互联网域间源地址验证的可部署性评价模型

刘冰洋[1),3)] 毕 军[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 近年来,IP 源地址伪造被频繁应用于网络攻击中,对互联网安全造成极大威胁.域间源地址验证方法通过对 IP 报文进行自治域级别的验证来防御这类网络攻击.学术界提出了这类方法的评价指标,并依照该指标设计出很多新的方法.然而,这些方法尽管指标值优秀,却无一能在实际中得到互联网服务提供商的广泛部署.究其原因,是现有评价指标主要关注互联网整体的安全性,而没有考虑到互联网服务提供商的个体利益.文中首次从互联网服务提供商的经济诉求出发,研究域间源地址验证方法的可部署性评价模型.作者提出将部署收益、部署开销和运维风险作为可部署性评价的 3 项基本指标,并给出其形式化定义;从理论上证明了该指标体系的合理性;建立了评价模型,为每个指标设计了完善的量化评价方法;以现有著名域间源地址方法的部署收益评价为例,展示了将理论模型应用于方法评价的具体流程,并对评价结果进行深入分析;最后,作者讨论了方法可部署性与互联网整体安全性的关系、方法设计的优化目标以及如何应用模型指导方法的设计.该评价模型的提出,对于设计更易于部署的方法具有指导意义,并有利于促进域间源地址验证方法在互联网的部署.

关键词 源地址验证;评价模型;可部署性;拒绝服务攻击;网络安全;域间;互联网

中图法分类号 TP393 **DOI 号** 10.3724/SP.J.1016.2015.00500

On the Deployability Evaluation Model of Internet Inter-Domain Source Address Validation

LIU Bing-Yang[1),3)] BI Jun[1),2),3)]

[1)](*Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing* 100084)

[2)](*Department of Computer Science, Tsinghua University, Beijing* 100084)

[3)](*Tsinghua National Laboratory for Information Science and Technology (TNList), Beijing* 100084)

Abstract In recent years, IP spoofing is frequently used in network attacks, which immensely threatens the Internet security. Inter-domain source address validation methods defend against these attacks by enforcing the domain-level source address verification on the IP packets. The academia has proposed the evaluation criteria for these methods, and designed many methods according to the criteria. However, although these methods meet the criteria, none of them is widely deployed by Internet service providers (ISPs) in practice. The reason is that the current criteria mainly focus on the security of the global Internet, but considers little about ISPs' individual interests. For the first time, this paper studies the deployability evaluation model of the inter-domain source address validation methods from the perspective of the ISPs' economic appeals. We propose deployment benefit, deployment cost and operational risk as the three deployability evaluation criteria, and present their formal definitions; the rationality of the criteria is proved

收稿日期:2013-06-27;最终修改稿收到日期:2014-09-30.本课题得到国家"八六三"高技术研究发展计划项目基金(2013AA013505)、国家自然科学基金(61472213)资助.**刘冰洋**,男,1985 年生,博士,博士后,主要研究方向为网络体系结构、IP 源地址验证、软件定义网络和互联网经济学等.E-mail:liubingyang@tsinghua.edu.cn;bingyangliu.cn@gmail.com.**毕 军**(通信作者),男,1972 年生,博士,教授,博士生导师,主要研究领域为互联网体系结构、未来互联网、互联网路由和 IP 源地址验证与追溯等.E-mail:junbi@tsinghua.edu.cn.

theoretically; an evaluation model is established, which specifies the comprehensive quantitative evaluation mechanism for each criterion; we apply the model on the evaluation of deployment benefit of existing methods to demonstrate the concrete evaluation process, and present deep analysis of the evaluation results; finally, we discuss the relationship between the deployability of the methods and the security of the global Internet, the optimization objective of the design of the methods, and the use of the model in guiding the method design. The evaluation model will guide the design of highly deployable methods, and facilitate the deployment of inter-domain source address validation methods on the Internet.

Keywords　source address validation; evaluation model; deployability; denial of service attack; network security; inter-domain; Internet

1　引　言

随着多年的飞速发展，互联网已经深入渗透到社会的方方面面，成为承载人类经济和文化活动的不可或缺的信息基础设施. 与此同时，互联网的安全问题也因为影响到人们的生产生活而得到了社会各界的广泛关注. 近些年来，基于源地址伪造的网络攻击由于流量巨大、难以追溯和难以防御等特点，被不法分子频繁利用，造成了重大的经济损失[1-4]. 此外，源地址伪造行为还对网络的可信、管理、计费、测量等造成危害，阻碍了网络的健康发展，成为当今互联网亟待解决的重要安全问题①②[5-6].

