软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(6):1274−1294 [doi: 10.3724/SP.J.1001.2013.04284]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

一种基于责任域的安全路由体系*

卢宁宁, 张宏科

(北京交通大学 下一代互联网互联设备国家工程实验室,北京 100044)

通讯作者: 卢宁宁, E-mail: radioboy@126.com

摘 要: 为了解决前缀劫持、路由伪造和源地址欺骗问题,设计了一种路由体系——基于责任域的安全路由体系(accountability realm based secure routing architecture,简称 Arbra).首先,提出了自治系统到责任域的映射方法和基于责任域的两级路由结构,责任域是具有独立管理主体的网络,也是 Arbra 网络拓扑的基本元素,因为它为内部用户的网络行为负责,所以称做责任域;其次,建立了基于责任域的路由体系设计框架,主要包括混合寻址方案、核心路由协议、标签映射协议、分组转发流程和公钥管理机制等研究内容;最后,比较了 Arbra 和其他著名路由结构(IPv4/v6,LISP,AIP)的异同,分析了 Arbra 的安全性、可扩展性、通信性能和部署代价.研究结果表明:(1) Arbra 具有的分布式信任模型,不仅有利于抵御前缀劫持、路由伪造和源地址欺骗攻击,而且还给许多其他网络安全问题的解决奠定了基础;(2) Arbra 具有优良的可扩展性,路由表的规模较小;(3) Arbra 具有合理的通信性能和部署代价.该研究成果可以看做是以网络安全为视角对未来信息网络体系结构的有益探索.

关键词: 前缀劫持;路由伪造;源地址欺骗;责任域;域间路由

中图法分类号: TP309 **文献标识码**: A

中文引用格式: 卢宁宁,张宏科.一种基于责任域的安全路由体系.软件学报,2013,24(6):1274−1294. http://www.jos.org.cn/1000-9825/4284.htm

英文引用格式: Lu NN, Zhang HK. Secure routing architecture based on accountability realm. Ruan Jian Xue Bao/Journal of Software, 2013,24(6):1274−1294 (in Chinese). http://www.jos.org.cn/1000-9825/4284.htm

Secure Routing Architecture Based on Accountability Realm

LU Ning-Ning, ZHANG Hong-Ke

(National Engineering Laboratory for Next Generation Internet Interconnection Devices, Beijing Jiaotong University, Beijing 100044, China)

Corresponding author: LU Ning-Ning, E-mail: radioboy@126.com

Abstract: The study proposes a novel routing architecture, accountability realm based routing architecture (Arbra for short), to sovle prefix hijacking, routing forgery and source address spoofing. In Arbra, the accountability realm (AR) is an independently administered network operated by distinct administrative unit and also the basic element of network topology. Because AR should be responsible for the network actions of users in it, the paper calls it the accountability realm. This paper first designs a mapping method from automous system to AR, and then proposes a two-level routing architecture based on AR. Further, the study builds a routing design framework, which mainly includes a hybrid addressing scheme, core routing protocol, identifier mapping protocol, packet transmitting process and public key management mechanism. Finally, Arbra and other famous routing architecture (such as LISP, AIP, etc) are compared, and the study analyzes the security, scalability, performance and deployment of Arbra. Analysis and evaluations show that: (1) Arbra can solve prefix hijacking, route forgery and source address spoofing; (2) the routing table needed by Arbra is smaller, so we can say that Arbra has better scalability; (3) the performance and deployment cost of Arbra is reasonable. Above all, it is clear that Arbra is a feasible secure routing architecture.

Key words: prefix hijacking; route forgery; source address spoofing; accountability realm; inter-domain routing

* 基金项目: 国家自然科学基金(60833002); 北京市自然科学基金(4091003)
收稿时间: 2011-07-15; 定稿时间: 2012-05-31

Internet 路由体系的安全性面临着严峻的挑战,主要表现在以下 3 个方面:

(1) 前缀劫持:恶意 AS(autonomous system,自治系统)以所有者身份向域间路由系统宣告一个其他组织拥有的 IP 前缀,以达到吸引网络流量,进而篡改、伪造信息内容或造成拒绝服务攻击的目的;

(2) 路由伪造:恶意 AS 通过伪造 BGP(border gateway protocol,边界网关协议)路由宣告消息中的路径属性将网络流量吸引到本地,以达到与前缀劫持相同的攻击效果;

(3) 源地址欺骗:为了隐藏真实身份或规避安全防御设备,攻击方任意伪造发送分组中的源 IP 项.

前缀劫持、路由伪造和源地址欺骗是研究的热点,它们不仅会造成大面积的网络故障,严重破坏正常的网络通信,而且还是黑客发动许多其他网络攻击的基础:

(1) 垃圾邮件:前缀劫持被用于发送垃圾邮件[1],垃圾邮件发送者首先向外声明一个较大的 IP 前缀,从而在互联网中建立起对应路由,而后使用该前缀中未使用或未分配的 IP 地址发送垃圾邮件.目前,以前缀劫持为前奏的垃圾邮件攻击逐渐成为一种趋势[1];

(2) 中间人攻击:互联网中具有特殊拓扑位置的自治系统[2],在发动前缀劫持攻击(或发动路由伪造攻击)将特定目的地址的分组吸引到本网络后,仍可以将它们转发到真正的目的地.这样,在通信双方毫无觉察的情况下就可以完成中间人攻击,如位于美国的自治系统可能使用这种方式监听欧洲、中东之间的网络通信;

(3) 恶性网络事故:自治系统可能由于管理不善等原因,向域间路由系统声明错误的 IP 前缀,这会造成大面积的网络中断.这样的事故已经在互联网中发生多起,例如,1997 年的 AS7007 事件[3]和 2006 年的 AS27506 事件[4];

(4) 拒绝服务攻击(denial-of-service,简称 DoS):源地址欺骗是某些拒绝服务攻击的基础,SYN Flood[5],RST Flood[6]等都是以源地址欺骗为前驱的拒绝服务攻击;源地址欺骗甚至被用于发动针对关键基础设施,如 DNS(domain name system,域名解析系统)服务器的拒绝服务攻击[7];

(5) 反射攻击:攻击者以受害者的 IP 地址为源地址(源地址欺骗)向网络(以广播地址或特定服务器为目的 IP)大规模发送请求报文,如果目的主机或服务器回复(称做跳板),就会形成以受害者为目标的海量数据流,从而造成受害者所宿网络的拥塞甚至瘫痪.smurf[8],DNS Amplification[9]等都是利用源地址欺骗构建的反射攻击.反射攻击难以防御,2006 年,黑客发动了以 DNS 为跳板的反射攻击,攻击流量一度达到 5Gbps[10]的规模;

(6) 弱化安全设备的防御能力:由于源地址欺骗,攻击分组中可能包含虚假的源 IP 项,因此,受害者或防火墙、入侵防御等中间设备不能依据源 IP 项确定攻击的真实来源和攻击者的真实位置,所以无法准确地构建自动过滤规则,难以进行有效防御;

(7) 干扰其他通信性能优化机制:拥塞控制、公平排队、基于来源的流量控制等技术根据源 IP 地址设定控制策略,源地址欺骗损害了这些技术的有效性.

针对前缀劫持、路由伪造和源地址欺骗问题,国内外的学者们相继提出了众多的解决方案,主要包括 Listen-Whisper[11],PHAS[12],IRV[13],PGBGP[14],Ingress Filtering[15],Egress Filtering[16],uRPF[17,18],SAVE[19],清华大学的 SAVI[20],国防科学技术大学的 ESP 方案[21],PPM[22],ICMP Trackback[23],CenterTrack[24],FIT[25],Pi[26],S-BGP[27],So-BGP[28],SPV[29],国防科技大学的 SE-BGP[30],清华大学的 GesBGP[31],解放军信息工程大学的 id^{2}r[32],IPsec[33]和 Passport[34]等.根据采用方法的不同,这些方案大体可以划分为两种类型(见表 1):第 1 类为轻量级的解决方案,也就是使用对称和非对称密码体制之外的其他方式检测或阻止前缀劫持、路由伪造和源地址欺骗等攻击的发生,如 Listen-Whisper,PHAS,IRV,PGBGP,Ingress Filtering,Egress Filtering,uRPF,PPM,ICMP Trackback,CenterTrack,FIT 和 Pi 等;第 2 类为基于密码体制的解决方案(或称重量级解决方案),主要思路为采用对称或非对称密码体制对路由体系进行主动防护,以避免上述攻击的发生,如 S-BGP,So-BGP,SPV,IPsec,Passport 和 AIP[35]等.根据着眼点的不同,还可以将基于密码体制的解决方案进一步划分为两个子类:① 改良型解决方案.在现有路由体系的基础上针对一种或两种网络攻击进行安全性增强,如 S-BGP,So-BGP, SPV,SE-BGP,

GesBGP,id^{2}r,IPsec 和 Passport 等;② 革新型解决方案.通过设计新的路由结构和寻址、路由、转发机制,一体地解决前缀劫持、路由伪造和源地址欺骗攻击,如 AIP 等.

Table 1 Security researches on routing architecture

表 1 路由体系安全研究现状

类型		具体方案
轻量级的解决方案		Listen-Whisper, IRV, PGBGP, PHAS, Ingress Filtering, Egress Filtering, uRPF, PPM, ICMP Trackback, CenterTrack, FIT, Pi
基于密码体制的解决方案	改良型解决方案	S-BGP, So-BGP, SPV, IPsec, Passport
	革新型解决方案	AIP

轻量级解决方案通过维护、挖掘 AS 级拓扑信息,或者使用过滤、在路由消息分组中添加附加信息等方式检测(或阻止)前缀劫持、路由伪造或源地址欺骗攻击.例如:

(1) Listen-Whisper 在路由消息中附加信息,以解决前缀劫持问题;

(2) IRV 通过查询验证服务器,判断路由宣告消息的真实性;

(3) PGBGP 通过维护、挖掘历史上的 AS 级拓扑信息检测前缀劫持攻击的发生;

(4) Ingress Filtering 和 Egress Filtering 均需要人为地在边缘路由器上安装过滤规则,从而分别对进入或流出网络的分组进行源地址过滤;

(5) uRPF 假设路由器中通往某给定 IP 地址的网络接口与该 IP 地址发送的分组进入路由器的网络接口相同,当分组进入 uRPF 路由器的网络接口与转发表中该分组源地址项对应的转发表项所描述的网络接口不同时,路由器认为发送方或中间设备伪造了分组首部的源地址项;

(6) PPM,ICMP Trackback,CenterTrack 通过在分组中附加信息,可以在一定程度上保证源地址的真实性.

虽然轻量级解决方案具有计算效率高、网络负担小的特点,但是由于它们一般存在下列问题:① 这类方案的安全性往往依赖于历史数据的实时性、运营人员的警觉性和手工操作的准确性,由于多家乡、流量工程等复杂路由策略的存在,可能存在较高的误报率;② 当攻击发生时,这类方案一般只能检测出攻击,是事后解决方案,无法提前避免攻击的发生.因此,本文仍然重点研究基于密码体制的解决方案.

