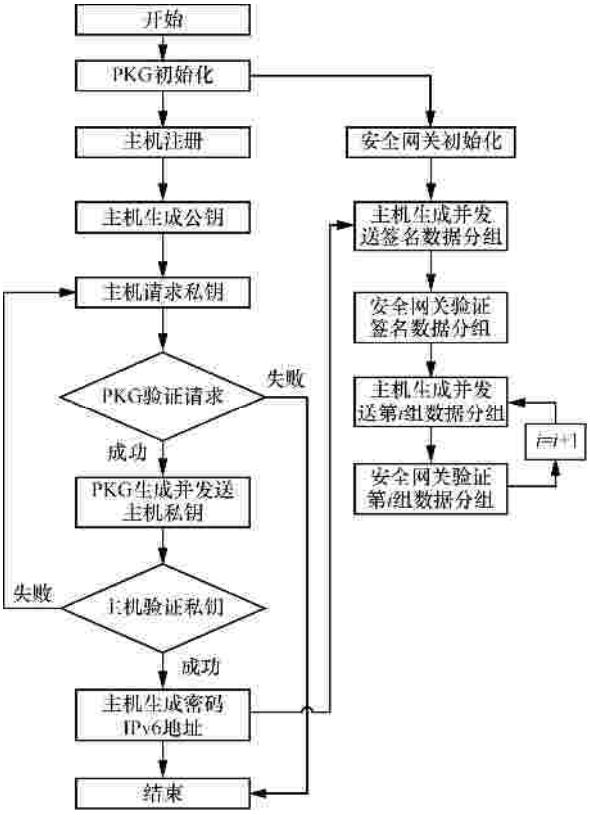

图 1 SASAV 流程

2.1.1 主机注册

1) 系统初始化。在该接入子网内设置一台可信计算机作为私钥生成中心 PKG。PKG 运行初始化算法。算法输入一个安全参数，输出一系列系统公开参数(包括明文空间、密文空间、散列函数等)、主公钥 *KMP* 和主私钥 *KMS*。主私钥用来生成用户私钥，将其安全保存在该可信计算机的可信平台模块(TPM, trusted platform module)中。

2) Host ? PKG: register (MAC)

每台主机在准备连接到该接入子网时，都需要先以 MAC 地址作为身份向私钥生成中心进行注册。

3) PKG ? Host: {Random, KMP, parameter}

私钥生成中心收到主机注册请求后，记录下该主机的 MAC 地址，并为其生成一个随机数 random。同时，将每个主机的 MAC 地址和分配给该主机的随机数对应起来，以列表的形式保存，称该列表为 LMAC。然后，私钥生成中心将随机数 random、主公钥 KMP 及系统公开参数发送给主机。

2.1.2 主机密钥产生

1) 主机公钥产生

主机根据上述注册过程中收到的主公钥 *KMP* 和系统公开参数，结合其 MAC 地址根据基

于身份的数字签名方案计算出主机公钥 KP，其过程如下。

系统参数的建立（由 PKG 执行）：随机选择一个数 $s \in Z_q^*$，计算 $P_{pub} = sP$，其中，P 为 G_1 的生成元。选择 2 个强密码杂凑函数 $H_1 : \{0,1\}^* \to Z_q^*$ 和 $H_2 : \{0,1\}^* \to G_1^*$，其中，$H_1$ 将任意长度输入映射到固定长度；H_2 把用户身份 ID 映射到 G_1 中的一个元素。最后，PKG 把 s 作为系统的私钥保存，并公开系统参数 $(G_1, G_2, \hat{e}, P, P_{pub}, H_1, H_2, p, q)$。

用户密钥生成（由 PKG 执行）：给定任一 MAC 地址，$MACID \in \{0,1\}^*$，计算公钥 $Q_{MACID} = H_2(MACID)$。计算私钥 $d_{MACID} = sQ_{MACID}$，其中，s 为系统私钥。