源地址伪造是指网络主机使用未被合法分配的IP 地址作为源地址发送报文的行为. 互联网上信息的传输采用分组交换的方式，每个 IP 分组(即报文)都携带着源地址和目的地址，路由器仅根据目的地址决定报文的传输方向，并逐跳地转发至目的主机. 在这种基于目的地址的转发模式中，路由器无需查看报文的源地址，也不对其进行检查. 这就使得主机可以使用假冒的源地址发送报文而不影响其到达目的主机.

源地址伪造可以应用于拒绝服务(Denial of Service，DoS)攻击中达到隐匿攻击源、放大攻击流量的目的，使得这种攻击更难发现、更难防御、危害更大[5]. 基于源地址验证的 DoS 攻击分为两类[7]. 第 1 类是 d-DoS，攻击者直接发送大量攻击报文至受害者来淹没其网络带宽，这些报文携带任意的(很多时候是随机的)源地址，使得受害者难以判断攻击者的位置[8]. 第 2 类是 s-DoS，攻击者向一些无关的服务器(比如域名服务器)请求大量的数据，这些请求报文的源地址被设置为受害者的 IP 地址，这样从服务器返回的大量数据就会淹没受害者. 第 2 类攻击也被称作反射攻击，由于返回的数据报文的尺寸往往远大于请求报文，就使得 s-DoS 产生了放大攻击流量的效果，因此也被称作放大攻击[9].

源地址验证技术通过识别和过滤伪造报文来防御基于源地址伪造的网络攻击. 根据 RFC5210 的描述，源地址验证体系结构分为 3 个层次，自底向上为接入网层、自治域内层和自治域间层，分别执行 IP 地址粒度、IP 地址前缀粒度和自治域粒度的源地址验证[10]，如图 1 所示.

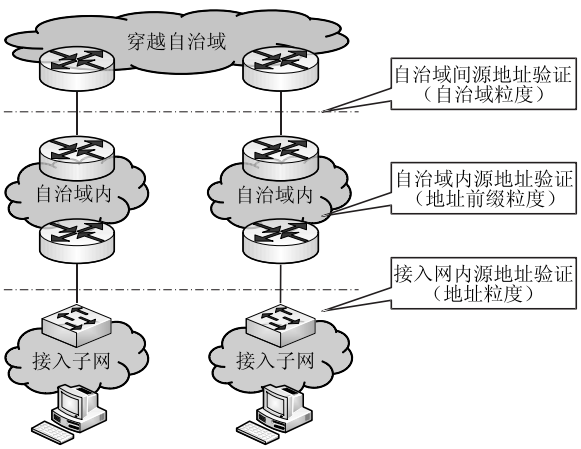

图 1　源地址验证体系结构的各个层次

其中，接入网和域内源地址验证都是部署在同一自治域内、对本自治域内的主机和子网向外发送的报文进行检查，而几乎无法(或极少能够)识别出从自治域外部发进来的伪造报文[11-13]. 因此，前两个层次的作用主要是完成本自治域的细粒度网络管理，在防御外来伪造攻击方面的作用不大. 而域间源

① Spoofer Project [EB/OL]. http://spoofer.cmand.org 2013, 12, 31

② The DDoS That Almost Broke the Internet [EB/OL]. http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet 2013, 9, 8

地址验证的主要作用，就是进行自治域之间伪造流量的识别和过滤，实现对自治域的保护. 域间源地址验证方法一般部署在自治域的边界路由器上，通过人工配置、自动学习或服务器部署等方式，将源地址绑定到路由器的入向端口或者密码学标识上，凡是与绑定不匹配的报文都会被识别为伪造报文而被丢弃掉[14-19]. 从互联网自治域级别拓扑的粒度来看，也可以视作将源地址映射到自治域，并将自治域绑定到拓扑的有向边或者密码学标识上. 域间源地址验证原则上只需检查一个源地址所属的自治域是否真实，而无需识别自治域内主机之间的相互伪造，其检查粒度比域内和接入网源地址验证要粗，但在防御基于源地址验证的 DoS 攻击方面十分有效[14,20].