基于密码体制的改良型解决方案以可信第三方为信任锚建立 IP 前缀、AS 号与网络管理者公钥的关联,从而避免前缀劫持、路由伪造或源地址欺骗攻击.这类方案往往以基于根节点的集中式认证模型管理可信第三方之间的信任关系,并主动提供路由宣告消息中 IP 前缀和 *as_path* 属性的真实性,或分组首部中源地址项的真实性.例如:

(1) 在 S-BGP 中,AS 向外声明 IP 前缀时需要携带:① 边缘网络对 IP 前缀-起源自治系统绑定关系的数字签名;② AS 使用自己拥有的私钥对该路由宣告消息的数字签名.在继续转发该路由宣告消息之前,每个 AS 都需要使用各自私钥对当前 *as_path* 属性签名,并将签名信息随路由宣告消息一起转发;

(2) SoBGP,SPV 是 S-BGP 的改进方案,两者抵御前缀劫持攻击的机理与 S-BGP 相同,只是提高了 S-BGP 中 *as_path* 累积签名及签名验证过程的计算和存储有效性;

(3) IPsec 可以解决源地址欺骗攻击.它支持预共享密钥和基于数字证书两种认证机制,其中,仅基于数字证书的认证方式适用于大规模的复杂网络环境,但是需要以可信第三方为信任锚建立 IP 地址和终端公钥之间的一一对应关系;

(4) Passport 提供 AS 层次的源地址验证功能.它使用特定的 BGP 扩展属性携带 DH(diffie-Hellman)参数,以协商任意两个 AS 间的对称密钥.在分组离开起源 AS 时,BGP 路由器使用对称密码体制为分组将要经过的每个 AS 生成该分组关键信息(包括源 IP 项)的杂凑值,其他 AS 通过验证该杂凑值就可以判断分组源 IP 项的真实性.由于 Passport 中 DH 密钥协商过程的安全性依赖于 BGP 协议的安全性,因此其本质上也是一种基于可信第三方的安全改良方案.

基于密码体制的改良型解决方案存在一些共同问题,主要包括:① 这类方案提供的安全性依赖于覆盖全球的公钥基础设施,易于引起互联网管理权之争,因此难以获得实际应用;② 这类方案需要较大的计算资源,加

重了路由器处理负担,增大了互联网收敛时间,并需要存储、管理大规模的数字证书;③ 这类解决方案都是分立的解决方案,一种方案只是针对一种或两种威胁,没有从整体上对前缀劫持、路由伪造和源地址欺骗进行考虑.因此,本文也未采纳这一技术路线.

基于密码体制的革新方案要求重新设计互联网路由结构和寻址、路由、转发机制,并由此出发一体地解决前缀劫持、路由伪造和源地址欺骗问题.AIP 是这个技术路线中的典型方案,它以非对称密码体制为基础,不仅完整地克服了前缀劫持、路由伪造和源地址欺骗等问题,具有较高的安全性,而且能够有效支持流量工程.但是,AIP 也存在部署代价高、可扩展性差等严重不足:首先,AIP 的部署代价非常庞大,它需要:(1) 全面更改 IP 协议、域间路由协议和域内路由协议;(2) 重新分配主机,并修改端主机的操作系统使得它们能够支持 AIP 变长的地址结构;(3) 升级所有应用程序以使其支持 AIP 地址结构;(4) 扩展 DNS 服务器的功能;其次,AIP 还存在可扩展性差的缺陷,据文献[35]的初步估计,与 IP 协议相比,AIP 存储 RIB(routing information base,路由信息库)所需的内存开销增长了 3 倍.

考虑到目前新型网络体系研究如火如荼展开的背景,本文延续了 AIP 的研究思路,但是本文的研究成果与 AIP 存在显著差别,不是对 AIP 的简单改进.本文在第 3 节详细对比了基于责任域的安全路由体系(accountability realm based secure routing architecture,简称 Arbra)和 AIP 在实现和功能上的差别,并分别在第 5 节~第 7 节对比了 Arbra 和 AIP 的可扩展性、通信性能和部署代价.与 AIP 相比,Arbra 不仅具有路由表规模小、通信延时低等特点,而且部署代价更小,非常有利于 Arbra 的实际应用.

1 责任域和两级路由结构

Arbra 将互联网中具有独立管理主体的网络当作责任域(accountability realm,简称 AR).这样,在 Arbra 中,互联网表现为“众多责任域的联合”,单个责任域则表现为互联网拓扑的元素形式,所以,可以将互联网视为一个无向图 $G=(V,E)$,其中,顶点集 V 表示责任域集合,边集 E 表示责任域之间的链路集合.

责任域具有以下特点:(1) 责任域边界就是信任边界;责任域为其内部设备(路由器或终端)的网络行为负责;责任域之间不存在担保关系;(2) 责任域的粒度是可变的;无论网络规模,任何具备单一、独立管理主体的网络都可以成为责任域,例如固定子网(企业网或校园网)、移动子网(火车、轮船上的子网)、自组织网络以及自治系统等都有可能被当做独立的责任域.本文按照如下方式定义自治系统到责任域的映射关系(如图 1 所示):

定义 1. $h:AS\rightarrow AR$,使得:

(1) PoP(Point-of-Presence,入网点)中的边缘路由器和接入该 PoP 的用户网络一起成为一个责任域;

(2) AS 中的其他部分成为一个责任域,包括 AS 中的骨干网,核心路由器和 NoC(network operation center,网络运营中心)中的全部服务器,这些设备是自治系统中提供数据传送服务的网络部分.

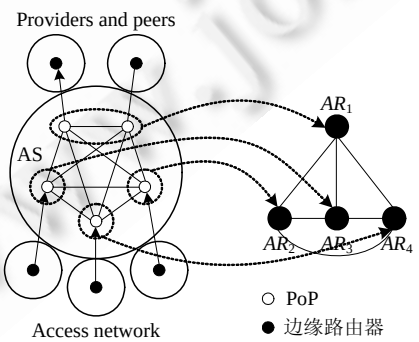

Fig.1 AS-to-AR mapping

图 1 自治系统到责任域的映射

目前,互联网中存在着将近 4 万个 AS,每个 AS 都拥有大量的 PoP(见表 2),这会在 Arbra 中形成数量众多的

责任域.为了避免引发严重的可扩展问题,本文采用两级路由结构进一步将责任域划分为端责任域(stub accountability realm,简称 SAR)和传送责任域(transit accountability realm,简称 TAR):

定义 2(端责任域). 由自治系统中,PoP 的边缘路由器和接入该 PoP 的用户网络映射成的责任域.

定义 3(传送责任域). 由自治系统的其他网络部分映射成的责任域.

定义 4. $g:G\rightarrow(G_t,G_s)$,使得(G_t,G_s)为 G 的分解,并且 $G_t=(V_t,E_t)$,$G_s=(V_s,E_s)$,其中,顶点集 V_t 表示传送责任域集合,V_s 表示端责任域集合;边集 E_t 表示传送责任域之间的连接集合,E_s 表示端责任域和传送责任域之间以及端责任域和端责任域之间的连接集合.

本文分别将 G_t 和 G_s 称为核心网(core network,简称 CN)和边缘网(edge network,简称 EN).在 Arbra 中,CN 和 EN 分别采用互相独立的路由空间,以使端责任域的路由振荡不会影响到核心网.具体地:

(1) 核心网运行核心路由协议.本质上是一种路径向量协议,除了将 IP 前缀和 AS 号替换为传送责任域标签外,其他同 BGP 相似;

(2) 边缘网运行标签映射协议.通过维护端责任域和传送责任域之间的映射关系,间接保持端责任域的全网可达性.

Table 2 Amount of PoPs in AS[37]

表 2 自治系统中 PoP 的数量[37]

AS 号	1221	1239	1755	2914	3257	3356	3967	4755	6461	7018
PoP 数	61	43	25	121	50	52	23	10	21	108

图 2 给出了 Arbra 两级路由结构主要涉及的网络设备.

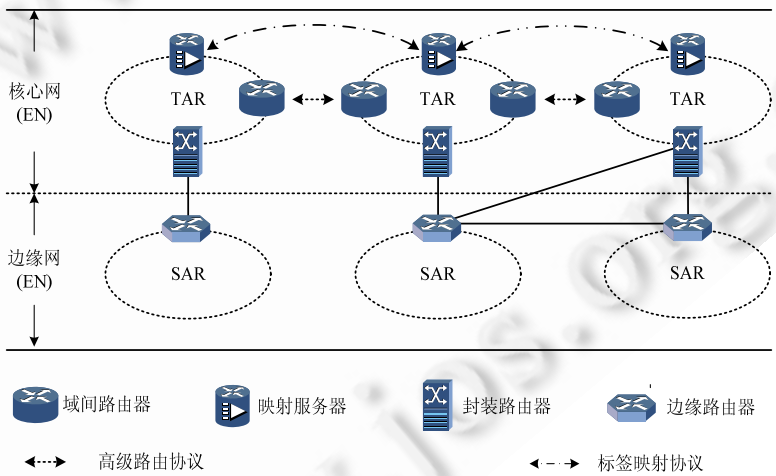

Fig.2 Arbra two-level routing architecture

图 2 Arbra 两级路由结构

(1) 边缘路由器(edge router,简称 ER):端责任域的入口/出口路由器,用于保持端责任域和传送责任域,或端责任域和端责任域之间的连通性;

(2) 域间路由器(inter-AR router,简称 IRR):传送责任域内运行核心路由协议的路由器.每个传送责任域都可以拥有一个或多个域间路由器,同一责任域的多个 IRR 之间通过路由反射器(route reflector,简称 RR)建立连接,以保证域内路由的同步和可扩展性;

(3) 封装路由器(tunnel router,简称 TR):端责任域在传送责任域中的接入点,用于保持传送责任域与它的客户端责任域之间的可达性.TR 可以接收来自核心网或边缘网的分组:对于来自核心网的分组,TR 执行解封装操作,并基于剩余分组的目的地址将分组转发到相应端责任域;对于来自边缘网的分组,TR 首先获得分组目的责任域连接的 TR 地址,然后执行封装操作,最后基于分组外层首部中的目的地

址向核心网转发分组;

(4) 映射服务器(mapping server,简称 MS):传送责任域中运行标签映射协议的服务器,用于维护端责任域-传送责任域映射关系数据库,每个 MS 中都保存了一份完整的映射关系数据库副本.

此外,因为定义 1 和定义 3,所以有定理 1 成立.

定理 1. Internet 中的自治系统和 Arbra 中的传送责任域一一对应.

因为定理 1,所以有下面定理成立:

定理 2. Arbra 中的核心网拓扑和 Internet 中的 AS 级拓扑同构.

2 路由体系设计框架

本节设计了 Arbra 网络的寻址、路由、转发和公钥管理机制.介绍的核心路由协议和标签映射协议都是运行于责任域间的路由协议,本文没有给出域内路由协议,但是第 2.1 节的混合寻址方案使得 OSPFv6(OSPF for IPv6)[38],RIPng(RIPng for IPv6)[39]等域内路由协议能够应用到责任域内,这增加了 Arbra 的灵活性.

2.1 混合寻址方案

Arbra 采用混合寻址方案,每个网络接口的地址都由平面结构的责任域标签 d 和层次结构的域内标签 f 混合组成,记作 d:f,简称 Arbra 地址.d 在全网范围内唯一表示责任域身份,f 在责任域内唯一表示网络接口的地址(如图 3 所示).

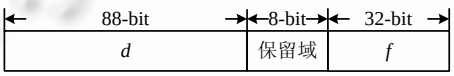

Fig.3 Arbra addressing

图 3 Arbra 地址

定义 5. d 由责任域公钥生成,是 88-bit 的杂凑值.令 D 表示责任域标签空间,则有 $D=\{1,...,2^{88}\}$.

d 的生成方法是:

$$d_i=prf_i(pk_i) \tag{1}$$

pk_i 表示责任域 i 自主生成的公钥,对应私钥记作 pr_i;$prf_i(\cdot)$表示责任域 i 选择的杂凑函数.

