自治域间真实源地址验证方法及技术实现

李　杰,吴建平,徐　恪

(清华大学计算机科学与技术系　北京 100084)

摘　要　随着网络规模的不断扩大和应用方式的日趋复杂,互联网正面临着漏洞多、可信度低等多样化的安全威胁,从可信任的角度出发,确保源 IP 地址的真实性是实现可信任下一代互联网的重要基础和前提。本文从体系结构出发,对基于真实 IPv6 源地址的网络寻址体系结构的域间、域内和接入子网 3 个层面的实现策略和关键进行了说明,并详细介绍了自治域间真实源地址验证方法的原理机制和技术实现。

关键词　真实源 IP 地址验证;自治域间;网络安全

1　概述

随着互联网的日益普及,异构环境、普适计算、泛在联网、移动接入和海量流媒体的等新应用的不断涌现,人们对互联网的规模、功能和性能等方面的需求越来越高。以 IPv4 协议为核心技术的互联网面临着越来越严重的技术挑战,其中网络安全漏洞多、可信度低等问题尤为突出,难以满足用户需求,不能保障高质可信的网络服务,缺乏更大规模扩展的有效机制。可以说,互联网可信任性的缺乏造成的安全问题已经相当严重。

4　RFC3633. IPv6 prefix options for dynamic host configuration protocol(DHCP) version 6, December 2003

5　RFC4818. RADIUS delegated-IPv6-prefix attribute, April 2007

6　RFC4862. IPv6 stateless address autoconfiguration, September 2007

7　RFC5072. IP version 6 over PPP, September 2007

User Access Authentication in IPv6 Transition

Hu Jie, Wang Qian, Chen Yunqing

(Beijing Research Institute of China Telecom Co., Ltd., Beijing 100035, China)

Abstract　Firstly, we discussed some Internet access related protocols, such as PPP, NDP/SLAAC, DHCP and Radius, then analyzed some new issues when IPv6 service is introduced to ISP, and also give some solutions to solve the problems.

Key words　IPv6, transition, access authentication, authorization and accounting　(收稿日期:2011-03-18)

真实源地址验证是可信任互联网的重要技术基础。从可信任的角度出发,真实IP地址访问的问题实际上是地址的归属关系问题,也就是说:网络实体发出的报文只应携带它拥有的地址,报文只应被拥有其源地址的实体发出,真实源IP地址验证则是对实体发出的报文进行检验和追溯进而确保实体本身、信息来源、信息内容的真实性。在当前的互联网中,地址是主机的标识,报文转发一般不对源地址做真实性检查,导致无法在网络层建立信任关系,也不能提供端到端的信任,各种应用独自实施认证,不但效率低下、无法统一,而且滋生了许多难以解决的网络威胁。因此,研究和实现真实源地址验证,为上层安全服务提供一个可信任的信息基础设施,对于可信任的下一代互联网的发展和构建具有相当重大的意义。

当前,互联网中源地址伪造问题主要表现在如下几个层面。

(1)安全层面,DoS/DDoS、僵尸网络(botnet)等多种攻击都依赖于地址欺骗,这些攻击已经对网络服务造成了难以估量的损失。

(2)网络管理层面,源地址伪造使得网络管理者对大量攻击事件的源无法追溯和监控。

(3)网络计量层面,管理机构无法获得准确的统计信息作为决策基础,垃圾流量(SPAM)使基于源地址的计费无法实现,大量伪造源地址攻击占用大量网络资源,造成大量经济损失。时至今日,源IP地址的真实性验证已给互联网的安全运营和可持续发展提出了诸多挑战。致力于互联网的长远利益,互联网只有提供高可信的网络服务,才能满足未来发展的需求。因此,确保源IP地址的真实性是实现可信任下一代互联网的核心问题。

2 真实地址验证体系结构及实现策略

2.1 体系结构

互联网的路由和寻址是一个层次结构,要实现全网的真实源IP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。为了解决全网真实源IP地址问题,清华大学吴建平教授等从网络体系结构的层面上,提出了基于真实IPv6源地址的网络寻址体系结构(source address validation architecture, SAVA)[1],在IETF完成一项RFC标准[2],提交3项标准草案[3-5],并以此为基础推动IETF成立专门工作组SAVI(source address validation improvements),使中国在参与IETF国际标准方面实现了新的突破,产生了重要的国际影响。按照互联网的层次结构,SAVA不同层次的机制分别在主机、IP地址前缀和自治域粒度上保证源IP地址的真实性。基于网络本身的分层结构,真实源地址验证体系结构被分为域间真实地址验证、域内真实地址验证和接入子网真实地址验证3个层次的真实IPv6源地址网络寻址系统,它们有机地组合在一起,共同形成真实源地址验证结构框架,如图1所示。