签名　为了使用私钥 d_{MACID} 对消息 $M \in \{0,1\}^*$ 签名，签名者需要执行随机选择 $r \in Z_q^*$，计算 $R = rP$，输出针对 M 的签名 $s = (R, rP_{pub} + H_1(M, R)d_{MACID})$。

验证　设 $s = (U, V)$ 为针对 M 的签名，验证者需要执行：计算 $Q_{MACID} = H_2(MACID)$；计算 $u = \hat{e}(V, P)$；计算 $v = \hat{e}(U + H_1(M, U)Q_{MACID}, P_{pub})$，如果 $u = v$，则输出接受签名，否则输出拒绝。

2) Host ? PKG: {MAC, Encrypt$_{KMP}$ ($random$)}

主机用主公钥 KMP 加密随机数 $random$，生成加密信息 Encrypt$_{KMP}$($random$)，以防止随机数在发送过程中被篡改。然后，主机把 MAC 地址及该加密信息发送给私钥生成中心，申请主机私钥。

3) 验证私钥请求

私钥生成中心收到主机请求后，首先根据信息中的 MAC 地址查找其保存的列表 LMAC。如果在列表中能找到对应表项，则说明该地址是注册过的，进行下一步验证；否则，说明该地址未注册过，丢弃该请求信息。找到对应的表项后，对收到信息的剩余部分进行解密，将解密得到的信息与对应表项中的随机数比较。如果匹配成功，则说明请求者是注册过的合法主机，验证成功；否则丢弃该请求信息。

4) PKG? Host:Sign$_{KMS}$(MAC ‖ ($random \oplus KS$))

验证成功后，PKG 根据该主机 MAC 地址和主私钥 KMS 生成主机私钥 KS。PKG 将该主机私钥 KS 与对应表项的随机数 $random$ 进行异或运算，然后，使用主私钥 KMS 对 MAC 地址及异或值进行私钥运算，将运算结果作为响应信息发送给主机。

5) 主机私钥验证与接收

主机收到响应信息后，使用之前收到的主公钥 KMP 验证该响应信息。如果其中的 MAC 地址信息部分与主机的 MAC 地址一致，则主机认为该信息是来自 PKG，将信息的剩余部分与其保存的随机数进行异或操作，得到私钥 KS，并将其安全保存；否则，丢弃该响应信息，主机重新发送私钥申请。

2.2　IPv6 真实源地址产生

该阶段主要使用之前产生的主机公钥生成一个基于身份密码的 IPv6 地址，具体过程如下。

1) 主机从路由器公告中获取一个地址前缀，或者使用链路本地地址的地址前缀。然后采用密码生成地址(CGA, cryptographically generated address)算法[10]生成 IPv6 地址。该算法对公共密钥和辅助参数进行 2 次散列运算，计算产生 IPv6 地址的接口标识符，在此接口标识符前面加上本地网络前缀得到的 IPv6 地址就是 CGA。公共密钥和辅助参数构成了 CGA 算法输入参数的数据结构，辅助参数包括伪随机序列、子网前缀、冲突数和扩充区域，其中，伪随机序列由计算机随机生成，在每次生成 CGA 的过程中使用，通过加入此随机数来加强抗攻击能力；子网前缀指的是本地子网前缀；冲突数为无符号整数，必须是 0、1 或 2，用于调整可能产生的地址冲突；公共密钥为自己的公共密钥；扩充区域将留待以后使用。

2) 主机使用上述 IPv6 地址作为目标地址发送邻居请求(neighbor solicitation)报文。报文附加一个选项头，其中包含主机公钥 KP 以及一个基于身份密码的签名，该签名中包含使用主机私钥 KS 对报文的签名。

如果上述 IPv6 地址不与其他主机的 IP 地址冲突，则此主机使用该地址作为其 IP 地址；如果地址有冲突，则调整密码生成地址算法中使用的参数，生成一个新的 IP 地址，再次发送邻居请求报文。