与其他公钥密码体制相比,椭圆曲线公钥体制(elliptic curve cryptography,简称 ECC)具备更高的比特安全强度[40],所以本文选择使用椭圆曲线公钥体制创建责任域公、私钥,以减少数字签名、数字签名验证过程中存在的计算、存储和带宽开销.具体地,本论文使用 ECDSA(elliptic curve digital signature algorithm,椭圆曲线数字签名算法)作为统一的责任域公钥密码体制,有限域选择 NIST's B-163[41],公、私钥长度分别为 326-bit 和 163-bit(与 1024-bit 密钥长度的 RSA 安全性相同).

本论文使用分组密码体制 AES,以标准方法 ISO/IEC 10118-2[42]构建 $prf_i(\cdot)$

$$H_i = prf_i(x_i) = g(AES_{K_i}(x_i) \oplus x_i) \tag{2}$$

其中,$g(x)$表示截取位组 x 的最左 88 比特;K_i 表示 AES 密钥,在网络中公开,称做 H_i 的生成参数;⊕表示异或.

公式(2)具有如下性质:

(1) 给定 $prf_i(\cdot)$和 H_i,找到 x_i,使得 $prf_i(x_i)=H_i$,在计算上不可行; (3)

(2) 找到 x_j,$x_j\neq x_i$,使得 $prf_i(x_j)=H_i$,在计算上不可行. (4)

因为公式(3)、公式(4),所以可以得到如下定理:

定理 3. 责任域标签与责任域公钥天然地一一对应.如果责任域 A 相信 $prf_x(pk_x)=d_x$,$d_x\in D$,$d_i\neq d_A$,那么 A 相信 pk_x 是责任域标签 d_x 对应的公钥.一般将责任域标签的这种性质称作自认证特性.

域内标签 f 为 32-bit 的位组,采用 CIDR 模式的层次结构,支持子网划分和前缀聚合.在责任域内使用基于身份的聚合签名算法,按需为域内的边缘路由器,核心路由器和终端等具体网络设备离线分配私钥,并使得对应公

钥就是它们各自的 Arbra 地址.具体地,本论文选择使用 JYH[43]算法,它主要包括以下步骤:

(1) 系统公共参数选择:

① 选择间隙 DH 群(gap Diffie-Hellman group)G,G 的阶为大素数 l,G 同时是一个加法循环群,G 的生成元为 P;

② 选择乘法循环群 G_T;

③ 选择双线性映射 $e:G\times G\to G_T$,e 满足下列条件:

双线性:对任意 $Q,R\in G$ 且 $a,b\in Z/lZ$,有 $e(aQ,bR)=e(Q,R)^{ab}$ (5)

非退化性:存在 $Q,R\in G$,满足 $e(Q,R)\neq 1$ (6)

计算有效性:对任意 $Q,R\in G$,存在计算 $e(Q,R)$的有效算法 (7)

④ 选择两个杂凑函数 $H_1:\{0,1\}^*\times G\to(Z/lZ)^*$和 $H_2:\{0,1\}^*\to G^*$.定义系统公共参数为$\pi_s=(G,G_T,l,P,e,H_1,H_2)$,$\pi_s$ 为互联网中的所有责任域共享;

(2) 各域自主生成域内主密钥和域内公共参数:对于任意 d_i,域运营人员随机选择主密钥 $s_i\in Z/lZ$;并令 $R_i=s_iP$,则域内公共参数$\pi_i=\{R_i\}$.s_i 仅为特定的域运营人员保有,π_i 在责任域内共享;

(3) 各责任域离线分发私钥:在任意 d_i 中,地址为 $d_i:f_j$ 的设备可以通过离线方式从域管理人员处获得私钥 $s_{i,j}=s_iH_2(d_i:f_j)$,相应公钥为 $H_2(d_i:f_j)$,因为 $H_2(d_i:f_j)$同 $d_i:f_j$ 一一对应,所以也可以说公钥是 $d_i:f_j$;

为了讨论的方便,这里一并给出 JYH 签名算法和数字签名验证算法.

(4) 签名:给定消息 $M_{i,j}$ 和网络设备私钥 $s_{i,j}$,选择随机数 $r\in Z/lZ$,则输出的数字签名为

$$\sigma_{ij}=(U,V)=(rP,rH_2(d_i:f_j)+H_1(M_{i,j},rP)s_{i,j}) \tag{8}$$

(5) 签名验证:给定来自 $d_i:f_j$ 的消息 $M_{i,j}$ 和数字签名$\sigma_{ij}=(U,V)$,仅当公式(9)成立时,数字签名正确.

$$e(H_2(d_i:f_j),U+H_1(M_{i,j},U)R_i)==e(P,V) \tag{9}$$

双线性映射 e 是提高 JYH 算法计算性能的关键,一般采用椭圆曲线上的 Weil Pairing 或 Tate Pairing 构造 e.因为 Tate Pairing 在特征为 3 的有限域上存在快速算法,所以本文按照如下方式生成群 G、G_T 和映射 e:

(1) 选择有限域 GF(3^{97}),域多项式为 $t^{97}+t^{12}+2$;

(2) 定义 GF(3^{97})上的椭圆曲线 $E:Y^2=X^3-X+1$(安全性和 1 024 比特的 RSA 相同);

(3) 按照文献[44]中的方法,由 GF(3^{97})和 E 生成 G、G_T 和映射 e.

2.2 核心路由协议

核心路由协议动态地维持核心网的可达性,它是一种路径向量协议,除了将 IP 前缀和 AS 号替换为传送责任域标签外,其他与 BGP 相似.核心路由协议同样具有 OPEN,Update,Notification,Keepalive 等消息和 ORIGIN,Path,NEXT_HOP,LOCAL_PREF 等属性(AGGREGATOR 属性除外,因为核心路由协议根据传送责任域标签组织路由表,所以不支持路由句柄的聚合,所以不需要 AGGREGATOR 属性).因此,一些针对 BGP 其他方面的改进仍然可以平滑迁移到 Arbra 核心路由协议中来.

本节将核心路由协议中的路由宣告消息形式化定义为公式(10).

$$r_i=(d_i,p_{ik}) \tag{10}$$

其中,d_i 是目的责任域标签,p_{ik} 表示路径属性.公式(11)中,p_{ik} 由 r_i 途径的传送责任域标签顺序组成.d_i 为 p_{ik} 中的第 1 个责任域标签.

$$p_{ik}=[d_i,\ldots,d_k] \tag{11}$$

图 4 给出了核心路由协议的路由宣告实例.总的来说,核心路由协议和 BGP 协议存在 3 个主要的区别:

(1) BGP 协议中的目的网络是 Internet 中边缘网络,以 IP 前缀表示;核心路由协议不涉及边缘网络,它的目的网络是传送责任域,目的网络以传送责任域标签表示;

(2) 在 BGP 中,目的前缀具有层次结构,中间自治系统可以根据层次上的相似性将多个目的前缀聚合成单一的覆盖前缀;在核心路由协议中,目的网络标签具有平面结构,任何中间责任域都无法对它执行聚合操作;

(3) BGP 以 AS 号表示自治系统,并使用 AS 号序列作为路径属性;核心路由协议使用传送责任域标签构建路径属性.

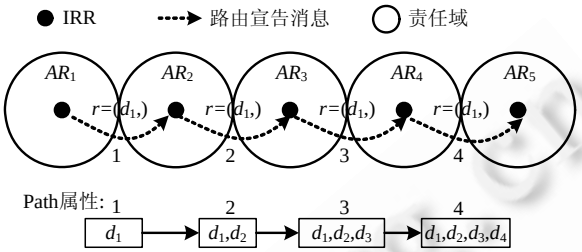

Fig.4 Routing protocol in core network

图 4 核心路由协议

此外,核心网中的路由器以传送责任域标签为句柄组织域间路由表(和转发表).因为责任域标签具有平面结构,所以在转发分组时路由器可以摒弃最长前缀匹配算法,转而使用哈希表精确定位给定地址的路由信息.

2.3 标签映射协议

将封装路由器在传送责任域内的地址称作端责任域的位置标签.标签映射机制通过建立、管理(端责任域、位置标签)映射关系,间接实现边缘网的可达性.

2.3.1 本节定义的两种类型的映射关系

定义 6(一般情况的映射关系). 对于端责任域 d_x,假设其直连的封装路由器地址为 d_y:f_y,则映射关系为

$$M^g=\langle d_x,d_y{:}f_y,ts\rangle,$$

其中,ts 表示 M^g 的生成时间.

定义 7(多宿情况的映射关系). 对于端责任域 d_x,假设其直连的封装路由器地址包括 $d_1{:}f_1,d_2{:}f_2,\ldots,d_i{:}f_i,\ldots,d_n{:}f_n,n\in R,n\geqslant 2$,则对应的映射关系为

$$M^m=\langle d_x,d_1{:}f_1,ts_{x,1},w_{x,1}\rangle\cup\langle d_x,d_2{:}f_2,ts_{x,2},w_{x,2}\rangle\cup\ldots\cup\langle d_x,d_i{:}f_i,ts_{x,i},w_{x,i}\rangle\cup\ldots\cup\langle d_x,d_n{:}f_n,ts_{x,n},w_{x,n}\rangle,$$

其中,$ts_{x,i}$,32 比特,表示生成时间;$w_{x,i}$,16 比特,表示权重信息,满足条件 $w_{x,i}>0$,且 $w_{x,1}+w_{x,2}+\ldots+w_{x,n}=1$,多宿的端责任域通过设定 $w_{x,i}$ 实现输入流量控制.

下面以图 5 所示拓扑为例说明上述概念.

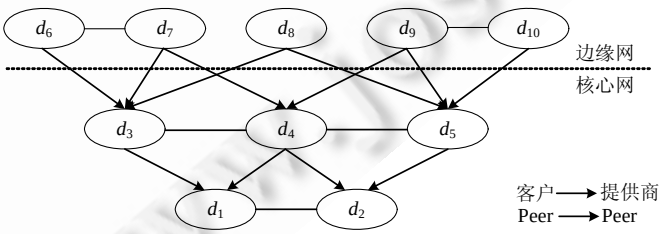

Fig.5 Identifier mapping relations

图 5 标签映射关系

假设责任域 $d_i,i\in[1,10]$的标签为 d_i.端责任域 d_6 和 d_{10} 仅拥有一个服务提供商,因此两者对应的映射关系分别为$\langle d_6,d_3{:}f_3,ts_6\rangle$和$\langle d_{10},d_5{:}f_5,ts_{10}\rangle$;$d_7,d_8$ 和 d_9 多宿,同时与多个服务提供商相连,因此它们对应的映射关系分别为

$\langle d_7,d_3{:}f_3,ts_{7,3},w_{7,3}\rangle\cup\langle d_7,d_4{:}f_4,ts_{7,4},w_{7,4}\rangle$;$\langle d_8,d_3{:}f_3,ts_{8,3},w_{8,3}\rangle\cup\langle d_8,d_5{:}f_5,ts_{8,5},w_{8,5}\rangle$;$\langle d_9,d_4{:}f_4,ts_{9,4},w_{9,4}\rangle\cup\langle d_9,d_5{:}f_5,ts_{9,5},w_{9,5}\rangle$.

