中国科学 E辑：信息科学 2008 年 第 38 卷 第 10 期：1583 ~ 1593
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE IN CHINA PRESS

构建基于真实 IPv6 源地址验证体系结构的下一代互联网

吴建平[①③*]，任罡[①③]，李星[②③]

① 清华大学计算机科学与技术系，北京 100084;
② 清华大学电子工程系，北京 100084;
③ 清华信息科学与技术国家实验室(筹)，北京 100084
* E-mail: jianping@cernet.edu.cn

收稿日期: 2008-06-03; 接受日期: 2008-07-30
国家重点基础研究发展计划(批准号: 2003CB314800)和国家自然科学基金重大研究计划(批准号: 90704001)资助项目

摘要 现有互联网对接收和转发的 IP 分组的源地址并不进行严格的检查，由此引发了很多安全、管理和计费的问题. 基于 IPv6 协议提供的巨大的 IP 地址空间，提出了一种“真实 IPv6 源地址验证体系结构”(SAVA: source address validation architecture)，用以验证互联网中转发的每一个分组的 IP 地址的真实性. 这一体系结构的主要设计原则是轻权、松耦合、多重防御和支持增量部署. 本文阐述了这一体系结构的设计，实现和部署的细节，包括接入子网内、自治系统内、自治系统间 3 个组成部分. 重点介绍了自治体系间 IP 源地址验证的协议设计. 这一体系结构已经部署在 CNGI-CERNET2，一个大规模纯 IPv6 主干网上. 这一体系结构将有助于提高互联网的安全性和可信任性.

关键词
IP 源地址验证
网络体系结构
网络安全

现有互联网的 IP 分组转发，主要基于目的 IP 地址，很少对分组的 IP 源地址的真实性进行检查，这使得分组的 IP 源地址容易伪造. 网络攻击者常常通过伪造分组的 IP 源地址逃避承担责任. IP 源地址验证已经成为互联网面临的一个挑战性的问题.

目前在研究和工程领域已经有很多相关的努力，主要包括基于加密认证的技术，基于过滤的技术和基于追踪的技术. 然而这些现有机制都没能在现有互联网上得到广泛的部署. 不支持增量部署和缺乏对运营商的激励是主要的原因.

本文提出了一种“真实 IPv6 源地址验证体系结构”(SAVA: source address validation architecture)，用以在网络层提供一种透明的服务，以确保互联网中转发的每一个分组都使用“真实

IP 源地址".

这里的"真实 IP 源地址"包含以下三重含义:

- 经授权的. IP 源地址必须是经互联网 IP 地址管理机构分配授权的, 不能伪造.
- 唯一的. IP 源地址必须是全局唯一的, 除了在对全局唯一性不做要求的特殊情形以外.
- 可追溯的. 网络中转发的 IP 分组, 可以根据其 IP 源地址找到其所有者和位置.

这一体系结构的实现可以使得互联网中携带真实 IP 源地址的分组更容易被追踪, 携带伪造 IP 源地址的分组无法转发, 被丢弃. 此外, 这一体系结构的实现还可以带来如下好处:

- 可以实现更精细粒度的网络管理和计费. 由于实现全局唯一的 IP 地址到用户应用的映射更加容易, 网络管理系统可以更容易对端到端的应用实现计费, 如同现有电话网络一样.
- 安全认证可以得到一定程度的简化. 传统的认证多基于加密方法. 如果实现真实 IPv6 源地址验证体系结构, 真实 IPv6 源地址和上层实体间的映射可以为认证提供帮助.
- 新的互联网应用, 例如 P2P 应用和基于 SIP 的大规模多媒体应用, 由于采用了全局唯一的 IP 源地址, 可以简化实现, 提高性能, 更方便部署.

尽管真实 IPv6 源地址验证体系结构的主要设计思想也可以应用在 IPv4 环境下, 我们目前的设计和研究主要集中在 IPv6 领域, 这主要是基于以下两个原因: 首先, 现有的基于 IPv4 的互联网已经部署和运行多年, 直接在其上部署新的源地址验证机制是困难的, 并且代价高昂; 其二, 因为 IPv4 地址空间有限, 网络地址转换(NAT)被广泛使用在现有网络上, 而 IPv6 协议巨大的地址空间使得每一个接入网络的端系统都获得一个全局唯一的真实 IP 源地址成为可能.