2.2 实现策略

在真实源地址验证体系结构中,接入子网源地址验证通过动态创建MAC地址、交换机端口和真实源IP地址间的关联,保证主机不能伪造接入子网中其他主机的地址;域内源地址验证要求域内路由器为每个路由器接口维护一个真实地址前缀表,对边缘接入网络应用入口过滤(ingress filtering)是解决方案的一种。根据自治域邻接关系,SAVA设计了两种生成域间验证规则的机制:应用于非相邻自治域间的基于端到端轻量级签名的域间真实源地址验证方法和应用于相邻自治域间的基于路由信息的真实源地址验证方法。其中,基于端到端轻量级签名的域间真实源地址验证方法的基本思想是:将部署本方法的域组成一个信任联盟,联盟内各个域的控制服务器通过端到端的方式交互彼此的地址空间信息和协商签名信息,然后由域的边界路由器在发送的IPv6分组中增加IPv6扩展报头存放签名,并在接收的分组中检查签名是否正确。基于路由信息的真实源地址验证方法的基本思想是:利用自治域互联关系,在自治系统边界路由器上生成与每一个路由器接口关联的真实IPv6源地址验证规则表,并利用其对伪造IPv6源地址的分组进行验证检查。

SAVA体系结构具有以下新特点:

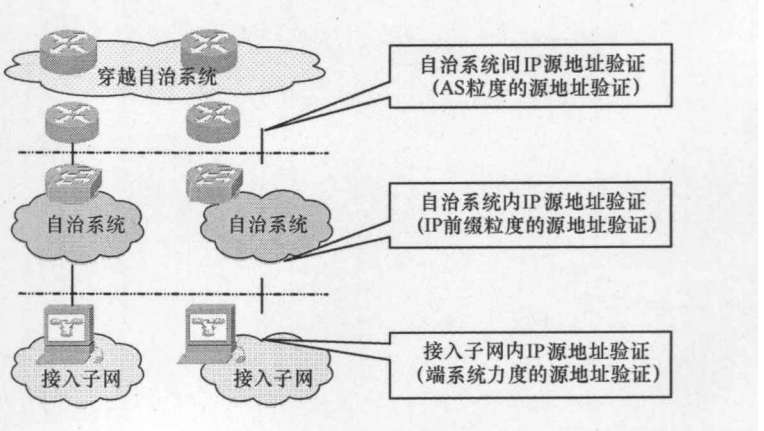

图1 SAVA源地址验证体系结构

- 简单,实现方案的存储和处理开销非常小,对真实源地址的网络分组的流量基本没有影响;
- 松耦合,真实源地址验证体系结构划分为自治系统内、自治系统间和接入子网3个部分,各个部分相互独立,每个部分可以实现不同粒度的真实地址检查,每个部分的功能实现不依赖于其他部分;
- 多重防御,对于一个伪造源地址的分组,设置接入子网、自治域内和自治域间3道防线实现真实源地址验证体系结构;
- 支持增量部署,真实源地址验证体系结构支持在全网渐进、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;
- 便于对上层可信任应用提供支持,真实源地址验证体系结构可以很好地为上层可信任的安全服务和应用提供基础设施的支持;
- 激励运营商部署,真实源地址验证体系结构的设计体现了"谁部署,谁受益"的原则,部署真实地址访问机制的网络可以更加容易地发现和追踪网络中伪造源地址的分组,保护自身网络。

SAVA通过IPv6源地址验证,为解决下一代互联网的安全隐患提供了重要保证,成为可信任下一代互联网的重要技术基础。

3 自治域间源地址验证方法及技术实现

域间源地址验证是SAVA体系结构中最困难和复杂的部分,其目标是实现自治域粒度的真实源地址验证。近年来,域间真实源地址验证方法研究得到了国际学术界和工业界的高度重视,开展了许多相关的研究、取得了一些有益的进展。典型的有Bremler-Barr等人提出的基于源—目的自治域对应密钥的域间IP欺骗过滤机制SPM[6],在SPM中每一对互为通信对端的自治域维护一对私密、惟一的密钥验证源地址的真实性,源域通过添加密钥可保证源地址的真实性,目的域通过检查密钥验证源地址的真实性。SPM适合应用在早期的部署真实地址寻址机制的自治域较少、分布稀疏的网络环境中,采用该方案可实现自治域粒度的真实源地址验证。