参数 $w_{x,i}$ 支持输入流量控制,如果 d_8 希望所有的输入流量都经过 d_3 到达,则应设定 $w_{8,3}=1,w_{8,5}=0$;如果 d_8 希望输入流量均衡,则应设定 $w_{8,3}=0.5,w_{8,5}=0.5$.时间参数 ts 可以作为映射关系的次序.假设 d_1 中存在 d_{10} 的一般映

射关系$\langle d_{10},d_5{:}f_5,ts{=}200\rangle$,这时,$d_1$ 中映射服务器接收到新的映射关系$\langle d_{10},d_x{:}f_x,ts'{=}300\rangle$,因为 $ts'>ts$,所以映射服务器认为$\langle d_{10},d_x{:}f_x,ts'\rangle$是最新的映射关系,因此使用$\langle d_{10},d_x{:}f_x,ts'\rangle$替换掉存储器中的$\langle d_{10},d_5{:}f_5,ts\rangle$.

2.3.2 映射关系的传播

在 Arbra 中,映射服务器都需要维护一份完整的映射数据库副本,用以包含网络中存在的全部(端责任域、位置标签)映射关系;而封装路由器仅需在高速缓存中保存最近使用的(端责任域、位置标签)映射.

因为(端责任域、位置标签)映射仅反映端责任域与传送责任域之间的 Customer-Provider 商业关系,边缘路由器与封装路由器之间的链路故障不会影响这种商业关系,所以在 Arbra 中,只有当端责任域切换服务提供商或变更网络接入点时,映射关系才会发生变动.这时,需要将(端责任域、位置标签)的变化传送给所有的映射服务器.为此,本节通过扩展核心路由协议,提出了一种映射关系传播机制.它的关键点包括:

(1) 每个映射服务器都具有 Arbra 核心路由模块,并且和它所属责任域中的域间路由器建立对等体关系;

(2) 映射服务器将映射关系封装成特殊的 BGP 属性(称作映射属性),并通过域间路由器组成的控制平面将它们传播到其他的传送责任域;

(3) 对于域间路由器,映射属性是可选过渡的.也就是说,域间路由器不必支持该属性,只需在接收后向其他的域间路由器传播;

(4) 映射服务器一般保持静默状态,从域间路由器接收路由信息,但是除了映射属性之外,不向域间路由器发送任何其他信息.

图 6 给出了映射传播机制的实例,其中:映射服务器 MS_1 和域间路由器 CR_1 处于传送责任域 d_1;映射服务器 MS_2 和域间路由器 CR_2 处于传送责任域 d_2.映射关系为 $M^g=\langle d_x,d_1{:}f_1,ts,w\rangle$.具体流程为:

(1) MS_1 首先将 M^g 封装成映射属性(记作 m_1),具体格式如图 7 所示;然后向 CR_1 发送携带该映射属性的路由更新报文 u_1;

(2) 因为 CR_1 是普通的域间路由器,不能识别出映射属性中的信息内容,所以它查找 m_1 的过渡属性位,发现 m_1 是一个过渡属性后,CR_1 向它的邻居转发路由更新报文 u_1;

(3) CR_1 同样不加任何处理地将 u_1 转发给 MS_2.

通过上述步骤,M^g 就被传送到了远端的映射服务器.

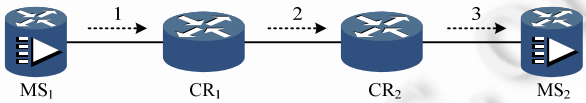

Fig.6 Mapping transmission

图 6 映射关系的传播

BGP attribute header	Flag	映射信息	保留域

Fig.7 Mapping attribute

图 7 映射属性

2.4 分组转发流程

如图 8 所示,本节以实例方式阐述 Arbra 中的分组转发流程.假设网络中存在:

(1) 传送责任域 TAR_1,TAR_2, TAR_3 和端责任域 SAR_4,SAR_5,它们的责任域标签分别为 d_1,d_2,d_3,d_4,d_5;

(2) 封装路由器 TR_4,TR_5,TR_6,终端 E_{12},E_{13},它们的 Arbra 地址分别为 $d_1{:}f_4$,$d_2{:}f_5$,$d_3{:}f_6$,$d_4{:}f_{12}$,$d_5{:}f_{13}$;

(3) 映射关系 $M_4=\langle d_4,d_1{:}f_4,ts_4\rangle$和 $M_5=\langle d_5,d_2{:}f_5,ts_{5,2},w_{5,2}\rangle\cup\langle d_5,d_3{:}f_6,ts_{5,3},w_{5,3}\rangle$.

若 E_{12} 计划与 E_{13} 通信,则有:

步骤 1. E_{12} 发送分组 P,P 的源地址为 $d_4{:}f_{12}$,目的地址为 $d_5{:}f_{13}$.由于 P 的目的地址不在端责任域 SAR_4 内,因

此 P 被转发到边缘路由器 BR_{10}.BR_{10} 检查分组目的地址后,将 P 继续转发到与其直接相连的封装路由器 TR_4;

步骤 2. TR_4 接收到来自 SAR_4 的分组 P 后,因为 P 的目的地址不在 TR_4 所宿的传送责任域 TAR_1 内,因此 TR_4 根据 P 的目的地址 d_5:f_{13} 查询本地缓存,以获得目的责任域 d_5 的位置标签:

步骤 2.1. 如果缓存中不存在 d_5 的映射关系 M_5,则执行步骤 3;

步骤 2.2. 如果缓存中存在 d_5 的映射关系 M_5,则执行步骤 5;

步骤 3. TR_4 向 TAR_1 中的映射服务器 MS_7 请求 d_5 的映射关系 M_5;

步骤 4. MS_7 查询映射表,获得 M_5 后,MS_7 将 M_5 回送给 TR_4.接收到 M_5 后,TR_4 执行缓存管理策略,首先将 M_5 存储在本地缓存中;

步骤 5. TR_4 从 M_5 中选择恰当的位置标签:假设 $w_{5,2}$=1,$w_{5,3}$=0,则按照第 2.3 节对 w 的定义,TR_4 应选择 d_2:f_5 作为 d_5 的位置标签.因此,TR_4 分别以 d_1:f_4 和 d_2:f_5 为源和目的地址形成新的首部,并封装在原始分组 P 之前,从而得到新的分组 P'.最后,TR_4 向核心网转发 P';

步骤 6. P'经核心网到达 TR_5 后,TR_5 首先去掉 TR_4 封装的外层首部,得到原始分组 P;然后,根据 P 的目的地址 d_5:f_{13} 查询本地转发表;最后,按照对应的转发条目,将 P 发送到与其直接相连的边缘路由器 BR_{11};

步骤 7. 因为目的地址 d_5:f_{13} 与 BR_{11} 一样,都在端责任域 SAR_5 内,所以接收到 P 后,BR_{11} 将 P 向 SAR_5 内转发.P 最终到达终端 E_{13}.

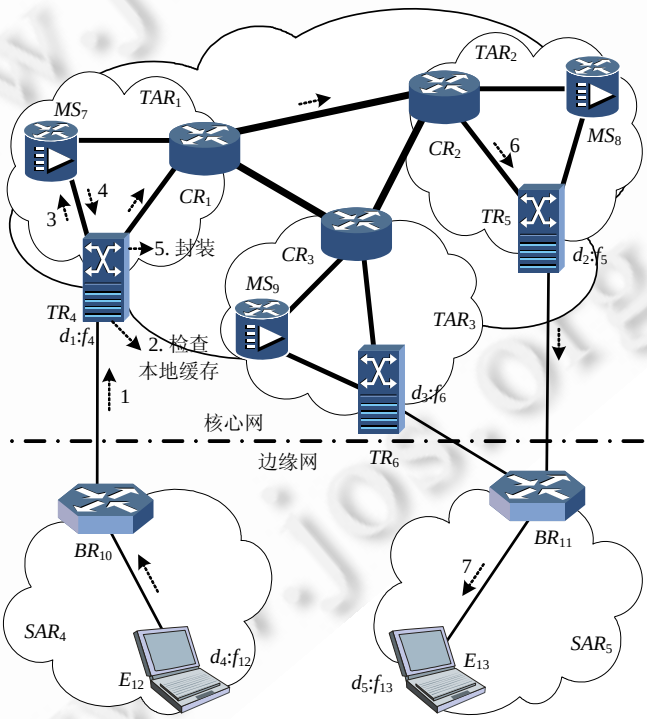

Fig.8 Packet forwarding in Arbra

图 8 Arbra 分组转发流程

图 9 给出了上述转发过程中分组在各个阶段的逻辑格式.

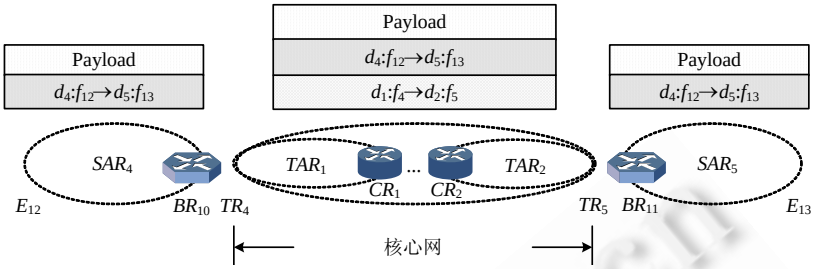

Fig.9 Logic format of a packet

图 9 分组的逻辑格式

2.5 公钥管理机制

Arbra 包含一个简单的集中式注册查询中心(public shared registry,简称 PSR),负责注册、存储、分发所有的责任域公钥和域内公共参数,并支持责任域标签、钥和域内公共参数的动态更新.因为在 Arbra 中,责任域标签与责任域公钥天然地一一对应(定理 3),所以 PSR 和 PKI(public key infrastructure,公钥基础设施)中的认证中心(certificate authority,简称 CA)在本质上是不同的,PSR 不需要以可信第三方的身份担保用户公钥和用户标签之间的绑定关系.换句话说,CA(或多个 CA 形成的体系)是一个覆盖全网络的权威机构,而 PSR 只是一个注册查询机构,所以建立 PSR 不会引起互联网管理权之争.PSR 的工作原理如下所述:

(1) PSR 以链表形式存储责任域标签、公钥、域内公共参数等信息.每个责任域标签都对应 PSR 中的一个表项.对于责任域 i,它在 PSR 中的存储表项可以形式化定义为

$$TB_i=\{d_i,pk_i,K_i,\pi_i,T_{C,i},T_{V,i},isr_i,[Re],\{d_i,pk_i,K_i,\pi_i,T_{C,i},T_{V,i},isr_i,[Re]\}_{pr_i}\} \quad (12)$$

其中:d_i,pk_i,K_i,π_i,$T_{C,i}$,$T_{V,i}$ 分别表示责任域 i 的标签、公钥、生成参数、域内公共参数、生成时间、有效期等信息;isr_i 表示 TB_i 的状态,值为 0 或 1,取值的意义见公式(13):

$$isr_i=\begin{cases}0, & d_i\text{仍然有效}\\ 1, & d_i\text{已被废止}\end{cases} \quad (13)$$

$\{d_i,pk_i,K_i,\pi_i,T_{C,i},T_{V,i},isr_i,[Re]\}_{pr_i}$ 表示 i 使用私钥 pr_i 对 d_i,pk_i,K_i,π_i,$T_{C,i}$,$T_{V,i}$,isr_i,$[Re]$的数字签名;[·]表示可选;$[Re]$表示 isr_i=1 时责任域 i 的新标签对应的表项位置;

(2) 分发:每个责任域周期性地查询 PSR,以实时更新其他责任域的标签、公钥、域内公共参数等信息;

(3) 更新:PSR 支持责任域标签的按需更新,以抵御可能发生的密钥强度退化问题.具体地,Arbra 支持 3 种形式的责任域标签更新:

① 定时更新.任何责任域 i 在时间超过有效期 $T_{V,i}$ 之前,都必须生成新的公/私钥对、标签和域内公共参数,并在 PSR 中废止旧有表项 TB_i(也就是将 isr_i 置为 1),注册新的存储表项;

② 临时更新.每个责任域在任何时间都可以主动更新公/私钥对、标签和域内公共参数,临时更新同样需要在 PSR 中废止旧有表项,注册新的表项;

③ 部分更新.Arbra 允许责任域单独更新 PSR 存储表项中的 π_i 属性.