2.3　源地址验证信息的产生与验证

2.3.1　网关初始化

1) 安全网关首先需要与 PKG 通信，获得主公钥 KMP 和系统公开参数。

2) 安全网关与该接入子网内的所有主机都共用一个相同的伪随机函数 F。

3) 每个主机分别估算出与安全网关通信所需要的大致时间（记为 T），即数据分组从主机发送到安全网关所花费的时间，由每个主机各自保存。

2.3.2 签名数据分组的发送及验证

1) 发送

主机在发送普通数据分组之前，需要向网关发送一个签名数据分组（如图 2 所示），以此为后续数据分组的验证传递一些必要信息。

图 2 签名数据分组

签名数据分组生成如下。主机使用其密钥发生器来生成 2 个会话密钥 K_0、K_1，并计算 $F(K_0)$、$F(K_1)$。然后使用主机私钥 KS 对源 IP 地址和 $F(K_0)$进行签名，得到 $S=\mathrm{sign}_{KS}(IP, F(K_0))$。使用 K_0 和 D_1 计算一个消息认证码 $\mathrm{MAC}_{K_0}(D_1)$，其中，$D_1=\{IP, K_0, F(K_1)\}$。将 $F(K_0)$和 $\mathrm{MAC}_{K_0}(D_1)$ 作为数据，生成一个数据分组，并将签名 S 添加到 IP 扩展首部，将该签名数据分组发送给安全网关。

2) 验证

安全网关收到主机发送的帧后，在数据链路层处理时，除了常规处理外，还需要额外记录下该帧的源 MAC 地址，然后再将其交付上层处理。

安全网关根据主公钥 KMP、系统公开参数及记录下来的 MAC 地址来计算出一个公钥 KP'。用公钥对数据分组扩展首部中的签名进行验证，将得到的 IP、$F(K_0)$与数据分组源地址、数据分组中的数据 $F(K_0)$分别进行比较。如果都一致，则验证通过，记录下数据分组的数据 $F(K_0)$、$\mathrm{MAC}_{K_0}(D_1)$ 及源 IP 地址，以列表的形式保存，称该列表为 LIP。LIP 以 IP 地址为索引，表项 $F(K_0)$及 $\mathrm{MAC}_{K_0}(D_1)$ 的值会随着安全网关接收的数据分组认证信息的变化而不断更新。

2.3.3 普通数据分组发送及验证

1) 发送

主机在发送完签名数据分组后，首先需要记录下发送完成的时刻 T_1。然后生成下一个密钥 K_2，计算出 $F(K_2)$和 $\mathrm{MAC}_{K_1}(D_2)$，其中，$D_2=\{IP, K_1, F(K_2)\}$。当主机需要发送数据分组时，都需要在其扩展首部中添加$\{K_0, F(K_1), \mathrm{MAC}_{K_1}(D_2)$（如图 3 所示）。当主机监听到信道空闲，准备发送数据分组时，首先计算此时时刻 T_2 与时刻 T_1 的差值 $DT=T_2-T_1$。如果 $DT>T$，则认为之前发送的签名数据分组已经到达安全网关，可以将这些数据分组全部发送出去（称这些数据分组为第 1 组数据分组）；否则需要等待片刻，直到 $DT>T$ 再发送数据分组。