本文的正文部分是这样组织和展开的: 第 1 节概要综述了相关研究情况. 第 2 节阐述了体系结构的设计原则、层次结构, 以及接入子网、自治系统内和自治系统间 3 个组成部分. 自治系统间的问题是相对最复杂的, 因此在第 3 节, 我们阐述了自治系统间真实 IPv6 源地址验证体系结构的方案和协议设计. 在第 4 节, 作为一个部署实例, 我们介绍了真实 IPv6 源地址验证体系结构在 CNGI-CERNET2, 一个纯 IPv6 主干网上的部署. 最后, 在第 5 节, 我们总结全文并展望了下一步的工作.

1 相关研究

与源地址验证相关的研究工作可以分为 3 类: 加密认证的方法、预先的过滤方法、事后的追踪方法.

加密认证方法主要有IPSec[1]和SPM[2]. IPSec是一种端到端的方法, 并且它的大规模部署, 依赖于全局的PKI; SPM是一个自治系统到自治系统的解决方案, 每一对互相通信的自治系统拥有一对单独的临时的密钥做地址验证. 采用以上两种方法, IP源地址真实性的检查只能在目的主机或者目的自治系统.

过滤方法是一种预先处置的方法. 它利用预先生成的验证规则, 在路由器上过滤伪造源地址的分组. 代表性的方法有入口过滤 [3]、DPF[4]、SAVE[5]和HCF[6]. 入口过滤需要在边界网络全局部署; DPF将验证规则的部署位置从边界网络扩展到了核心网络, 并且支持增量部署, 但是它只能获得IP前缀粒度的地址验证; SAVE设计了一个新的协议在全网传递源地址验证规则信息, 但是协议不分层, 可部署性和可扩展性受到制约. 这些过滤方法的一个共同的问题在

于它们无法处理一个接入子网内的地址伪造的情形, 那时IP地址前缀是相同的、真实的.

追溯方法是一种事后处置的方法. 分组转发时, 记录路径信息, 并从目的端追踪伪造源地址分组的起源. 主要的工作包括SPIE[7], iTrace[1)], iTrace-CP[8], PPM[9]和DPM[10]. SPIE在路由器上记录路径信息; iTrace和iTrace-CP利用ICMP消息保留路径信息; PPM和DPM直接使用IP分组记录路径信息. 事后处置的设计思想, 复杂的追溯算法是这类方法的主要缺陷.

上述方法部分解决了IP源地址的验证问题, 但是还缺乏一个可行的有效的系统的解决方案. 本项目课题组提出了真实IPv6 源地址验证体系结构 [11], 并在国际互联网标准化组织互联网工程任务组(IETF)完成一项RFC标准 [12], 并提交标准草案多项 [2)~4)]. 论文接下来的章节将展开详细说明.

2 真实 IPv6 源地址验证体系结构

2.1 设计原则

在真实 IPv6 源地址验证体系结构的设计中, 以下设计原则需要考虑.

● 性能. 真实 IPv6 源地址验证体系结构的部署不应降低现有路由和交换设备的分组转发性能.

● 可扩展性. 真实 IPv6 源地址验证体系结构应该支持在整个互联网的大规模部署.

● 多重防御. 真实 IPv6 源地址验证体系结构应该支持分层的、部署在网络不同位置的、满足不同粒度需求的源地址验证.

● 松耦合. 真实 IPv6 源地址验证体系结构应允许不同运营商可以采用各自不同的实现, 系统各个部分相互独立, 每个部分可以实现各自粒度的真实地址检查, 每个部分的功能不依赖其他部分的实现.

● 支持增量部署. 真实 IPv6 源地址验证体系结构应该支持在全网渐进的、增量的部署. 部分部署时仍可以获得一定程度的真实源地址验证效果.

● 激励运营商. 真实 IPv6 源地址验证体系结构的设计应体现谁部署谁受益的原则, 部署真实 IPv6 源地址验证机制的运营商可以更加容易地发现和追踪网络中伪造源地址的分组, 保护自己的网络.

2.2 体系结构

要实现全网的真实 IPv6 源地址验证, 依赖单一的方法, 部署在单一层次的位置是不现实的. 因为互联网的路由和寻址是一个层次结构, 相对应的, 我们设计的真实 IPv6 源地址验证体系结构也应该是分层的. 这里我们划分为 3 个层次: 接入子网真实 IPv6 源地址验证、自治

1) Bellovin S, Leech M, Taylor T. ICMP Traceback messages. IETF Internet Draft, draft-ietf-itrace -03, 2003

2) Wu J, Ren G, Bi J, et al. A First-Hop Source Address Validation Solution for SAVA. IETF Internet Draft, draft-wu-sava-solution-firsthop-eap-00, 2007

3) Wu J, Bi J, Ren G, et al. Source Address Validation Architecture (SAVA) Framework. IETF Internet Draft, draft-wu-sava-framework-01, 2007

4) Wu J, Ferguson P, Bi J, et al. Source Address Verification Architecture Problem Statement. IETF Internet Draft, draft-sava-problem-statement-02, 2007

系统内真实 IPv6 源地址验证和自治系统间真实 IPv6 源地址验证, 如图 1 所示.