因为在 Arbra 中,核心网根据责任域标签组织路由表和转发表,边缘网根据责任域标签构建映射信息,所以当发生定时更新和临时更新时,每个责任域都需要将路由表、转发表或映射关系表中旧的责任域标签替换成新的责任域标签.

此外,对于可能发生的责任域标签碰撞问题:

一方面,目前互联网中存在着将进 4 万个 AS,假设每个 AS 平均拥有 100 个 PoP,那么由定义 1 可知,Arbra 中责任域的数量不会超过 404 万个,而 $D=\{1,...,2^{88}\}$的大小为

309 485 009 821 345 068 724 781 056

所以,Arbra 中的责任域标签在 D 内是稀疏的,责任域标签发生碰撞的概率很小;

另一方面,每个责任域在向 PSR 注册信息时,可以首先检查它选择的责任域标签是否同其他责任域冲突,如果冲突,那么责任域需要重新生成恰当的责任域标签.责任域乐于进行这种检查,因为一旦碰撞发生,就意味着它有可能接收不到它的客户发送给它的分组.

3 各种路由结构的比较

本节从路由结构、网络标签、寻址方案、路由协议、转发流程、安全性、可扩展性这 7 个方面对比了 Arbra, IPv4,IPv6,LISP 和 AIP 方案,比较结果见表 3.在所有指标中,安全性和可扩展性是 Arbra 的关键优点,第 4 节和第 5 节将分别深入分析 Arbra 在这两方面的特点.

Table 3 Comparisons of various routing architectures

表 3 各种路由结构的对比

指标\方案	Arbra	IPv4/v6	LISP	AIP
路由结构	责任域,两级	自治系统	两级	责任域*
网络标签	自认证标签	前缀&AS 号	前缀&AS 号	自认证标签
寻址方案	两层	CIDR 式	CIDR 式	层次式
路由协议	EAR/CAR 分离 基于 AR 标签	无分离 基于前缀	边缘/核心分离 基于前缀	无分离 基于 AD 标签
转发流程	间接转发	直接转发	间接转发	直接转发
安全性	优	差	差	优
可扩展性	优	差	优	差

*注:虽然同称为责任域,但是 AIP 中的责任域和 Arbra 中的责任域有所不同.

4 安全性分析

本节首先研究 Arbra 中的信任模型,然后基于该信任模型依次提出了解决前缀劫持、路由伪造和源地址欺骗问题的 3 种具体机制.研究结果表明:(1) Arbra 具有分布式的信任模型;(2) Arbra 的信任模型为解决前缀劫持、路由伪造和源地址欺骗问题奠定了基础.

4.1 信任模型

虽然 Arbra 需要集中式的注册查询中心,但是在信任关系上,它的混合寻址方案和公钥管理机制一起形成了一种分布式的信任模型.在 Arbra 中,每个责任域都是域内设备的信任锚,整个信任模型中不存在“根信任锚”,这是一种完全分布式的信任结构.换句话说,Arbra 信任模型的特别之处在于:(1) 责任域自己保证其公钥的可信;(2) 责任域通过担保域内公共参数保证域内设备公钥的可信.这里,公钥的可信是指:

定义 8(可信公钥). 假设网络实体 A(标签为 Q_A)声称拥有公钥 pk,如果网络实体 B 相信 pk 确实是 A 公钥,或者 pk 对应的私钥 pr 仅仅正当地被 A 所拥有,那么就说 B 相信 A 的公钥 pk 可信.

下面对 Arbra 中的分布式信任模型进行证明.

不失一般性,假设责任域 d_1 和 d_2 中分别存在网络设备 i 和 j;d_1 和 d_2 的公/私钥对分别为 pk_1/pr_1 和 pk_2/pr_2,且有 $d_k=prf_k(pk_k),k\in[1,2]$;$d_1$ 和 d_2 在 PSR 中的存储表项分别为 $TB_k=\{d_k,pk_k,K_k,\pi_k,...,\{d_k,pk_k,K_k,\pi_k,...\}_{pr_k}\}$,$k\in[1,2]$;$i$ 和 j 的地址为 $a_i=d_1{:}f_i$ 和 $a_j=d_2{:}f_j$.由第 2.1 节可知,i 和 j 可以分别从责任域 d_1 和 d_2 的运营人员处获得私钥 pr_i,pr_j,使得公钥分别为 $pk_i=d_1{:}f_i,pk_j=d_2{:}f_j$.

定理 4. 责任域自己保证其公钥的可信.

证明:因为责任域标签与责任域公钥一一对应(定理 3),所以责任域公钥的可信性极其容易验证.假设 d_1 从 PSR 处获得了 $TB_2,TB_2=\{d_2,pk_2,K_2,\pi_2,...,\{d_2,pk_2,K_2,\pi_2,...\}_{pr_2}\}$,那么它通过下列步骤就可以确定 pk_2 的可信性:

① 判断是否 $d_2=g(AES_{K_2}(pk_2)\oplus pk_2)$:如果不是,说明 TB_2 是错误的;如果是,说明在 K_2 真实的前提下,d_2 与 pk_2 对应.也就是说,pk_2 确实是 d_2 的公钥.这时,需要继续执行下面步骤以判断 K_2 是否真实.

② 使用 pk_2 验证 $\{d_2,pk_2,K_2,\pi_2,...\}_{pr_2}$ 是否是 $d_2,pk_2,K_2,\pi_2,\ldots$的签名:如果是,说明注册 TB_2 的实体确实拥有 pk_2 对应的私钥(也就是 d_2 的私钥),并用该私钥生成数字签名保护 $d_2,pk_2,K_2,\pi_2,\ldots$的完整性.所以,这时 d_1

应当相信:(a) 是 d_2 注册了 TB_2;(b) TB_2 是真实的;(c) K_2 也是真实的.

综合步骤①、步骤②,pk_2 是可信的. □

定理 5. 责任域通过担保域内公共参数保证域内设备公钥的可信.

证明:在上面步骤②中,通过验证签名,可以确定 TB_2 的真实性.因为 TB_2 包含多个项,所以 d_1 除了可以确定 K_2 真实以外,还可以确定域内公共参数 π_2 等信息的真实性.因此,不失合理性,可以首先假设责任域 d_1 和 d_2 都相信:① pk_1 是 d_1 的公钥,π_1 是 d_1 的域内公共参数;② pk_2 是 d_2 的公钥,π_2 是 d_2 的域内公共参数.

如果 i 向 j 发送$(m,S_i(m))$,m 表示分组,其源地址为 $m.src=d_1:f_i$,$S_i(m)=(U_i,V_i)$表示 i 按照公式(8)对 m 的数字签名,那么 j 通过表 4 所示算法就可以验证 i 的公钥 $pk_i=d_1:f_i$ 的可信性:

① 假设算法执行完毕,并返回 True,那么由步骤 1 可知,m 声称来自于责任域 d_1 内的设备 $m.src=d_1:f_i$.因为在 Arbra 中,设备的地址同时是设备的公钥,所以这等价于"m 的发起方 i 的公钥是 $pk_i=d_1:f_i$";

② 因为步骤 4、步骤 5 返回 True,所以 j 相信,在 π_1 真实的情况下(即 j 相信 π_1 确实是 d_1 的域内公共参数),$S_i(m)$ 是发送方使用 pk_i 对应的私钥 pr_i 对 m 的数字签名.也就是说,j 相信 i 拥有 $m.src$ 的私钥.所以这时,"i 的公钥是 $m.src=d_1:f_i$"是可信的;

③ 由步骤 2 可知,j 从 d_2 处获得 $\pi_1=\{R_1\}$,因 d_2 相信 π_1 是 d_1 的域内公共参数,并且 d_2 是 j 的信任锚,所以 j 相信 π_1 是 d_1 的域内公共参数.

所以,综合步骤②、步骤③可知,发送方 i 的公钥是可信的. □

Table 4 Validation of the intra-domain public key

表 4 域内设备公钥的可信性验证

算法	d_2:f_j 验证 $pk_i=d_1:f_i$ 的可信性
输入:$(m,S_i(m))$, $\pi_s=(G,G_T,l,P,e,H_1,H_2)$, $S_i(m)=(U_i,V_i)$;	
输出:True——pk_i 真实;False——pk_i 虚假.	
1	j 从 m 中取出源地址 $m.src=d_1:f_i$
2	j 从 d_2 中获得 d_1 的域内公共参数 $\pi_1=\{R_1\}$
3	j 计算 $n_1=H_2(m.src)$, $n_2=U_i+H_1(m,U_i)R_1$
4	if $e(n_1,n_2)==e(P,V_i)$ then
5	return True
6	else
7	return False
8	end if

4.2 安全机制

本节提出了解决前缀劫持、路由伪造和源地址欺骗问题的 3 种具体机制.这些机制完全基于 Arbra 的分布式信任模型,因此它们本身就是对 Arbra 安全性的最好证明.

4.2.1 前缀劫持

前缀劫持是攻击者对 IP 前缀的不正当使用.因为路由表使用 IP 前缀充当边缘网络标签,所以前缀劫持又可以看做是攻击者对边缘网络标签的伪造.因为 Arbra 将边缘网络映射为端责任域(由定义 1 和定义 2 可知),所以在 Arbra 中,前缀劫持的攻击形式变换为攻击者对端责任域标签的伪造.又因为端责任域标签只出现在标签映射协议中,所以本节主要通过改进标签映射协议达到防御前缀劫持攻击的目的.

4.2.1.1 映射证明

假设映射关系为 $M^g=\langle d_x,d_y:f_y,ts,w\rangle$,则映射证明可以形式化定义为

$$ma_{x,y}=(s_x(M^g,c_{x,y}),s_y(M^g,c_{x,y})) \tag{14}$$

其中,$s_i(m)$表示责任域 i 使用私钥 pr_i(公钥为 pk_i,且 d_i 由 pk_i 生成)对信息 m 的数字签名;$c_{x,y}$ 是控制项,表示 M^g 的状态,值为 0 或 1,取值的意义见公式(15).

$$c_{x,y}=\begin{cases}0, & M^g\text{仍然有效}\\ 1, & M^g\text{已被废止}\end{cases} \tag{15}$$

4.2.1.2 传播机制

如果 M^g 发生变化,映射服务器需要将 M^g,$ma_{x,y}$ 和 $c_{x,y}$ 一起封装成“映射属性”($ma_{x,y}$ 和 $c_{x,y}$ 封装到图 7 的保留域中),然后按照第 2.3 节给出的传播方法向外发送映射属性.