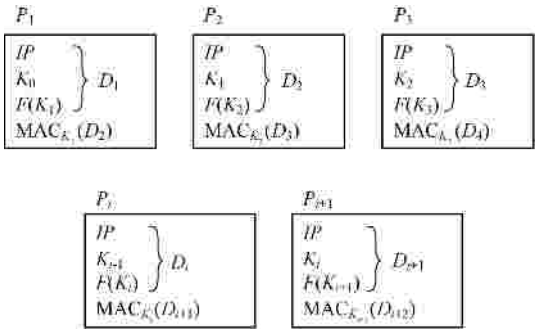

图 3 普通数据分组中包含的认证信息

第 1 组数据分组发送完之后，主机记录下发送完成时刻，然后生成一个新密钥 K_3，计算出 $F(K_3)$和 $\mathrm{MAC}_{K_2}(D_3)$，其中，$D_3=\{IP, K_2, F(K_3)\}$。需要发送的第 2 组数据分组，都要在其扩展首部中添加$\{K_1, F(K_2), \mathrm{MAC}_{K_2}(D_3)\}$。第 2 组数据分组在准备发送时，也需要将发送时刻与上一组数据分组发送完成时刻的差值与 T 进行比较，根据比较结果来决定是否能立即发送。

第 2 组数据分组发送完之后，主机记录下发送完成时刻，并为下一组数据分组计算需要添加的扩展首部信息。依此类推，为第 i 组数据分组添加的数据分组扩展首部信息为$\{K_{i-1}, F(K_i), \mathrm{MAC}_{K_i}(D_{i+1})\}$，其中，$D_{i+1}=\{IP, F(K_{i+1}), K_i\}$。将 2 次信道空闲之间所准备发送的数据分组划分为一组。

2) 验证

安全网关收到某主机发送的第 1 组数据分组后，需要对其中的每个数据分组分别进行验证。对每个数据分组的验证过程基本相同：根据数据分组中的源 IP 地址在表 LIP 中找到对应的 $F(K_0)$和 $\mathrm{MAC}_{K_0}(D_1)$；再使用数据分组扩展首部中的 K_0 来计算 $F(K_0)$，将此计算结果与表 LIP 中的 $F(K_0)$进行比较，如果比较结果一致，则说明传递过来的 K_0 是合法的；然后，用 K_0 来验证表 LIP 中的 $\mathrm{MAC}_{K_0}(D_1)$，如果此验证通过，则认为该数据分组通过了源地址验证，将数据分组扩展首部去除后向外转发。

对于该组中第 1 个验证成功的数据分组，在执行完上述验证后，还要在表 LIP 对应表项中添加上 $F(K_1)$和 $\mathrm{MAC}_{K_1}(D_2)$。对于该组中最后一个被验证的数据分组，还要将表 LIP 对应表项中的 $F(K_0)$和

$\mathrm{MAC}_{K_0}(D_1)$ 删除。对此后收到的该主机的数据分组与安全网关执行类似的验证过程。

3　安全性分析

为了保证安全性的同时提高效率，本方案同时采用了基于身份的公钥密码体制和对称密码体制。基于身份的公钥密码体制把主机的 MAC 地址作为用户的身份，通过用户的身份再衍生出用户的公钥，再由用户的公钥获得 IPv6 接入子网内的 IP 地址，从而实现了 MAC 地址和 IPv6 地址的绑定。虽然存在修改 MAC 地址的方法，但是本方案在注册 MAC 地址时采用了人工离线的方式进行，杜绝了 MAC 地址伪造的可能性，由此也就确定了 IPv6 地址产生的真实性。

接入网关通过基于身份的算法直接获得用户的公钥，减小了传统 PKI 中查询用户证书的开销，提高了效率。用户主机发送的数据分组分成 2 类：签名数据分组和普通数据分组。其中，签名数据分组包含了用户主机采用身份私钥对 IP 地址和第一个对称密钥的伪随机函数运算值进行签名，确保了签名数据分组确实是从签名验证公钥对应的 MAC 地址主机发出来的。为确认后续其他数据分组的真实性，本方案通过把 MAC 密钥延缓发送的方法把签名数据分组后面的若干普通数据联系起来实现顺序认证。当第一个签名数据分组通过验证后，网关可以从签名数据分组中获得 $F(K_0)$和 $\mathrm{MAC}_{K_0}(D_1)$ 并保存下来，在收到第 1 组中的普通数据分组时，从数据分组的扩展首部中获得了$\{K_0, F(K_1), \mathrm{MAC}_{K_1}(D_2)\}$，由此就可以对网关从签名数据分组中获取的记录在列表 LIP 中的 $F(K_0)$、$\mathrm{MAC}_{K_0}(D_1)$ 进行验证，如果验证成功，再用该数据分组中包含的信息在表 LIP 对应表项中添加上 $F(K_1)$和 $\mathrm{MAC}_{K_1}(D_2)$，为第 2 组数据分组的验证做好准备。这种方案能够应对多种可能的攻击。