十余年来，工业界和学术界为防御伪造攻击做出了大量努力. 工业界的 Ingress/Egress Filtering(IEF)和 unicast Reverse Path Forwarding(uRPF)技术已经在路由器中广泛实现[21-22]，但很多网络运行者并没有启用和维护这些技术. 这导致互联网上仍有大量自治域允许源地址伪造[6]，而且这些技术的启用率已经多年没有提升[5]. 学术界提出了许多新的域间源地址验证方法[23-24]，但尚没有一种方法能够在实际中得到广泛部署. 这样的现状说明了已有的域间源地址验证方法在促进部署方面都存在一定的缺陷. 更糟的是，在本领域现有的评价体系下，这些方法看上去都很优秀；而新提出的方法往往依照该评价体系进行设计优化，其结果依然是难以得到部署. 因此，我们认为，在现阶段，本领域研究的关键点并不是新方法的设计，而是需要回答两个更加根本的问题：什么样的方法更易于部署，以及如何评价方法的可部署性.

我们知道，今天的互联网是由数万个自治的网络组成的，而这些网络由不同的互联网服务提供商(Internet Service Provider，ISP)运营. 绝大多数的 ISP 都以营利目的，他们是否部署一项新的网络技术，取决于该技术是否能够给自己带来利润的增长，而非能否为整个互联网的安全做出贡献. 而现有评价体系所主要关心的恰恰就是互联网的整体利益. 比如，在衡量方法的过滤效果时，该评价体系主要考虑互联网整体的伪造流量的减少，而不是攻击部署者的流量的减少；再如，该评价体系关心达到某种防御效果需要多少自治域的部署(越少越好)，却不关心在实际中如何激励这些自治域去部署. 在这样的评价体系下，方法的设计也更偏重整体利益而轻部署者的利益，因此难以得到 ISP 的认可.

本文的主要动机和基本目标是，从部署者的利益出发，通过研究方法可部署性的基本指标并建立其评价模型，指引方法的设计更加贴合部署者的利益诉求，从而促进方法的广泛部署，以达到互联网整体安全性的最终目标. 本文的特色和创新之处在于：通过对 ISP 的调研，首次提出将部署收益、部署开销和运维风险作为评价域间源地址验证方法可部署性的 3 项基本指标，并给出形式化定义；通过 ISP 的利润公式的推导，从理论上验证了该评价体系的合理性和完备性；我们为每个指标建立了理论评价模型，将方法的指标值与方法的工作原理、互联网的结构和攻击的特征联系起来，从而可以利用现实数据予以定量评价；通过对现有方法的部署收益的评价，介绍了模型应用的具体流程，并通过对评价结果的深入分析提炼出具有高部署收益的方法的技术特征；此外，我们还讨论了方法可部署性与互联网整体安全性的关系以及方法设计的优化目标. 最后，我们总结了本文的主要贡献，并对未来发展方向做出展望.

本文第 2 节介绍源地址验证评价工作的发展现状；第 3 节介绍本文所提出的评价指标，并证明其合理性和完备性；第 4 节介绍理论评价模型；第 5 节介绍模型应用的示例；第 6 节讨论可部署性与互联网整体安全性的关系、方法设计的优化目标及如何应用模型指导方法设计；第 7 节进行总结和展望.

2 域间源地址验证评价工作现状

文献[23]总结了现有域间源地址验证方法所采取的评价指标. 尽管各个方法所提及的概念略有差异，但归纳起来，使用较多的评价指标主要包括有效性(减少的伪造流量的比例)、假阳性率(错误地丢弃合法报文的比例)、计算开销、存储开销和网络开销等. 但是，在具体应用这些指标进行评价时，各个方法所采取的参数不尽相同. 比如，在评价有效性时，Hop Count Filtering(HCF)侧重于评价被攻击网络独立地部署方法时(既有部署率为 0% 时)的有效性，这是因为 HCF 的优势是独立部署的高效性[25]；而 Path Identifier(PiIP)侧重于评价既有部署率高于 50% 时的有效性，这是因为 PiIP 在高部署率下非常有效、在低部署率下存在较大的假阳性[26]. 可见，尽管本领域中存在较为通用的评价指标，但如何应用这些指标仍然较为混乱，难以进行方法间的横向比较.

一些综述性的文章也提出了一些指标来对方法

比较评价. 比如，文献[24]提出的 6 项指标为识别能力、可部署性、本质特征、路由协议无关性、攻击缓解能力和定位能力；而文献[20]采取了有效性、开销、安全性和假阳性率这 4 项指标. 这些指标当中，识别能力、攻击缓解能力、定位能力、有效性等主要描述的是方法得到部署后对整个互联网的伪造行为的遏制，而不是体现部署者个体利益. 此外，方法的开销尽管描述了部署者所关注的要点，但是却无法直接将具体的计算复杂度、存储复杂度等参数与现实中 ISP 的部署支出联系起来.