4.2.1.3 映射验证算法

对于任何一个映射服务器 MS_Z,如果它接收到映射关系 $M^g=\langle d_x,d_y{:}f_y,ts,w\rangle$,控制项 $c_{x,y}$ 和映射证明 $ma_{x,y}$,那么在将 M^g 读入本地数据库之前,该映射服务器应首先验证 $ma_{x,y}$ 中的数字签名 $s_x(M^g,c_{x,y})$和 $s_y(M^g,c_{x,y})$是否正确:如果不正确,则直接丢弃该映射关系;如果正确,则对该映射关系进行后续处理:(1) 如果 $c_{x,y}$=1,则从本地数据库中删除内容为 M^g 的表项;(2) 如果 $c_{x,y}$=0,则需要执行如下操作:① 如果本地数据库中没有 d_x 和 $d_y{:}f_y$ 之间的映射关系,则将 M^g 添加到本地映射数据库的恰当位置;② 如果本地数据库中存在 d_x 和 $d_y{:}f_y$ 之间的映射关系$\langle d_x,d_y{:}f_y,ts_1,w_1\rangle$,并且 $ts_1<ts$,则用 M^g 替换掉$\langle d_x,d_y{:}f_y,ts_1,w_1\rangle$;③ 否则,丢弃 M^g.

4.2.2 路由伪造

路由伪造是攻击者对路径属性中 AS 号的不正当使用.因为 BGP 使用 AS 号充当自治系统标签,所以路由伪造又可以看做是攻击者对自治系统标签的伪造.因为在 Arbra 中,自治系统和传送责任域一一对应(定理 1),所以在 Arbra 中,路由伪造的攻击形式变换为攻击者对传送责任域标签的伪造.又因为传送责任域标签只出现在核心路由协议中,所以本节主要通过改进核心路由协议达到防御路由伪造攻击的目的.

为了解决路由伪造攻击,可以将 S-BGP[27]移植到 Arbra 中.具体地:(1) 传送责任域中的域间路由器向外声明路由时,需要使用它自己拥有的私钥(公钥为输出接口的 Arbra 地址)对该路由宣告消息进行数字签名,并将该路由器输出接口的域内标签和数字签名随路由消息一起发送;(2) 在继续转发该路由宣告消息之前,每个传送责任域的出口路由器都需要使用各自私钥对当前路径属性签名,并将该路由器输出接口的域内标签和签名信息随路由宣告消息一起发送;(3) 其他传送责任域从路由宣告消息中可以得到该消息依次经过的域间路由器的 Arbra 地址(组合路径属性中的传送责任域标签和对应的域内标签),然后使用这些地址依次验证相应的数字签名,就可以辨别出是否发生了路由伪造攻击.

4.2.3 源地址欺骗

因为 Arbra 的分布式信任模型,许多抵御源地址欺骗的方案都可以在 Arbra 网络中发挥作用.

首先,在责任域内可以部署 Ingress Filtering[15],SAVE[19],SAVI[20]等轻量级解决方案.Arbra 层次结构的域内标签为这些技术的灵活应用保留了空间.

其次,Passport[34]提供 AS 层次的源地址验证功能.因为 AS 和责任域都是具有独立管理主体的网络(责任域的地理范围可能更小),所以 Passport 也可以移植到 Arbra 中来.此外,Passport 的工作原理在于,使用对称密码体制为分组将要经过的每个 AS 生成该分组关键信息(包括源 IP 项)的杂凑值,其他 AS 通过验证该杂凑值就可以判断分组源 IP 项的真实性.如何安全地分发对称密钥是 Passport 方案的关键,在设计中,Passport 使用 Diffie-Hellman 交换完成密钥协商,而密钥协商过程的安全性依赖于域间路由的安全性.由第 4.2.1 节和第 4.2.2 节可知,Arbra 消除了安全路由机制的部署障碍,因此也为 Passport 方案的应用扫清了道路.

5 可扩展性分析

本节以路由表规模为指标对比了 Arbra,Internet,LISP 和 AIP 的可扩展性.为了与 Internet 和 LISP 具有可比性,本节在计算 Arbra,AIP 的路由表规模时没有考虑安全路由和安全转发机制的影响.研究表明:虽然 Arbra 不允许前缀聚合,但是同 Internet,LISP 和 AIP 相比,它明显降低了路由表的规模.

我们使用 2009 年 1 月~2010 年 6 月的 RouteViews RIB[45]数据定量分析 Arbra,Internet,LISP 和 AIP 的路由表规模,涉及的符号见表 5.

Table 5 List of symbols

表 5 符号说明

s	路由表规模,单位:比特	e	路由表表项数
b	路由表项的长度,单位:比特	r	域间路由器的对等体数
q	互联网中的 AS 数	p	互联网中的 IP 前缀数
q_t	互联网中传输 AS*数	p_t	传输 AS 拥有的 IP 前缀数

*将仅在 BGP 路径属性末端出现的 AS 称作残桩 AS;残桩 AS 之外的其他 AS 称作传输 AS.

为了讨论的简明,不失合理性,假设每个责任域(Arbra),AD(AIP)和 AS(Internet 和 LISP)仅拥有一个域间路由器.因为 Arbra,AIP 和 LISP 的域间路由机制和 BGP 相似,都是一种路径向量协议,所以上述路由结构中的每个域间路由器都需要维护本地路由表和转发表,此外,还需要为每个对等体保持一份完整的路由表,所以有

$$s=(r+2)\times b\times e \tag{16}$$

下面通过分析 RouteViews RIB 数据给出 Arbra,Internet,LISP 和 AIP 中 r,b 和 $e(r_a,r_i,r_l,r_p;b_a,b_i,b_l,b_p;\ e_a,e_i,e_l,e_p)$ 的取值情况:

(1) r:由文献[46]可知,可以假设 r_i=100;因为 Arbra 中的核心网拓扑和 Internet 中的 AS 级拓扑同构(定理 2),所以 $r_a=r_i$=100;同样,由文献[47]可知,$r_l=r_i$=100;由文献[35]可知,$r_p=r_i$=100;

(2) b:路由表表项中包含的信息,主要有“目的网络标签”、“下一跳地址”、“路径属性”.不失合理性,假设所有的路由表表项仅包含上述信息,那么有

$$b=d+n+k\times l \tag{17}$$

其中,d 表示目的网络标签的长度,n 表示下一跳地址的长度,k 表示路径属性序列中元素的个数,l 表示路径属性序列中每个元素的长度.表 6 给出了 d,n,l 在 Arbra,Internet,LISP 和 AIP 中的取值情况.

Table 6 Values of d, n, l in various networks

表 6 各种网络中 d,n,l 的取值

单位(bits)\方案	Arbra	Internet	LISP	AIP
d	88	64	64	160
n	128	32	32	160
l	88	16	16	160

下面推导 k 值,k 在 Arbra,Internet,LISP 和 AIP 中分别记作 k_a,k_i,k_l,k_p.

分析 2009 年 1 月~2010 年 6 月 RouteViews RIB 数据,可以得到 k_i 的均值 $E(k_i)$,见表 7.由表 7 可以看出,从 2009 年 1 月~2010 年 6 月共 18 个月的时间内,$E(k_i)$的最大值为 4.92(2010 年 3 月),最小值为 3.35(2009 年 4 月),平均值为 4.03.所以,可以令 $E(k_i)$=4.03.

由 $E(k_i)$可以得到 $E(k_a)$和 $E(k_p)$:

① 因为 Arbra 中的核心网拓扑和 Internet 中的 AS 级拓扑同构(定理 2),所以 $E(k_a)=E(k_i)$=4.03;

② 由文献[35]可知,$E(k_p)=E(k_i)$=4.03.

Table 7 Mean of k in the Internet

表 7 互联网中 k 的均值

时间	$E(k_i)$	时间	$E(k_i)$	时间	$E(k_i)$	时间	$E(k_i)$	时间	$E(k_i)$
2009.01	4.15	2009.05	4.41	2009.09	4.86	2010.01	3.54	2010.05	4.34
2009.02	3.81	2009.06	4.27	2009.10	3.43	2010.02	4.00	2010.06	4.02
2009.03	4.70	2009.07	3.99	2009.11	3.82	**2010.03**	**4.92**	/	/
2009.04	**3.35**	2009.08	3.74	2009.12	3.55	2010.04	3.59	/	/

LISP 将边缘网络排除在域间路由之外.因为 LISP 没有划定边缘网络的具体范围,所以本节采用通常做法,将残桩 AS 的全体当做边缘网络.所以在计算 $E(k_l)$时,应该预先从 RouteViews RIB 数据中剔除和残桩 AS 相关的路由表表项.表 8 列出了 $E(k_l)$的取值情况.可以看到,$E(k_l)$的最大值为 4.69(2010 年 3 月),最小值为 3.12(2009 年 4 月),平均值为 3.79.所以,可以令 $E(k_l)$=3.79.

Table 8 Mean of k in the LISP

表 8 LISP 中 k 的均值

时间	$E(k_l)$	时间	$E(k_l)$	时间	$E(k_l)$	时间	$E(k_l)$	时间	$E(k_l)$
2009.01	3.89	2009.05	4.13	2009.09	4.61	2010.01	3.34	2010.05	4.14
2009.02	3.56	2009.06	4.04	2009.10	3.19	2010.02	3.76	2010.06	3.79
2009.03	4.45	2009.07	3.72	2009.11	3.57	**2010.03**	**4.69**	/	/
2009.04	**3.12**	2009.08	3.51	2009.12	3.35	2010.04	3.35	/	/

这时,由公式(17)可以分别求得 b 在 Arbra,Internet,LISP 和 AIP 中的平均值(分别记做 $E(b_a)$,$E(b_i)$,$E(b_l)$和 $E(b_p)$),见表 9.

Table 9 Length of the routing table entry

表 9 路由表表项的长度

$E(b_a)$	$E(b_i)$	$E(b_l)$	$E(b_p)$
570.64-bit	160.48-bit	156.64-bit	964.8-bit

(3) e:从 RouteViews RIB 数据可以得到 e_a,e_i,e_l,e_p 的值.