攻击 1　恶意攻击者伪造签名数据分组。由于攻击者从 PKG 获得所选 MAC 地址对应的私钥，所以构造出的签名不能在网关得到验证，从而不能通过网关的源地址验证，数据分组将会被丢弃。

攻击 2　恶意攻击者伪造普通数据分组。如果攻击者不进行精确的计算从而确定数据分组的内容和发送时间，则根据网关对数据分组的验证方法，此类数据分组必然无法通过认证。如果攻击者希望通过精确计算构造一个普通数据分组，那么由于数据分组扩展首部中的密钥是由主机随机产生的，攻击者很难生成一个随机密钥通过 MAC 算法的认证。

攻击 3　恶意攻击者截获了正常主机发送的数据分组，进行转发攻击。此时攻击者获得正常主机数据分组扩展首部中的 K_{i-1}, $F(K_i)$, $\mathrm{MAC}_{K_i}(D_{i+1})$，把这些值放入到自己数据分组的扩展首部中，同时把自己数据分组的源 IP 地址改为被截获数据分组中的地址，然后发送给网关。由于方案中每个数据分组都增加了序列号，网关收到数据分组后会对序列号进行验证，如果出现重复的序列号会被丢弃。当网关发现有数据分组到达时间超过一定的时间时，也会丢弃相应的数据分组。

4　效率分析

4.1　验证网关设计

验证网关是一台安装有验证网关软件的服务器。验证网关软件在路由软件 XORP 1.6 版本基础上设计，其结构如图 4 所示。图中单播路由模块主要存储了各种单播传输协议，RIB 模块用以存储路由信息，FEA 为转发引擎抽象模块，用以将 RIB 中的路由信息通过转发引擎实现。在上述 XORP 基本模块基础上，设计了验证模块实现了验证网关功能。验证模块由 3 部分构成：运算模块、验证信息存储模块以及验证分组缓存模块。运算模块用以完成对数据分组的验证；验证信息存储模块中存储了验证数据分组所需的信息，数据分组中携带的验证信息暂存于该模块，并以主机地址为索引进行排列；验证分组缓存模块是一块独立运行的 RAM，用以对路由缓存进行补充，所有需要验证的数据分组先存入该模块，进而转给信息运算模块进行处理，针对网络流量的不同可以对该模块的 RAM 大小进行调整。

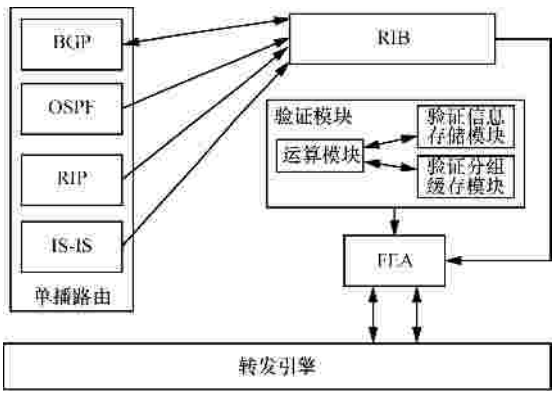

图 4　验证网关设计

当验证网关收到数据分组后，首先交给验证模块进行验证，验证模块首先提取数据分组的验证信息，将其存入信息存储模块，而后信息运算模块根据验证信息对数据分组进行验证，并将验证结果提交给 FEA，若通过验证，FEA 将依据该数据分组的数据转发协议利用转发引擎对数据分组进行转发。