总而言之，目前域间源地址验证的评价研究主要存在两个问题. 一是指标体系较为混乱，不同的方法采取不同的指标和参数完成自身的评价，方法之间难以横向比较. 二是现有指标无法或者难以描述部署实体(ISP)的个体诉求，这就造成了即便依照这些指标进行设计、并且指标十分优秀的方法，也可能无法得到 ISP 的认可、难以在实际网络中得到部署应用. 因此，我们需要统一的、能够描述 ISP 利益诉求的可部署性评价指标，来促进方法设计的研究和方法在实际中的部署.

3　评价指标

3.1　互联网服务提供商的部署诉求

为了设计切合实际的评价指标，我们在北美网络运营组①中调研了实际网络的运营人员，考察其在部署和运维源地址验证方法时最关心的指标，归纳起来主要包括以下 3 点(调研全文见②)：

(1) 部署收益. ISP 是以经济利益为驱动的市场主体，其部署新技术的动力是追求潜在的经济利益，而非单纯地为互联网整体做贡献. 因此，部署源地址验证技术一定要给该 ISP 带来额外的收益.

(2) 部署开销. 新技术的部署和应用必然带来新的开销. 此开销包含配置维护开销；如果新的开销无法被当前设备所支持(如存储空间不足、计算资源不足等)，还需要对设备的软件甚至硬件进行升级，造成额外的经济支出.

(3) 运维风险. 源地址验证方法一般会将所识别出的伪造报文丢弃掉. 如果源地址验证技术存在假阳性，则会造成部分合法的报文被误判为伪造报文而丢弃掉，导致合法用户的数据传输业务被破坏. 这样的运维风险可能导致直接或间接的经济损失，经济损失往往是 ISP 无法忍受的.

3.2　评价指标的定义

我们将 ISP 的诉求进行抽象，给出 3 项评价指标，定义如下.

3.2.1　部署收益

定义 1.　一个方法的部署收益是指当一个自治域部署了这个方法后，其受到的伪造攻击中伪造报文的减少比率的增量的期望.

为了形式化描述该定义，我们定义如下符号(表 1).

表 1　基本符号定义

符号	定义
V	互联网节点(自治域)的集合
E	互联网边(自治域邻接关系)的集合
G	互联网的域间拓扑，又作 $G(V,E)$
G^*	带有路由信息的互联网域间拓扑
f	所考虑的域间源地址验证方法
D	已经部署了 f 的节点的集合
N	尚未部署 f 的节点的集合，显然 $N=V-D$
n	一个自治域节点，$n\in V$

基于以上符号，考虑一个尚未部署方法 f 的节点 $n\in N$，其部署收益的函数形式为 $benefit(f,G^*,D,n)$. 假设在某次伪造攻击中，全球网络攻击 n 的伪造报文的集合为 att_n. 由于 D 中的节点部署了 f 而过滤掉了一些伪造报文，设被 D 过滤掉的伪造报文的集合为 $att_{n,D}$；而当 n 也部署了 f 之后，部署节点集变为 $D\cup\{n\}$，其过滤掉的的伪造报文的集合为 $att_{n,D\cup\{n\}}$. 相应地，被 D 和 $D\cup\{n\}$ 过滤掉的伪造报文的比率分别为 $reduce_{n,D}=|att_{n,D}|/|att_n|$ 和 $reduce_{n,D\cup\{n\}}=|att_{n,D\cup\{n\}}|/|att_n|$. 部署收益表达的是“减少比率的增量”，即 $reduce_{n,D\cup\{n\}}-reduce_{n,D}$，也即“比之前更好了多少”，或者“增加的收益是多少”，而这也恰恰是 ISP 所关注的.

进一步地，我们将部署收益定义为减少比率的增量的期望来消除在具体的网络攻击个体之间的差异，也即统计意义上的平均值. 根据期望的线性特性，部署收益的表达式如下(其中 $E[x]$ 表示变量 x 的期望)：

$$benefit(f,G^*,D,n)=E[reduce_{n,D\cup\{n\}}]-E[reduce_{n,D}].$$

3.2.2　部署开销

定义 2.　一个方法的部署开销是指，在当前网络设备功能和资源的限制下，部署此方法给 ISP 带来的额外开销的离散度量.