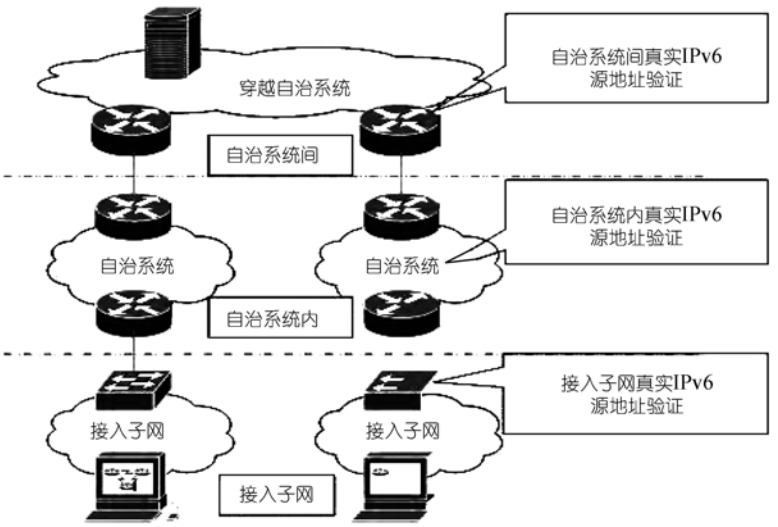

图 1　真实 IPv6 源地址验证体系结构

不同的层次实现不同粒度的 IPv6 源地址真实性验证. 在每一个层次, 允许不同的运营商采用不同的方法. 这一体系结构设计是一个整体结构的简单性和各部组成的灵活性的平衡.

2.2.1　接入子网真实 IPv6 源地址验证

这是体系结构的重要组成部分, 实现端系统 IP 地址一级的细粒度的真实 IPv6 源地址验证. 如果没有这一级验证, 一个主机依然可以伪造 IP 前缀相同的同一子网内其他主机的地址.

接入子网真实 IPv6 源地址验证具有以下特点:

- 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密切相关.
- 解决方案与端系统的接入方式密切相关.

针对目前网络中大量端系统通过交换机接入网络的情形, 我们采用的解决方案的主要思想是在交换机的端口和真实有效的 IP 地址之间实现动态绑定.

移动性是下一代互联网的一个重要特征, 对于基于移动 IPv6 协议接入互联网的移动节点, 有时会出现家乡地址(home address)和转交地址(care of address)无法同时满足真实 IPv6 源地址验证规则的情形, 需要依据情形进行分别处理, 而不是简单丢弃.

2.2.2　自治系统内真实 IPv6 源地址验证

这一层次相对简单. 其目标是实现IP地址前缀粒度的真实IPv6 源地址验证. 因为自治系统内的网络设备都在同一个管理机构管理之下, 主要的验证机制只需部署在运营商网络和接入网络的边界. 我们采用的解决方案的主要思想是在路由器上部署入口过滤验证规则, 这些规则把每一个路由器的接口和一组真实有效的IP地址前缀关联起来. 入口过滤 [3]是一个主要

采用的方案.

2.2.3 自治系统间真实 IPv6 源地址验证

这是最复杂的一个层次, 其目标是实现自治系统粒度的真实 IPv6 源地址验证.

自治系统间真实 IPv6 源地址验证具有如下特点:

- 需要在不同自治系统间协同工作.
- 机制必须简单轻权, 不给自治系统间的高速通信带来明显影响.

这一层次的协议机制我们将在第 3 节中展开阐述.

3 个层次的真实 IPv6 源地址验证, 将真实 IPv6 源地址验证的问题分解为 3 个部分, 分别实现端系统 IP 地址、IP 地址前缀和自治系统粒度的源地址验证. 在互联网的边界, 实现细粒度的端系统 IP 地址一级的验证; 而在高流量的核心网络中, 则通过简单并且可扩展的解决方案实现粗粒度的自治系统一级的验证, 有效地避免了真实IPv6源地址验证机制成为网络的瓶颈.