APPA[7]在SPM的基础上进行了有益的改进,其实现思想是:由部署验证机制的自治域作为成员单位组建一个信任联盟,联盟内每一对互为通信对端的成员自治域都各自维护有一对分别用来生成和验证标签的状态机,源域依据相应状态机生成确保源于本域的数据报文源地址真实性的标签并添加在报文扩展头中,目的域依据同样的状态机去验证标签,若验证通过则判定源地址是真实可信的,从而实现源地址前缀的验证。

该方法的有效实施需要由联盟注册服务器、控制服务器以及边界路由器协同工作完成,如图2所示。在每一成员域内部,都配属有一台控制服务器,该服务器主要负有验证规则部署职能:完成注册并获取联盟成员列表以及控制服务器地址列表;与其他控制服务器交互地址前缀信息并协商生成标签所需的状态机;控制边界路由器,配置地址前缀与自治域的映射列表和进出方向的状态机列表。在整个信任联盟内部,配属有一台联盟注册服务器,其负有成员信息管理职能,用于动态维护信任联盟成员信息,管控成员的加盟及退出,向控制服务器实时发布联盟成员信息。

该方法引入了一种基于轻量级标签的自治域端到自治域端的加密认证机制,在确保本域的地址不被伪造的同时,还可验证其他来源地址的真实性,具有一定的增量部署特点和激励机制,标签的自动更新降低了控制服务器之间的通信开销,适合部署在联盟规模较小的网络环境中。

4 层次化的域间真实源地址验证方法及技术实现

层次化的域间真实源地址验证方法是一种可自下而上分层级建立信任联盟、基于轻量级标签替换的自治域间真实源地址验证方法。

4.1 基本思想

该方法采用一种基于轻量级标签替换的自治域端到自治域端的加密认证机制,通过自下而上的分层,将部署了该方法的所有自治域(AS)划分为多层级信任联盟,每一层级联盟可以作为成员(抽象为一个系统整体)参加更高层级的联盟,使得整个信任联盟系统构成一种具有源地址验证功能的、层次化的体系结构。

在数据层面,在层次化的信任联盟体系结构中,通过分层数据通信被扩展为3类。

第一类,单一信任联盟数据通信,某一最低层级信任联盟内成员AS互为通信对端,报文仅在该联盟内部网络中交互。在此类数据通信场景中,源地址验证过程无需标签替换,只需依据该最低层级联盟状态机,采用传统的验