① 对于 Arbra 网络,因为核心路由协议以传送责任域为目的网络,并根据传送责任域标签组织路由表,所以 e_a 等于传送责任域的数目.又因为 Arbra 中的核心网拓扑和 Internet 中的 AS 级拓扑同构(定理 2),所以 $e_a=q$.也就是,e_a 等于互联网中自治系统的数量.所以分析 2009 年 1 月~2010 年 6 月的 RouteViews RIB 数据,可以得到 e_a 随时间的变化关系,如图 10 所示.由图 10 可见,当置信水平为 95%时,e_a 随时间 τ(表示距离 2009 年 1 月的月份数)的变化关系可以拟合为指数函数:

$$e_a(\tau)=q(\tau)=3.057\mathrm{e}^{7.046\tau\times10^{-3}}\times10^4 \tag{18}$$

② 对于 Internet,$e_i=p$.分析 RouteViews RIB 数据,可以得到 e_i 随时间 τ的变化关系,如图 11 所示.可见,当置信水平为 95%时,e_i 随 τ的变化关系可以拟合为指数函数:

$$e_i(\tau)=p(\tau)=2.901\mathrm{e}^{7.384\tau\times10^{-3}}\times10^5 \tag{19}$$

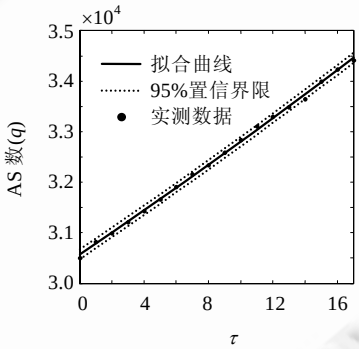

Fig.10 Number of Ases

图 10 自治系统的数量

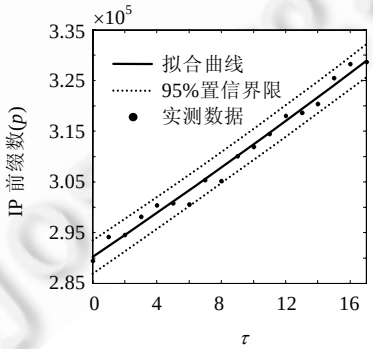

Fig.11 Number of IP prefixes

图 11 IP 前缀的数量

③ 对于 LISP,$e_l=p_t$,即 e_l 等于传输自治系统拥有的 IP 前缀数.分析 RouteViews RIB 数据,可以得到 e_l 随时间 τ的变化关系,如图 12 所示.可见,当置信水平为 95%时,e_l 随 τ的变化关系可以拟合为指数函数:

$$e_l(\tau)=p_t(\tau)=1.625\mathrm{e}^{7.494\tau\times10^{-3}}\times10^5 \tag{20}$$

④ 由文献[35]可知,$e_p=p$.所以由图 11 可见,当置信水平为 95%时,e_p 随 τ的变化关系可以拟合为指数函数:

$$e_p(\tau)=p(\tau)=2.901\mathrm{e}^{7.384\tau\times10^{-3}}\times10^5 \tag{21}$$

将 $r_a=r_i=r_l=r_p=100$、表 9 中的 $E(b)$值和公式(18)~公式(21)代入公式(16),可以分别求得 Arbra,Internet,LISP 和 AIP 中路由表规模 s_a,s_i,s_l,s_t 的均值随时间 τ的变化关系:

$$E(s_a(\tau)) = 1.78\mathrm{e}^{7.046\tau\times10^{-3}}\times10^9 \tag{22}$$

$$E(s_i(\tau)) = 4.75\mathrm{e}^{7.384\tau\times10^{-3}}\times10^9 \tag{23}$$

$$E(s_l(\tau)) = 2.60\mathrm{e}^{7.494\tau\times10^{-3}}\times10^9 \tag{24}$$

$$E(s_p(\tau)) = 2.85\mathrm{e}^{7.384\tau\times10^{-3}}\times10^{10} \tag{25}$$

按照公式(22)~公式(25)可以画出 $E(s_a(\tau))$,$E(s_i(\tau))$,$E(s_l(\tau))$和 $E(s_p(\tau))$在区间$\tau\in[1,240]$(2009 年~2029 年)内的变化情况,如图 13 所示.可以看到:

① $E(s_a(\tau))$,$E(s_i(\tau))$,$E(s_l(\tau))$和 $E(s_p(\tau))$随着 τ的增加而指数增加;

② 对于任意τ,都有 $E(s_a(\tau))\leqslant E(s_l(\tau))\leqslant E(s_i(\tau))\leqslant E(s_p(\tau))$成立.其中,AIP 路由表的规模($E(s_p(\tau))$)最大,大约比其他 3 种路由结构高出一个数量级;

③ Arbra 路由表的规模($E(s_a(\tau))$)最小,与 Internet 相比大约下降了 64.4%,与 LISP 相比下降了 36.1%.

所以,图 13 清晰地表明:虽然 Arbra 不允许前缀聚合,但是它的路由表规模仍然远远小于 Internet,LISP 和 AIP.与 Internet,LISP 和 AIP 相比,Arbra 具有更好的可扩展性.

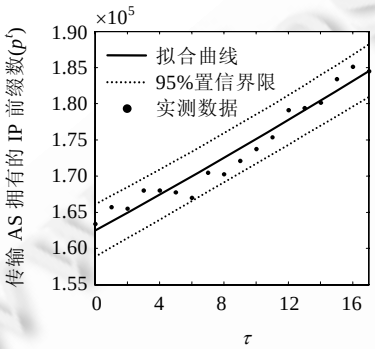

Fig.12 Number of IP prefixes in transimitting Ases

图 12 传输自治系统拥有的 IP 前缀数

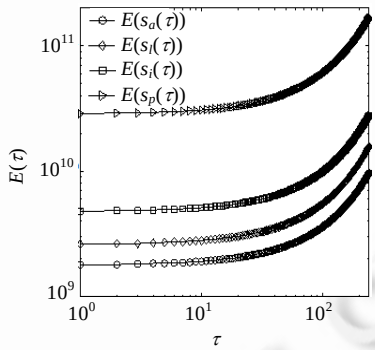

Fig.13 Scale of routing table

图 13 路由表规模

6 性能分析

本节从端到端延时方面对比了 Arbra,Internet,LISP 和 AIP 的性能.这里的端到端延时是指消息由源端到目的端的传输时间,它是路由体系数据平面(data plane)的重要性能指标.本节的研究表明,与 AIP,LISP 等著名新型路由体系相比,Arbra 的通信性能处于合理水平.

将消息由源端到目的端的传输延时定义为 T,将 Arbra,IPv4,IPv6,LISP 和 AIP 等路由结构中的 T 值依次记作 T_r,T_4,T_6,T_l 和 T_a.定义消息大小为 M,定义核心网中分组的首部大小为 n,定义路径最大传输单元(path maximum transmission unit,简称 PMTU)为 K.传输之前,应将 M 分解成一个或多个分组,定义这些分组的总比特数为 N.公式(26)给出了 N 的计算方法.

$$N = M + \left\lceil \frac{M}{K-n} \right\rceil \times n \tag{26}$$

假设网络处于轻负载状态,所以可以忽略丢包重传、排队延时和处理延时.这样,$T(M)$可以表示为

$$T(M) = \begin{cases} ((j-1)K+N)/R, & M > (K-n) \\ j(M+n)/R, & M \leqslant (K-n) \end{cases} \tag{27}$$

其中,j 是源端和目的端之间的链路数,R 是每条链路的传输速度.

因为 Arbra 和 IPv6 一样,地址长度都是 128-bit,所以在 Arbra 中可以使用和 IPv6 一样的首部格式.将 Arbra,IPv4,IPv6,LISP with IPv4,LISP with IPv6 和 AIP 中的 n 值分别记做 n_r,n_4,n_6,n_{l4},n_{l6} 和 n_a,从第 2.4 节、文献[47]和

文献[35]可以计算得到 n_r,n_4,n_6,n_{l4},n_{l6} 和 n_a,见表 10.

Table 10 Length of packet headers (Byte)

表 10 分组的首部大小 (字节)

n_r	80	n_4	20	n_6	40
n_{l4}	56	n_{l6}	96	n_a^*	138

*计算 n_a 时,假设每一个端节点的地址具有格式 AD_1:AD_2:EID

假设 K=1500 字节,j=6,R=100MB/s(注意,j 和 R 值的选取不会影响最终比较结果),则从公式(26)、公式(27)和表 10 可以计算出 $T_r(M)$,$T_4(M)$,$T_6(M)$,$T_{l4}(M)$,$T_{l6}(M)$和 $T_a(M)$,如图 14 所示.

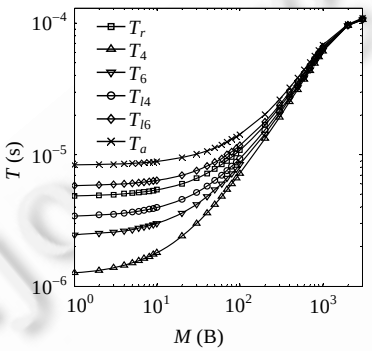

Fig.14 Message transimitting delay

图 14 消息传输延时

从图 14 可以看到:

(1) 随着 M 的增加,$T_r(M)$,$T_4(M)$,$T_6(M)$,$T_{l4}(M)$,$T_{l6}(M)$和 $T_a(M)$相应地增加,并且它们都处于相同的数量级.这表明,在以 T 为评估指标的情况下,Arbra,IPv4,IPv6,LISP with IPv4,LISP with IPv6 和 AIP 的性能处于同一水平;

(2) 对于任意 M,都有 $T_a(M)>T_{l6}(M)>T_r(M)>T_{l4}(M)>T_6(M)>T_4(M)$成立.这表明,当以 T 为评估指标时,虽然 Arbra 的性能差于 IPv4,IPv6,LISP with IPv4,但是优于 AIP 和 LISP with IPv6.因为 AIP 和 LISP 都是具有较大影响力的研究方案,所以可以说,Arbra 的性能是合理的.

7 可部署性分析

本节以端节点、边缘网络、核心网络中可能发生设备的软硬件改变为指标,对比了 Arbra,LISP 和 AIP 的部署代价.比较结果见表 11,其中,“√”表示需要改变,“×”表示不需要改变.注意,在表 11 中,Arbra,LISP 和 AIP 所谓的改变都是相对于 IPv6 网络而言.

由表 11 可以看到,Arbra 对 IPv6 网络的改变小于 AIP,大于 LISP.然而考虑到 Arbra 的可扩展性和安全性,Arbra 相对于 LISP 额外引入的部署代价是合理的,这是因为:一方面,虽然 LISP 是以提高域间路由可扩展性为目标的设计方案,但是由第 5 节可知,它的可扩展性要差于 Arbra;另一方面,LISP 和 Internet 一样,仍然缺乏必要的安全措施,然而,Arbra 通过分布式的信任模型,为解决前缀劫持、路由伪造和源地址欺骗问题奠定了基础.

Table 11 Comparisons of deployment cost

表 11 部署代价的比较

指标/方案		Arbra	LISP	AIP
端节点	硬件	×	×	√
	操作系统	×	×	√
	应用程序	×	×	√
边缘网络	边缘路由器	×	×	√
	域内路由器	×	×	√
	路由机制	×	×	√
核心网络	BGP,iBGP 路由器	√	×	√
	域内路由器	×	×	√
	域间路由机制	√	×	√
	域内路由机制	×	×	√
	封装路由器	√	√	×
	映射服务器	√	√	×
其他	DNS	×	×	√

8 结论和展望

本文提出了一种基于责任域的两级路由结构 Arbra,分析了 Arbra 的安全性,对比了 Arbra 与其他 4 种路由结构的异同,并从可扩展性、通信性能和部署代价等方面研究了 Arbra 的可行性.本文的研究表明:

(1) Arbra 具有分布式的信任模型,为前缀劫持、路由伪造和源地址欺骗问题的解决奠定了基础;

(2) Arbra 的路由表规模比 AIP 下降了一个数量级,与 Internet 和 LISP 相比,Arbra 的路由表规模分别下降了 64.4%和 36.1%;

(3) 以端到端延时为指标时,Arbra 同其他路由结构的通信性能处于同一水平,但是 Arbra 要差于 IPv4, IPv6,LISP with IPv4,同时优于 AIP 和 LISP with IPv6;

(4) Arbra 的部署代价大于 LISP,但是小于 AIP.

此外,还可以从以下方面进一步拓展,加深本文的研究成果:

(1) 细粒度的策略路由和流量工程.