2.3 支持真实 IPv6 源地址验证体系结构的网络节点

真实 IPv6 源地址验证体系结构通过部署在各个网络节点上的解决方案来实现. 这些网络节点可以是交换机, 路由器或网关. 图 2 显示了一个支持真实 IPv6 源地址验证体系结构的网络节点的结构, 主要由以下逻辑部分组成:

- 转发信息数据库. 这一数据库保存着分组转发的路由和交换信息.
- 源地址验证信息数据库. 这一数据库保存着实现源地址验证的验证规则信息.
- 路由和交换协议. 这一模块在网络节点间互相交换转发信息, 更新转发信息数据库.
- 源地址验证协议. 这一模块在网络节点间互相交换源地址验证信息, 更新源地址验证信息数据库.
- 转发引擎. 这一模块依照转发信息数据库, 转发 IP 分组.
- 源地址验证引擎. 这一模块依照源地址验证信息数据库检查待转发分组源地址的真实性, 只有检查源地址真实, 才交由转发引擎转发.

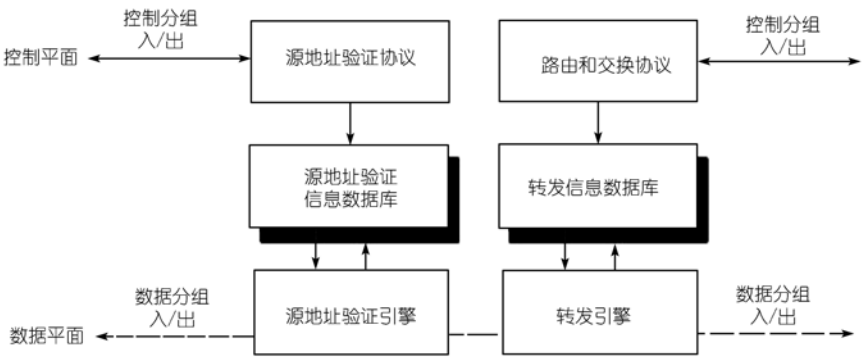

图 2 支持真实 IPv6 源地址验证体系结构的网络节点结构

转发信息数据库, 路由和交换协议,以及转发引擎是现有转发功能的主要组成部分. 而源地址验证信息数据库, 源地址验证协议和源地址验证引擎则实现了新增的源地址验证功能.

源地址验证协议模块是一个控制平面的模块, 可以通过软件实现, 或者实现在现有网络路由交换设备中, 或者实现在单独的控制服务器中. 源地址验证引擎模块是一个数据平面的模块, 这一模块通常实现在路由和交换设备的线卡中.

3 自治系统间真实 IPv6 源地址验证

3.1 方案概述

所有的支持真实 IPv6 源地址验证体系结构的自治系统共同组成一个信任联盟, 自治系统间真实 IPv6 源地址验证可以划分为两种情形:

● 两个支持真实 IPv6 源地址验证体系结构的自治系统直接互联, 以下简称“直接互联”.

● 两个支持真实 IPv6 源地址验证体系结构的自治系统不直接互联, 中间经过不部署真实 IPv6 源地址验证体系结构的自治系统, 以下简称“非直接互联”.

要生成源地址验证信息数据库中的验证规则, 在网络设备(路由器, 交换机)间需要交换信息, 根据这些交换信息类别的不同, 相应的真实 IPv6 源地址验证机制可以划分为两类:

● 基于路径或路由信息的机制. 验证规则的生成来自分组转发经过的路径或路由信息. 这类方法的好处是验证规则直接以 IP 地址前缀的形式表示, 缺陷是生成验证规则的网络节点之间需要直接互联, 共同配合生成验证规则.

● 基于标记或签名信息的机制. 这类机制通过增加附加的标记或者签名信息来验证 IP 分组源地址的真实性. 这类方案的好处是生成验证规则的网络节点之间不需要直接互联, 缺陷是签名和标记信息增加了额外的处理开销.

“直接互联”是我们设计中主要关注的情形, 我们提出了一种基于自治系统互联关系的验证机制应用于这种情形, 这是一个基于路径或路由信息的方案. 为了整个设计方案的完整性, 我们还为“非直接互联”情形设计了解决方案.

3.2 直接互联

对于两个支持真实 IPv6 源地址验证体系结构的自治系统直接互联的情形, 我们设计了一种基于自治系统互联关系生成验证规则的方案. 这一方案的基本思想如下. 它为自治系统边界路由器的每一个接口建立一个验证规则表, 这个验证规则表, 将一组真实有效的 IP 地址前缀和路由器接口关联起来. 验证规则的生成是基于自治系统互联关系. 自治系统的互联关系决定了域间路由的策略, 域间路由策略决定了 BGP 路由的配置, 而 BGP 路由表是生成域间转发表的主要信息. 自治系统互联关系相对稳定.