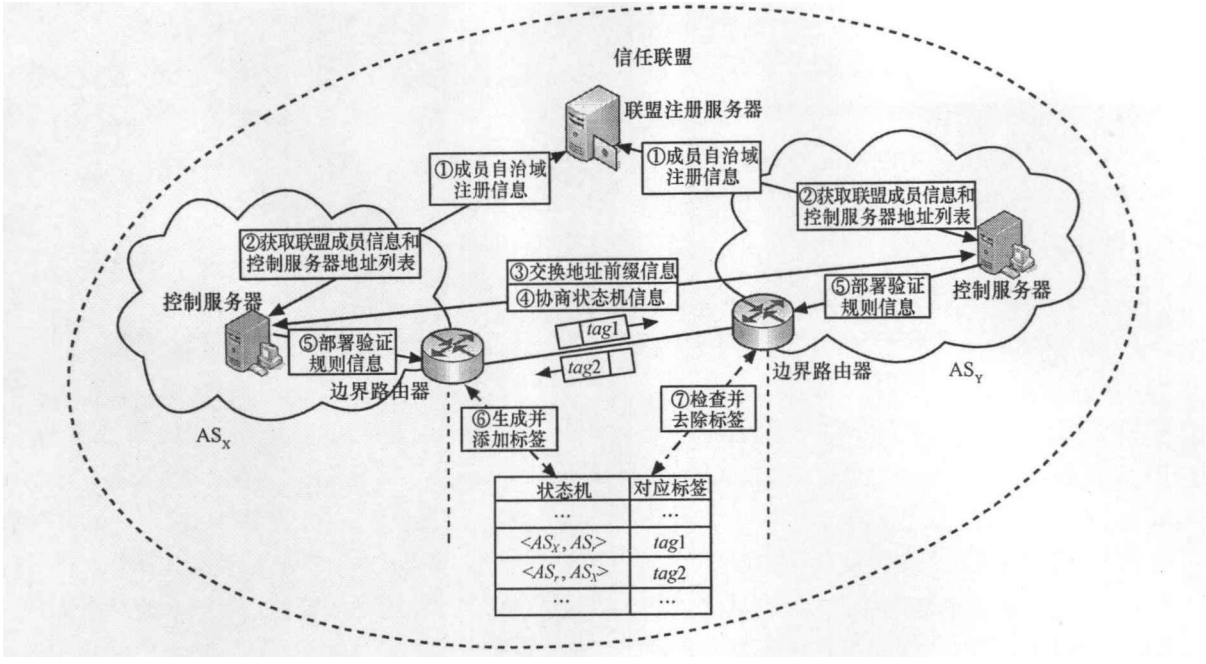

图 2　基于端到端轻量级标签的域间真实源地址验证方法

证机制即可有效实现源地址验证。

第二类,跨信任联盟数据通信,隶属于不同层级信任联盟的 AS 互为通信对端,数据报文需要在跨越联盟的网络中交互,在此类数据通信场景中,处在不同层级联盟中的源 AS 和目的 AS 间无需通过建立状态机双向共享,而是通过引入 TAE 和联盟映射状态机充当跨联盟数据报文交互的"中继代理",完成自下而上的逐级标签替换,延续报文源地址真实性的信任关系,实现源地址验证,如图 3 所示。

第三类,非信任联盟数据通信.信任联盟中的 AS 与其他非信任联盟 AS 间进行的数据通信,在此类数据通信场景中无需源地址验证也不涉及标签的任何操作。

4.2　体系结构

层次化的域间源地址验证方法,允许联盟管理机构依据实际情况灵活选取不同的划分原则和组合模式构建层次化的信任联盟体系结构。首先以 AS 为单位成员,将部署本方法的所有 AS 按照相同属性聚合成多个最低层级信任联盟,然后再以这些最低层级信任联盟为单位成员,依据一定的划分原则聚合成更高层级的信任联盟,由此自下而上地不断以同一层级的信任联盟为单位嵌套式聚合,直至形成一个最高层级信任联盟,如图 3 所示。

4.3　技术实现

在控制层面,该方法需要由 RES、ACS 以及 AER/TAER 协同工作完成验证策略的协商和决策,生成相应的验证控制规则和指令,控制数据报文的验证动作。

在技术层面,为有效抵御针对验证规则部署和成员信息管理过程的窃听、截获和破解等安全威胁,增强验证机制的健壮性,该方法着重考虑了以下 4 点关键设计。

(1)状态机的周期更替机制

为每一个状态机设置了启用和到期时间,在到期时间来临后,互为通信对端的源域和目的域必须同步完成新旧状态机更替,确保了生成的标签在一定周期内的时效性、惟一性和可靠性。

(2)时间同步

要求 RES 通过 NTP 协议定期向各成员 ACS 发送时间校准报文,由 ACS 实时校准本域 AER/TAER 的时间,同时在各 AER/TAER 上设置一个共享时间片,规定在该时间片内,刚刚到期的标签与新的标签均被认为是有效的,从而确保各成员 AER/TAER 之间的时间同步,进而实现状态机的同步。

(3)安全信道

立足现有域间链路,采用开启 TCP 拦截和 Diffie-Hellman 协议结合的方式,通过 TCP 连接建立起验证规则信息交互的安全信道。

(4)TAER 工作模式

允许 TAER 在进行标签替换的同时可依据网络安全等级灵活设置工作模式(直接替换模式或替换并验证模式)。

层次化域间真实源地址验证方法具有以下特点:

· 通过分层构建多级并存、层次化的体系结构;