4.2 实验方案

为分析本方案的验证效率和可靠性，在实验室构造了实验系统，如图 5 所示。将 20 台客户机 PC01,…,PC20 使用交换机连接构造局域网，在交换机的出接口连接验证网关，并在验证网关的另一端设置一台接收主机。实验系统中设备的具体参数如下：客户机 PC01,…,PC20，Pentium Dual-Core 2.7GHz CPU，2GB 内存，安装了 Windows 操作系统以及源地址验证客户端软件；交换机为 10/100Mbit/s 自适应以太网交换机；验证网关主机硬件配置为 Pentium Dual-Core 2.7GHz CPU，6GB 内存，安装了 Linux 操作系统以及验证网关软件，验证网关缓存为 32MB，验证模块内部的验证分组缓存模块设置为 16MB；各设备间使用 10/100MMbit/s 网线进行连接。

实验由 2 部分构成，实验 1 为源地址验证效率实验，实验 2 为验证网关的压力测试。在实验过程中，局域网中的客户机分别向接收主机发送数据，从客户机提出发送请求开始计时，接收主机将分别记录来自于不同客户机的每个数据分组的到达时间，首先记录未启动验证网关时的接收数据分组所需的时间，然后记录启动验证网关时的接收数据分组所需的时间，并将 2 次数据进行比较，从而验证验证网关的效率以及抗压性。

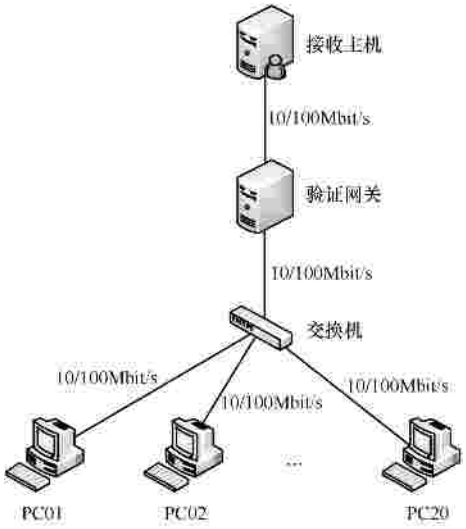

图 5 实验系统示意

实验 1 中，由 PC01 以 512kbit/s 向接收主机连续发送数据。从 PC01 提出发送请求开始计时，接收主机分别记录接收到每个数据分组的启动验证网关的传输时延以及未启动验证网关的传输时延，图 6 记录了接收主机接收前 100 个数据分组的延时曲线。从发送请求发出到接收第一个数据分组之间的时间间隔较长，而后续数据分组的接收时延较短，整体而言启动验证网关的传输时延略大于未启动验证网关的传输时延。

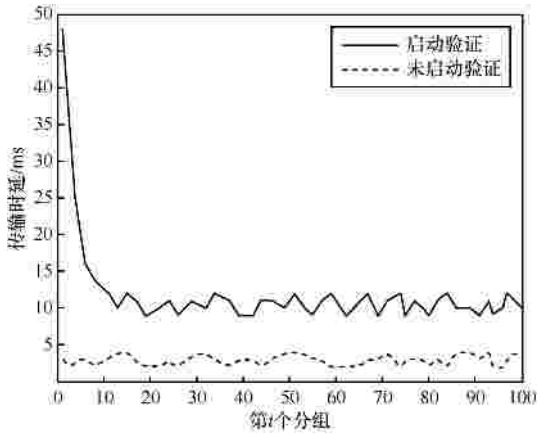

图 6 数据分组传输时延结果

实验 2 中，由 20 台客户机分别同时以递增的传输速率向接收主机连续发送同样大小的数据，记录传输过程中的分组丢失数量以测实验证网关所能承受的极限传输速率。结果如图 7 所示，在验证网关缓存为 32MB，验证模块内部的验证分组缓存模块设置为 16MB 的情况下，当客户机的传输速率大于 2 048kbit/s 时开始出现分组丢失，且随着传输速率的进一步提升分组丢失数快速增加。实际应用中，可以通过提高路由器的缓存大小来满足更高的传输需要。