系统主要由 3 个部分组成: 验证规则生成引擎(VRGE), 验证引擎(VE)和 AS 编号到 IPv6 地址前缀映射服务器(AIMS), 如图 3 所示. 验证规则(VR)由验证规则生成引擎生成, 并最终以 IPv6 地址前缀的形式表示.

● VRGE 生成 VR, 每一个支持真实 IPv6 源地址验证体系结构的自治系统有一个 VRGE,

它和其他自治域的 VRGE 通信, 交换 VR 信息; 它和本自治域的 VE 通信, 配置 VR 信息.

- VE 加载 VRGE 生成的 VR, 并利用这些 VR 验证转发的分组.
- AIMS 维护着自治系统号到其对应拥有的 IPv6 地址前缀信息的映射.

自治系统(AS)间有 4 种关系: 服务者到客户、客户到服务者、对等互联、兄弟互联, 参见文献 [13]. 对于一个AS, VRO, VRC, VRS, VRP和VRE分别被定义为来自本自治域、客户自治域、兄弟互联自治域、服务者自治域和对等互联自治域的验证规则. EVRC, EVRS, EVRP和EVRE分别被定义为一个自治系统要向它的客户自治域、兄弟互联自治域、服务者自治域和对等互联自治域传递的VR.

一个自治系统的导出规则表是指自治系统依据互联关系向其相邻自治系统传递 VR 的规则. 我们定义如下:

- EVRC=VRO∪VRC∪VRS∪VRP∪VRE;
- EVRP=VRO∪VRC∪VRS;
- EVRS=VRO∪VRC∪VRS∪VRP∪VRE;
- EVRE=VRO∪VRC∪VRS.

即一个自治系统会把它所拥有的、它客户自治系统拥有的、它服务者自治系统拥有的、它兄弟互联自治系统拥有的、它对等互联自治系统拥有的 IP 地址前缀集合传递给它的客户自治系统和兄弟互联自治系统. 而只将它所拥有的、它客户自治系统拥有的、它兄弟互联自治系统拥有的 IP 地址前缀集合传递给它的服务者自治系统和对等互联自治系统.

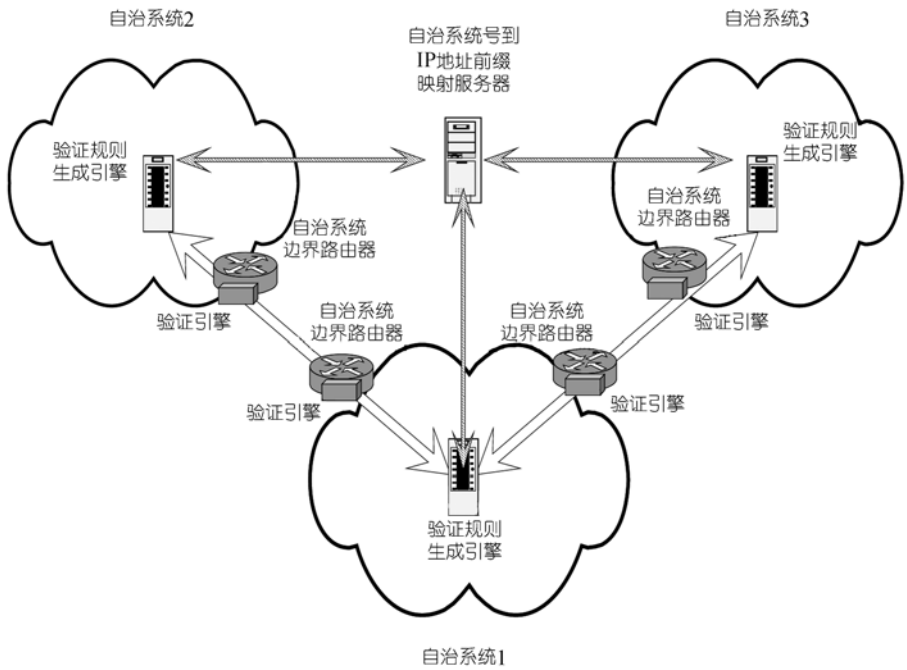

图 3 基于自治系统互联关系的自治系统间 IP 源地址验证方法

基于 AIMS 的支持, 只有自治系统编号在不同 VRGE 间传递, 并在 VRGE 处被映射为地址前缀集合, 降低了附加协议的传输开销. 自治系统互联关系相对稳定, 避免了路由震荡带来的影响, 只有当自治系统互联关系发生变化或者一个自治系统所拥有的地址前缀集合发生变化时, 才会引起 VR 的更新.