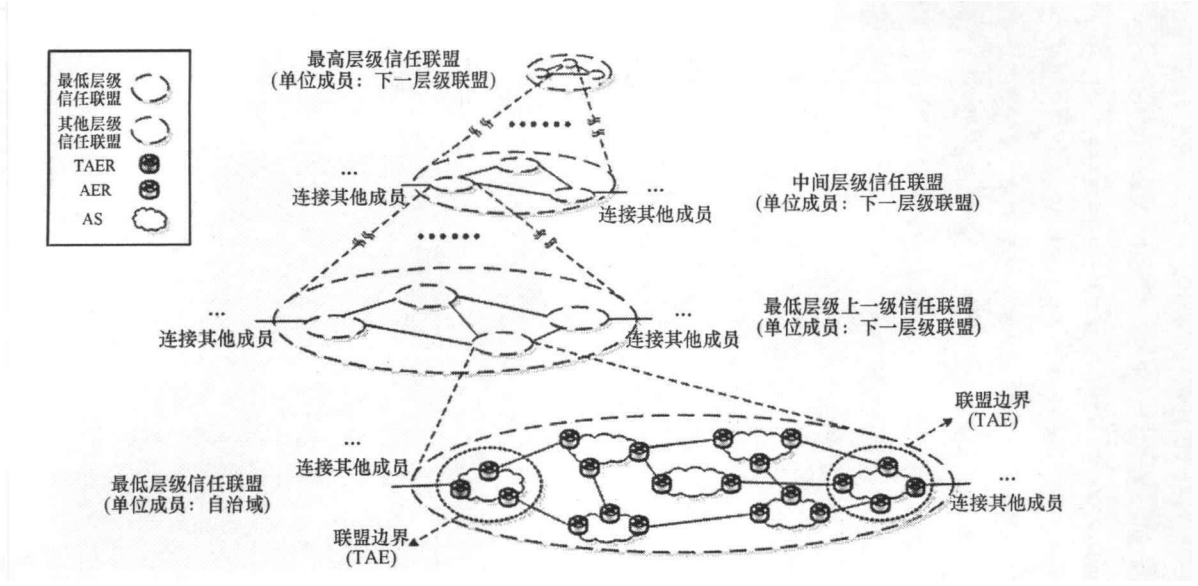

图3 基于标签替换的域间真实源地址验证方法构建的层次化的信任联盟体系结构

- 通过引入实现标签替换的“中继代理”联盟边界，将每一层级联盟和外界网络隔离，在保持域间高速通信的同时使得不同层级联盟内部的网络环境彼此互不可见、互无影响；
- 有效降低了边界路由设备的状态机存储、查找、同步和处理等验证开销，确保处在不同层级联盟内的通信对端AS在不建立状态机双向共享的情况下仍然可以实现全局性的源地址验证，实验证明，该方法能够确保即使在规模较大的层次化信任联盟中仍然可以实现AER/TAER状态机的存储、查找、管理和处理开销的大幅缩减，有效缓解状态机同步难度，保证验证的简单、轻权和高速、高效。

4.4 实验部署

目前，真实IPv6源地址验证体系结构的实现系统已经在CNGI-CERNET2网络上试验性部署、运行和测试，并且吸引了多家国内外机构、运营商和设备制造商参与实现，这些机构都拥有多个全局独立的自治域编号，为域间真实源地址验证方案的实现提供了一个多自治域的实验环境。在实验中采用的AER/TAER、ACS和REG验证设备分别由盛科网络(苏州)有限公司(以下简称盛科)和比威网络技术有限公司(以下简称比威)负责研制。盛科和比威聚焦于互联网安全应用，分别基于自主研发的核心芯片和板卡，研制了专用验证设备。经过系统测试和实验验证，这些设备能够有效完成在报文中添加、检验和去除签名字段等验证功能，实现了真实源地址访问并有效防御了源地址伪造。目前，盛科系列AER/TAER验证设备采用标准1RU固定配置盒式机架设计，提供1G/10G以太网接口支持高带宽应用全线速转发及高于500 Mbit/s的路由能力，具有较为完善的硬件和软件冗余机制设计(包含电源热插拔冗余设计、系统实时监测保护机制)以及可扩展的系统架构。比威系列AER/TAER则在原有边界路由交换设备上进行增加板卡或系统固件升级，从而实现源地址验证功能。ACS和REG则采用由盛科研制的配备验证专用的软硬件平台的商用服务器。