在 Internet 中,通过修改链路开销,自治系统能够灵活地支持 IP 前缀级别的路由选择功能和入站流量控制功能.但是在 Arbra 中,边缘网被排除在核心网之外,核心路由协议基于传送责任域组织路由表,这意味着,所有链接到同一个传送责任域的端责任域,必须共享相同的网络路径.为了应对这种功能缺失,计划在 Arbra 中支持多路径,具体思路为:① 修改 Arbra 地址中的保留域,以表示不同的网络路径;② 在(端责任域、位置标签)映射关系中添加路由参数,以选择不同的网络路径,从而实现端责任域级别的路由选择功能和入站流量控制功能.虽然多路径会增大域间路由表规模和路由更新数量,但是考虑到它同样具有许多突出的优点(例如故障容忍、带宽的增加和安全性的进一步提高),所以在 Arbra 中增加对多路径的支持是有益的.当然,这需要详细的分析和评估.

(2) 对其他安全问题的思考.

除了前缀劫持,路由伪造和源地址欺骗攻击,拒绝服务泛洪也是路由体系面临的一个重要挑战.计划借鉴 TVA[48]方案应对 Arbra 中可能存在的拒绝服务泛洪攻击.在 TVA 方案中,终端在发送分组之前需要获得一个来自接收方的令牌,令牌中包含了接收方对本次通信的许可和要求.终端必须将该令牌添加到要发送的分组中.分布在网络中的验证节点检查令牌,以确定是否应该清除分组.虽然本文没有考虑拒绝服务攻击,但是因为 Arbra 可以有效保证源地址的真实性,所以在 Arbra 中,TVA 能够得到极大地简化.例如,TVA 中充当源标签的预能力和路径标识都可以省略.

References:

[1] Ramachandran A, Feamster N. Understanding the network-level behavior of spammers. Computer Communication Review, 2006, 36(4):291−302. [doi: 10.1145/1151659.1159947]

[2] Ballani H, Francis P, Zhang XY. A study of prefix hijacking and interception in the Internet. In: Proc. of the ACM SIGCOMM 2007. 2007. [doi: 10.1145/1282380.1282411]

[3] Bono VJ. 7007 explanation and apology. 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html

[4] Lad M, Oliveira R, Zhang BC, Zhang LX. Understanding resiliency of internet topology against prefix hijack attacks. In: Proc. of the DSN. 2007. [doi: 10.1109/DSN.2007.95]

[5] Cert advisory CA-1996-21 TCP SYN flooding and IP spoofing attacks. 1996. http://www.cert.org/advisories/CA-1996-21.html

[6] Touch J. Defending TCP against spoofing attacks. RFC 4953, Internet Engineering Task Force, 2007.

[7] Moore D, Shannon C, Brown DJ, Voelker GM, Savage S. Inferring Internet denial-of-service activity. ACM Trans. on Computer Systems, 2006. 115-139. [doi: 10.1145/1132026.1132027]

[8] Cert advisory CA-1998-01 smurf IP denial-of-service attacks. 1998. http://www.cert.org/advisories/CA-1998-01.html

[9] Paxson V. An analysis of using reflectors for distributed denial-of-service attacks. ACM Computer Communications Review, 2001, 31(3):38−47. [doi: 10.1145/505659.505664]

[10] Scalzo F. Anatomy of recent DNS reflector attacks from the victim and reflector points of view. Nanog37 Presentation, 2006.

[11] Subramanian L, Roth V, Stoica I, Shenker S, Katz RH. Listen and whisper: Security mechanisms for BGP. In: Proc. of the Symp. on Networked Systems Design and Implementation (NSDI). 2004.

[12] Lad M, Massey D, Pei D, Wu YG, Zhang BC, Zhang LX. PHAS: A prefix hijack alert system. In: Proc. of the USENIX Security Symp. (Security). 2006.

[13] Goodell G, Aiello W, Griffin T, Ioannidis J, McDaniel P, Rubin A. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In: Proc. of the ISOC NDSS 2003. 2003.

[14] Karlin J, Forreat S, Rexford J. Pretty good BGP: Improving BGP by cautiously adopting routes. In: Proc. of the IEEE Int'l Conf. on Network Protocols. 2006. [doi: 10.1109/ICNP.2006.320179]

[15] Ferguson P, Senie D. Network ingress filtering: Defending denial of service attacks which employ IP source address spoofing. RFC 2827, Internet Engineering Task Force, 2000.

[16] Killalea T. Internet service provider security service and procedures. RFC3013, Internet Engineering Task Force, 2000.

[17] Baker F. Requirements for IP version 4 routers. RFC 1812, Internet Engineering Task Force, 1995.

[18] Baker F, Savola P. Ingress filtering for multihomed networks. RFC 3704, Internet Engineering Task Force, 2004.

[19] Li J, Mikovic J, Wang MQ, Reiher P, Zhang LX. SAVE: Source address validity enforcement protocol. In: Proc. of the IEEE INFOCOM. 2002. 1557−1566. [doi: 10.1109/INFCOM.2002.1019407]

[20] Wu JP, Bi J, Bagnulo M, Baker F. Source address validation improvement framework. Draft-ietf-savi-framework-06, Internet Engineering Task Force, 2011.

[21] Lü GF, Sun ZG, Lu XC. Enhancing the ability of inter-domain IP spoofing prevention. Ruan Jian Xue Bao/Journal of Software, 2010,21(7):1704−1716 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3573.htm [doi: 10.3724/SP.J.1001.2010.03573]

[22] Savage S, Wetherall D, Karlin A, Anderson T. Practical network support for IP traceback. In: Proc. of the ACM SIGCOMM 2000. 2000. [doi: 10.1145/347059.347560]

[23] Bellovin SM. ICMP traceback messages. draft-bellovin-itrace-00, Internet Engineering Task Force, 2000.

[24] Stone R. CenterTrack: An IP overlay network for tracking DoS floods. In: Proc. of the 9th USENIX Security Symp. 2000. 2000.

[25] Yaar A, Perrig A, Song D. FIT: Fast Internet traceback. In: Proc. of the IEEE INFOCOM 2005. 2005.

[26] Yaar A, Perrig A, Song D. Pi: A path identification mechanism to defend against DDoS attack. In: Proc. of the IEEE Symp. on Security and Privacy. 2003. 93−107. [doi: 10.1109/SECPRI.2003.1199330]

[27] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications (JSAC), 2000,18(4):582−592. [doi: 10.1109/49.839934]

[28] Ng J. Extensions to BGP to support secure origin BGP (soBGP). Draft-ng-sobgp-bgp-extension-00, Internet Research Task Force, 2006.

[29] Hu YC, Perrig A, Sirbu M. SPV: A secure path vector routing for securing BGP. In: Proc. of the ACM SIGCOMM 2004. 2004. [doi: 10.1145/1015467.1015488]

[30] Hu XJ, Zhu PD, Gong ZH. SE-BGP: An approach for BGP security. Ruan Jian Xue Bao/Journal of Software, 2008,19(1):167−176 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/167.htm [doi: 10.3724/SP.J.1001.2008.00167]

[31] Li Q, Wu JP, Xu MW, Xu K, Zhang XW. GesBGP: A good-enough-security BGP. Chinese Journal of Computers, 2009,32(3):506−515 (in Chinese with English abstract).

[32] Wang N, Zhi YJ, Zhang JH, Cheng DN, Wang BQ. Identity-Based secure inter-domain routing protocol. Ruan Jian Xue Bao/Journal of Software, 2009, 20(12):3223−3239 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3396.htm [doi: 10.3724/SP.J.1001.2009.03396]

[33] Kent S, Seo K. Security architecture for the internet protocol. RFC 4301, Internet Engineering Task Force, 2005.

[34] Liu X, Li A, Yang XW, Wetherall D. Passport: Secure and adoptable source authentication. In: Proc. of the 5th USENIX Symp. on Networked Systems Design & Implementation (NSDI 2008). 2008. 365−378.

[35] Andersen DG, Balakrishnan H, Feamster N, Keoponen T, Moon D, Shenker S. Accountable Internet protocol (AIP). Computer Communication Review, 2008,38(4):339−350. [doi: 10.1145/1402946.1402997]

[36] Hinden R. New scheme for internet routing and addressing (ENCAPS) for IPNG. RFC 1955, Internet Engineering Task Force, 1996.

[37] Spring N, Mahajan R, Wetherall D. Measuring ISP topologies with rocketfuel. In: Proc. of the ACM SIGCOMM 2002. 2002. [doi: 10.1109/TNET.2003.822655]

[38] Coltun R, Ferguson D, Moy J, Lindem A. OSPF for IPv6. RFC 5340, Internet Engineering Task Force, 2008.

[39] Malkin G, Minnear R. RIPng for IPv6. RFC 2080, Internet Engineering Task Force, 1997.

[40] Blake-Wilson S, Bolyard N, Gupta V, Hawk C, Moller B, Bochum RU. Elliptic curve cryptography (ECC) cipher suites for transport layer security (TLS). RFC 4492, Internet Engineering Task Force, 2006.

[41] Digital Signature Standard (DSS). Federal information processing standards publication. DRAFT FIPS PUB 186-3, 2008.

[42] Caesar M, Condie T, Kannan J, Lakshminarayanan K, Stoica I, Shenker S. ROFL: Routing on flat labels. Computer Communication Review, 2006,36(4):363−374. [doi: 10.1145/1151659.1159955]

[43] Cheon JH, Kim Y, Yoon HJ. A new ID-based signature with batch verification. Report 2004/131, Cryptology ePrint Archive, 2004.

[44] Granger R, Page D, Stam M. Hardware and software normal basis arithmetic for pairing-based cryptography in characteristic three. IEEE Trans. on Computers, 2005,54(7):852−860. [doi: 10.1109/TC.2005.120]

[45] University of Oregon RouteViews project. http://www.routeviews.org

[46] Fall K, Godfrey PB. Routing tables: Is smaller really much better? In: Proc. of the HotNets-IX. 2010.

[47] Farinacci D, Fuller V, Meyer D, Lewis D. Locator/ID separation protocol (LISP). Draft-farinacci-lisp-12, Internet Engineering Task Force, 2007.

[48] Yang XW, Wetherall D, Anderson T. TVA: A Dos-limiting network architecture. IEEE/ACM Tran. on Networking, 2008,16(6): 1267−1280. [doi: 10.1109/TNET.2007.914506]

附中文参考文献:

[21] 吕高峰,孙志刚,卢锡城.域间 IP 欺骗防御服务增强机制.软件学报,2010,21(7):1704−1716. http://www.jos.org.cn/1000-9825/3573.htm [doi: 10.3724/SP.J.1001.2010.03573]

[30] 胡湘江,朱培栋,龚正虎.SE-BGP:一种 BGP 安全机制.软件学报,2008,19(1):167−176. http://www.jos.org.cn/1000-9825/19/167.htm [doi: 10.3724/SP.J.1001.2008.00167]

[31] 李琦,吴建平,徐明伟,徐恪,张新文.自治系统间的安全路由协议 GesBGP.计算机学报,2009,32(3):506−515.

[32] 王娜,智英建,张建辉,程东年,汪斌强.一个基于身份的安全域间路由协议.软件学报,2009,20(12):3223−3239. http://www.jos.org.cn/1000-9825/3396.htm [doi: 10.3724/SP.J.1001.2009.03396]

卢宁宁(1982－),男,河北石家庄人,博士生,主要研究领域为路由与交换技术,网络安全.
E-mail: radioboy@126.com

张宏科(1957－),男,博士,教授,博士生导师,主要研究领域为未来互联网,基于 IPv6 的路由协议.
E-mail: zhk@njtu.edu.cn