3.3 非直接互联

对于两个支持真实 IPv6 源地址验证体系结构的自治系统不直接互联的情形, 我们设计了一种基于轻权标记的自治系统间真实 IPv6 源地址验证方法. 其基本思想如下: 对于任何一对不直接相邻却都属于信任联盟的自治系统, 它们拥有一对单独的临时的标记. 当一个分组离开它自己发出的源自治系统, 且目的地址也在另一个属于信任联盟的自治系统内, 源自治系统的边界路由器依据目的地址, 查询预先协商好的标记表, 并把这个标记加在分组的一个 IPv6 协议扩展头上. 当一个分组到达目的自治系统, 如果分组的源地址属于一个在信任联盟内的自治系统, 目的自治系统的边界路由器根据分组 IP 源地址查找预先协商好的标记表, 如果匹配, 则去掉标记后转发给目的端, 如果不匹配, 则丢弃分组.

系统主要有 3 个组成部分: 注册服务器(REG)、自治系统控制服务器(ACS)和自治系统边界路由器(AER), 如图 4 所示.

- REG 维护着部署真实 IPv6 源地址验证体系结构的信任联盟的自治系统成员列表. 它响应 ACS 的请求, 提供信任联盟成员列表, 当成员列表发生变化时, 通知 ACS.
- 每一个部署这一机制的自治系统有一个 ACS. 它和注册服务器通信获得更新的信任联盟成员列表, 它和其他自治系统的 ACS 通信来交换协商标记信息, 它和所有的边界路由器通信来配置由标记信息组成的验证规则.
- AER 则负责在发送端将标记添加到分组中或者在接收端将标记检查和移除.

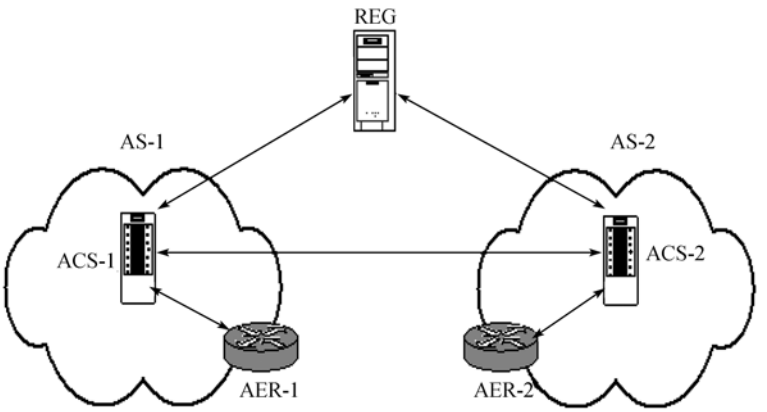

图 4 基于标记的自治系统间真实 IPv6 源地址验证方法

标记附加在 IPv6 分组的一个扩展头上, 目前我们使用 hop-by-hop 扩展头, 运用一个 128 位的随机数来做签名, 如图 5 所示.

假设自治系统间的主干网不容易被窃听, 猜测标记的方法在文献 [2]中进行了阐述, 这是

相对困难的, 我们可以通过增大标记长度和动态更新标记来进一步增加标记的复杂性. 由于标记由随机数生成, 增加的IP分组处理开销极小. 为了不造成携带真实IPv6 源地址的分组被误判而丢弃, 在标记的动态更新中, 保留原标记和新标记同时有效一段时间. 在部署实验中, 我们根据实验网络的运行情形设定这一时间为 5 s, 在标记更新过程中, 没有携带真实IPv6 源地址的分组因为被误判而丢弃.

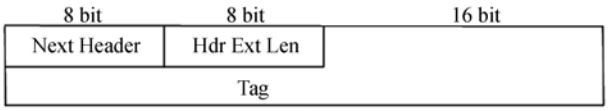

图 5 携带标记的 IPv6 扩展头格式

3.4 可扩展性分析

自治系统间的真实 IPv6 源地址验证方法具有可扩展性, 可以良好地支持加入信任联盟的自治系统数量的增加, 下面对此进行分析.

为了便于分析, 将互联网抽象为无向图 $G(W; N; F)$. 其中 W 是节点集合, 每个节点表示一个 AS; $N \in W$, 是网络中部署了 IP 源地址验证机制的 AS 集合, 即信任联盟集合; F 是边的集合, 每条边表示 AS 间的直接互联.