依据CNGI-CERNET2实际网络环境，在域间源地址验证方案实际部署时，验证设备的部署点分别选取在：①盛科设备应用在CNGI-CERNET2原有自治域(管理域)内的边界设备(核心和边界节点中的路由器或三层交换机)上，以旁挂方式与CNGI-CERNET2原有自治域(管理域)内的商用边界设备(核心和边界节点中的路由器或三层交换机)配合使用，增加源地址验证功能；②比威设备则在CNGI-CERNET2原有自治域(管理域)内的比威边界设备(核心和边界节点中的路由器或三层交换机)上，在不影响原有设备功能、性能和正常运行的前提下，通过增加板卡或系统固件升级的方式，增加源地址验证功能。

经过对CNGI-CERNET2实际部署条件的综合考量，可行的部署方案确定为阶段性部署：阶段一，部署可升级实现域间源地址验证功能的节点(升级比威设备)；阶段二，部署增配验证设备实现域间源地址验证功能的节点(旁挂盛科设备)；阶段三，部署其他加入信任联盟的机构或单位节

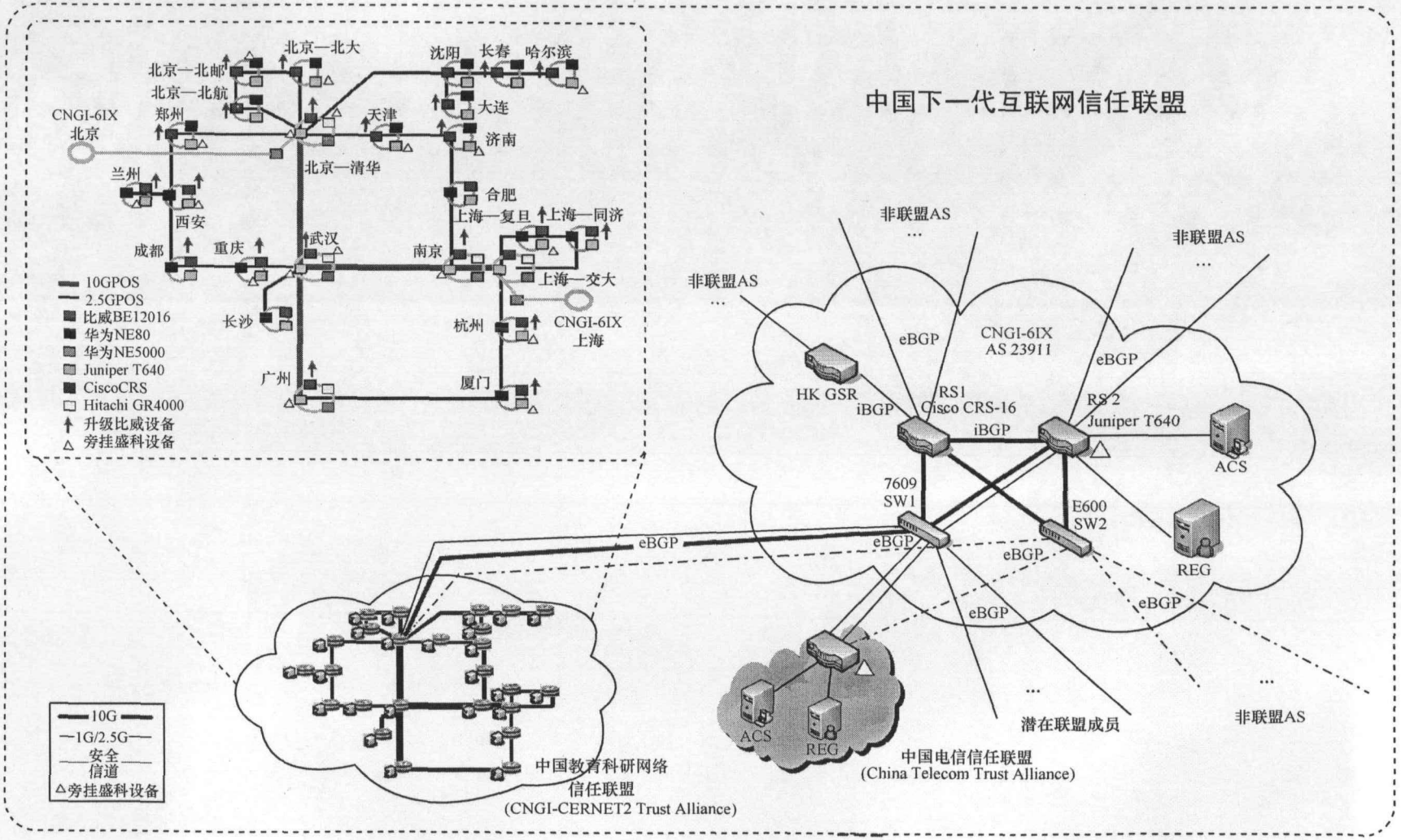

图 4　CNGI-CERNET2 自治域间真实源地址验证方案试验性部署示意图

点(CNGI-6IX、中国电信等)。部署可行方案示意如图4所示。实验结果表明域间真实源地址验证方法可以提供完整、有效的地址真实性保证功能。

5 结束语

作为可信任下一代互联网的重要基础,真实源地址验证策略为上层应用提供了一个方便、有效的平台。本文介绍了真实源地址验证体系结构,域间、域内和接入子网3个层面的真实地址寻址实现策略,并对在真实源地址验证结构框架下,自治域间真实源地址验证的主要原理、机制和技术实现做了详细介绍。

参考文献

1 Wu J, Ren G, Li X. Source address validation: architecture and protocol design. In: Proceedings of the 15th IEEE International Conference on Network Protocols(ICNP), Beijing, China, 2007

2 RFC5210. A source address validation architecture (SAVA) testbed and experiences, 2008

3 Wu J, Ren G, Bi J, *et al*. A first-hop source address validation solution for SAVA. Internet-Draft draft-wu-sava-solution-firsthop-eap-00.txt, 2007

4 Wu J, Bi J, Ren G, *et al*. Source address validation architecture(SAVA) framework. Internet-Draft draft-wu-sava-framework-01.txt, 2007

5 Wu J, Bi J, Li X, *et al*. SAVA testbed and experiences to date, Internet-Draft, draft-wu-sava-testbed-experience-02.txt, 2007

6 Bremler-Barr A, Levy H. Spoofing prevention method. In: Proc of IEEE Infocom. Washington, IEEE, 2005

7 Shen Y, Bi J, Wu J P, *et al*. A two-level source address spoofing prevention based on automatic signature and verification mechanism. IEEE Symposium on Computers and Communications (ISCC), Marrakech, 2008

8 Wu J P, Xu K. Next generation internet architecture. Journal of Computer Science Technology, 2006, 21(5): 726~734