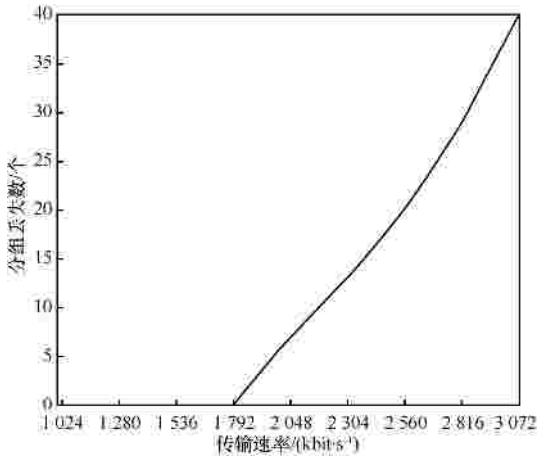

图 7 极限传输速率测试结果

5　结束语

本文提出了一种 IPv6 接入子网中主机源地址验证方案——SASAV，由于采用了基于身份的密码技术和流认证技术，它不仅可以快速验证主机源地址，还可以实现不可否认性服务。方案的安全性分析表明，SASAV 能够抵抗已知的多种攻击。通过实验对 SASAV 的效率进行了验证，网络分组丢失率和接入网关验证效率都在可接受的范围内。未来的工作包括进一步提高 SASAV 的工作效率和抵抗针对密码协议的攻击能力，并在更大的范围内进行实验性部署。

参考文献：

[1] KENT S, ATKINSON R. Security Architecture for the Internet Protocol[R]. 1998.

[2] BREMLER-BARR A, LEVY H. Spoofing prevention method[A]. Proc IEEE INFOCOM[C]. Washington, USA, 2005. 536-547.

[3] BEVERLY R, BERGER A. Understanding the efficacy of deployed internet source address validation filtering[A]. Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement Conference[C]. New York, USA, 2009.15-26.

[4] WU J P, BI J. Source Address Validation Improvement Framework[S]. 2011.

[5] PERRIG A. The BiBa one-time signature and broadcast authentication protocol[A]. Proc of the ACM Conference on Computer and Communications Security[C]. New York, USA, 2001.28-37.

[6] KRAWCZYK H, BELLARE M, CANETTI R. HMAC: Keyed-hashing for Message Authentication[R]. 1997.

[7] PERRIG A, SONG D, CANETTI R. Timed Efficient Stream Loss-tolerant Authentication (TESLA): Multicast Source Authentication Transform Introduction[R]. 2005.

[8] PERRIG A, CANETTI R, SONG D. Efficient and secure source authentication for multicast[A]. Proc of Network and Distributed System Security Symposium[C]. San Diego, USA, 2001.35-46.

[9] BONEH D, FRANKLIN M. Identity based encryption from the Weil pairing[A].Proc of the 21st Annual International Cryptology Conference on Advances in Cryptology[C]. Berlin, Germany,2001.213-229.

[10] AUR T. Cryptographically Generated Addresses (CGA)[R]. 2005.

作者简介：

陈越（1965-），男，河南开封人，博士，解放军信息工程大学教授、博士生导师，主要研究方向为网络与信息安全。

贾洪勇（1975-），男，河南西平人，博士，解放军信息工程大学讲师，主要研究方向为应用密码学、网络安全等。

谭鹏许（1984-），男，河南许昌人，解放军信息工程大学博士生，主要研究方向为网络安全、云存储等。

邵婧（1986-），女，江西鹰潭人，解放军信息工程大学博士生，主要研究方向为网络安全、信息系统等级保护等。