做如下设定:

- n 是信任联盟中需要两两协商签名的元素个数;
- t 是 G 中所有的穿越 AS 节点数;
- a 是 G 中总的 AS 数;
- v 是新加入信任联盟的 AS;
- 若 $\exists v_i \in N$, 并且边 $vv_i \in F$, 则在 v 和 v_i 间部署基于自治系统互联关系的验证方法, v 和 v_i 合并为一个 N 中的 AS 子集, 对外作为一个整体和其他元素协商标记.

引理 1 n 的最大值是连通图 G 的独立数.

证明 由前述设定可知: n 是信任联盟中需要两两协商签名的元素个数.

若 $\exists v_i \in N$, 并且边 $vv_i \in F$, 则在 v 和 v_i 间部署基于自治系统互联关系的验证方法, v 和 v_i 合并为一个 N 中的 AS 子集, 对外作为一个整体和其他元素协商标记.

又由连通图 G 独立数的定义: 设 I 包含于 $V(G)$, I 中任 2 顶不邻, 则称 I 是图 G 的一个独立集; 任取 $u \in V(G)-I$, $I \cup \{u\}$不是独立集, 则称 I 是极大独立集; G 中已无独立集 I_1, 使得$|I_1| > |I|$, 则称 I 是 G 的最大独立集, 这时, 记$\beta(G)=|I|$, $\beta(G)$叫做 G 的独立数.

因此 $n \leqslant$连通图 G 的独立数.

引理 2 G 中所有的穿越 AS 节点组成 G 的最小支配集.

证明 由连通图 G 的最小支配集的定义: D 包含于 $V(G)$称为图 G 的一个支配集, 若任何顶点 $u \in V(G)$, 要么 $u \in D$, 要么 u 与 D 内一顶相邻. 一个支配集称为极小支配集, 若它的任何真子集皆非支配集. D_0 是一个支配集, 但已无支配集 D_1, 使得$|D_1| < |D_0|$, 则称 D_0 是最小支配集, 这时记$\gamma(G)=|D_0|$, $\gamma(G)$叫做 G 的支配数.

G 中所有的节点, 或者是穿越自治系统节点, 或者是末端自治系统节点(stub AS), 而末端自治系统节点必定和一个或几个穿越自治系统相邻.

综上, G 中所有的穿越 AS 节点组成 G 的最小支配集.

定理 信任联盟中需要两两协商签名的元素最大个数小于等于互联网内总 AS 数和穿越 AS 数的差.

证明 由已知图论定理, 连通图 G 的独立数和支配数的和等于图 G 的顶点数.

由引理 1, $n \leqslant$连通图 G 的独立数, 由引理 2, t 是 G 的支配数, 所以 $n \leqslant a - t$, 定理得证.

在真实 IPv6 源地址验证体系结构的增量部署过程中, 因为网络 AS 互联拓扑符合幂率分布, 当 n 达到最大可能值 $a - t$ 时, 任何一个穿越 AS 加入 N 都会降低 n. 当 $N = W$ 时, $n = 1$, 只需部署基于自治系统互联关系的验证方法. 而由于 n 的大小是受限的, 因此这一方法具有可扩展性.

4 部署

真实 IPv6 源地址验证体系结构的实现系统已经在 CNGI-CERNET2 网络上部署、运行和测试. 有多家国内外的设备厂商参与了相关机制的实现.

CERNET2 是中国下一代互联网(CNGI)的主干网之一, 它以 2.5~10 Gbps 的速度,连接了分布在全国 20 个城市的 25 个核心节点. CNGI-CERNET2 主干网是纯 IPv6 的网络. CNGI-CERNET2 主干网、驻地网、国内互联和国际交换中心(CNGI-6IX)都拥有全局独立的自治系统编号, 共同提供了一个多自治系统的实验环境.

真实 IPv6 源地址验证体系结构的部署分布在与 CNGI-CERNET2 主干网互联的 12 所高校, 如图 6 所示. 这些高校有清华大学、北京大学、北京邮电大学、上海交通大学、华中科技大学、东南大学、华南理工大学、东北大学、西安交通大学、山东大学、电子科技大学和重庆大学.