9 Wu J P, Liu Y, Wu Q. The research progress on theory of next generation internet architecture. Science in China, 2008, 38(10): 1540~1564

10 Wu J P, Wu Q, Xu K. Research and exploration of next generation internet architecture. Chinese Journal of Computers, 2008, 31(9): 1536~1548

11 Xie L, Bi J, Wu J P. An authentication based source address spoofing prevention method deployed in IPv6 edge network. In: ICCS, 2007

12 毕军,吴建平,程祥斌.下一代互联网真实地址寻址技术实现及试验情况,电信科学,2008,(1)

13 陈仲华.IPv6技术在物联网中的应用.电信科学,2010,26(4)

14 张琳峰,张岚,黎明雪.cdma2000移动网IPv6演进策略探讨.电信科学,2010,26(5)

15 朱永庆,邹洁.三网融合与IPv6应用探讨.电信科学,2010,26(7)

16 王帅,沈军,金华敏.电信IPv6网络安全保障体系研究.电信科学,2010,26(7)

17 陈琦.IPv6环境下的PPPoE接入技术研究.电信科学,2010.26(7)

18 赵慧玲,陈运清,邝剑萍,刘谦.下一代互联网在湖南电信网络的试商用部署实践.电信科学,2010,26(7)

Inter Domain Authenticated Source Address Validation Solution: Principle and Technology Implementation

Li Jie, Wu Jianping, Xv Ke

(Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

Abstract With the increasing scale and complexity of the size and applications grow so quickly that security flaws and low trustworthy is challenging and restricting the development of Internet. For the sake of the secure operation and sustainable development of the Internet, next generation Internet must focus on the trustworthy and reliableness. The foundation of trustworthy is authenticated source IP address. From the point of view of architecture, this paper introduces the implementation schemes and key technologies of the IPv6 source address validation architecture(SAVA). SAVA was divided into three levels: first-hop, local subnet source address validation, intra-domain source address validation, and inter-domain source address validation, which are explained and discussed successively in this paper. Specially, we also introduce the key scheme and technology implementation of inter-domain authenticated source address validation solution in details.

Key words inter domain, IP source address validation, network security (收稿日期:2011-03-18)