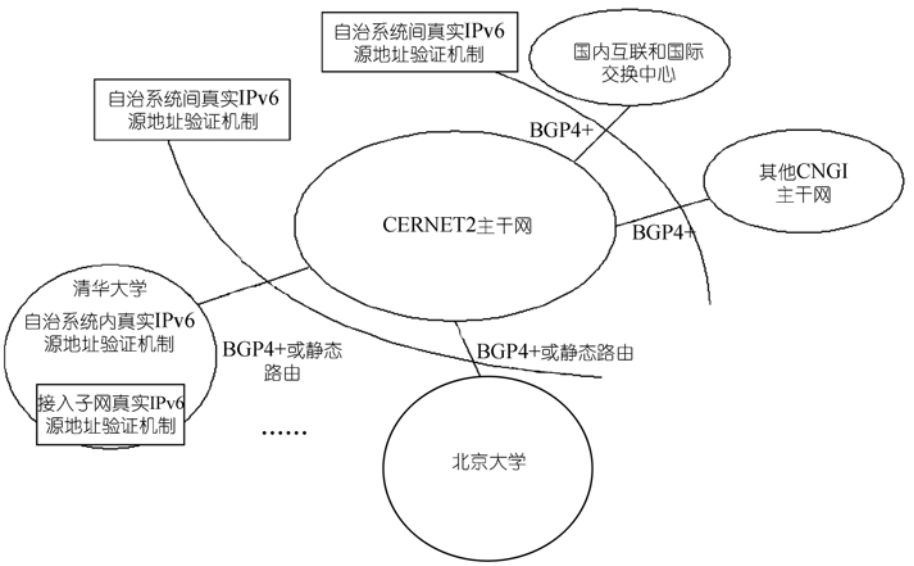

图 6 真实 IPv6 源地址验证体系结构在 CNGI-CERNET2 的部署

各个高校都通过自治系统间真实IPv6源地址验证机制与CNGI-CERNET2主干网互联, 其中清华大学部署和实验了接入子网, 自治系统内和自治系统间 3 个层次的真实 IPv6 源地址验证机制.

实验中完成了对真实IPv6 源地址验证体系结构各个层次解决方案的功能性和稳定性测试, 实验床的实验结果是成功的. 详细的实验床设计和结果已经提交国际互联网标准化组织互联网工程任务组(IETF), 被批准成为RFC5210[12].

5 结论和下一步的工作

论文提出了一种"真实 IPv6 源地址验证体系结构", 对互联网中转发分组的源地址进行验证, 使每一个转发分组的 IP 源地址都是真实的. 这一体系结构将源地址验证的问题划分为 3 个部分: 接入子网内、自治系统内和自治系统间. 本文阐述了体系结构和相关机制的设计. 这一体系结构具有轻权、松耦合、多重防御的特点, 支持增量部署, 对网络管理、安全、计费以及应用都有所帮助. 我们下一步的工作是为各个支持真实 IPv6 源地址验证体系结构的自治系统建立合适的信任模型, 并进一步改进和完善体系结构中各个层次的解决方案.

参考文献

1 Kent S, Atkinson R. Security Architecture for the Internet Protocol. IETF, RFC2401. 1998

2 Bremler-Barr A, Levy H. Spoofing prevention method. In: Proc IEEE INFOCOM. Washington: IEEE, 2005. 536—547

3 Ferguson P, Senie D. Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing. IETF, RFC2827. 2000

4 Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. ACM SIGCOMM Comput Commun Rev, 2001, 31(4): 15—26

5 Li J, Mirkovic J, Wang M, et al. SAVE: source address validity enforcement protocol. In: Proc IEEE INFOCOM. Washington: IEEE, 2002. 3: 1557—1566

6 Jin C, Wang H. Hop-count filtering: an effective defense against spoofed DDoS traffic. In: Proc ACM CCS. New York: ACM, 2003. 30—41

7 Snoeren A, Partridge C, Sanchez L, et al. A Hash-based IP traceback. ACM SIGCOMM Comput Commun Rev, 2001, 31(4): 3—14

8 Lee H, Thing V, Xu Y, et al. ICMP traceback with cumulative path, an effcient solution for IP traceback. Information and Communications Security. Berlin: Springer, 2003. 124—135

9 Savage S, Wetherall D, Karlin A, et al. Pratical network support for IP traceback. ACM SIGCOMM, Comput Commun Rev, 2000, 30(4): 295—306

10 Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Commun Lett, 2003, 7(4): 162—164 [DOI]

11 Wu J, Ren G, Li X. Source address validation: architecture and protocol design. In: ICNP, 2007

12 Wu J, Bi J, Li X, et al. A Source Address Validation Architecture (SAVA) Testbed and Experiences. IETF, RFC5210. 2008

13 Gao L. On inferring autonomous system relationships in the internet. IEEE ACM Trans Netw, 2001, 9(6): 733—745 [DOI]