① North American Network Operators' Group (NANOG) [EB/OL]. http://www.nanog.org/

② BCP38 Deployment[EB/OL]. http://mailman.nanog.org/pipermail/nanog/2012-March/047086.html

具体地说，部署开销是传统开销(计算开销、存储开销、网络开销等)的阶梯函数，其取值分为 4 个等级：(L_0)不产生任何投资或运维开销，(L_1)只产生配置维护开销，(L_2)只产生软件或固件的更新开销以及可能的配置维护开销，(L_3)产生硬件更新开销以及可能的软固件开销和配置维护开销. 显然，对 ISP 来说，4 个等级的经济支出依次递增. L_0 是基准线，实际上不存在“不做任何事情就可以完成源地址验证”的方法. 开销为 L_1 的方法充分利用了现有路由器的功能和资源，通过配置的更新和维护即可实现. 开销为 L_2 的方法的计算和存储等需求可以利用现有路由器的硬件资源来实现，但需要更新软件或固件来增加或优化某些功能，一般需要投入开发和测试新的软固件映像. 开销为 L_3 的方法的计算和存储开销无法通过当前的路由器硬件资源来实现，需要升级硬件，从而造成购买新设备以及更换或添加设备的投资开销. 需要说明的是，如果升级硬件仍然无法满足方法的需求，则该方法是无法在现实中得到实现的，因此也无法给 ISP 带来部署开销的问题. 本文不对此类方法进行评价.

下式为方法的部署开销函数的自然语言描述，我们将在模型中对式中各项条件进行完整的形式化表达.

$$cost(f)=\begin{cases}L_0, & \text{当不需要做任何改变}\\ L_1, & \text{当传统开销可通过更新配置实现}\\ L_2, & \text{当传统开销可通过更新软固件及配置实现}\\ L_3, & \text{当传统开销只有更新硬件才能实现}\end{cases}$$

3.2.3 运维风险

定义 3. 一个方法的运维风险是该方法的时均假阳性率，也就是在长期运行过程中方法错误地过滤掉合法报文的平均比率.

设在 n 部署了 f 之后的相当长的一段时间内，经过 n 的合法报文的集合为 leg_n，而被 n 判断为伪造且被丢弃掉的报文的集合为 dis_n，那么产生的假阳性率即运维风险就是

$$risk(f,G^*,D,n)=|leg_n\cap dis_n|/|leg_n|.$$

运维风险沿用了传统指标中的假阳性率的概念，但却与传统的假阳性率有两点重要的不同：

(1)时间维度. 传统的假阳性率其实描述的是方法的“过滤时假阳性率”，对于如下两类方法不作区分：第 1 类方法是，不管是否正在发生攻击，过滤机制一直开启，假阳性在过滤时一直存在；第 2 类方法是，配合攻击检测机制，仅当攻击发生时开启过滤. 而本文所定义的运维风险从长期的运维时间内来观察假阳性率，显然第 2 类的方法要具有更低的运维风险，更符合 ISP 的实际诉求.

(2)空间维度. 一个 ISP 可能覆盖很大的地理范围和很多的子网，而网络攻击一般只针对一个或几个子网. 这样看来，仅对遭受攻击的子网前缀开启过滤、而对其他的前缀不进行过滤可以将假阳性率控制在一个较小的范围，对 ISP 来说具有更低的风险. 传统的假阳性率只描述“过滤处假阳性率”，对于如下两类方法不作区分：第 1 类方法是，无论遭受攻击的是哪些子网，对整个域的流量都开启过滤；第 2 类方法是，仅对遭受攻击的子网开启过滤，对其他子网不过滤. 本文所定义的运维风险在计算中考虑到了第 2 类方法，其运维风险低于第 1 类方法，体现出了 ISP 的实际诉求.

3.3 评价指标的合理性验证

本文通过对 ISP 的调研总结提炼出可部署性的 3 项评价指标，这是一个逆向推导的过程. 下面，我们直接从 ISP 的利润公式正向推导来验证所提出的评价指标的合理性.

在经济学中，一个企业的利润等于其总的收益减去总的成本[27]，即

$$PROFIT=Total\ REVENUE-Total\ COST.$$

ISP 的总体收益和总体成本的构成可能非常复杂，而我们只关心“部署域间源地址验证方法”这一个业务带来的利润的增量，即

$$\Delta PROFIT=\Delta REVENUE-\Delta COST,$$

其中，$\Delta PROFIT$ 是ISP要最大化的目标，$\Delta REVENUE$ 为部署该方法为该 ISP 带来的收益增量，$\Delta COST$ 为部署开销的增量. 下面我们对 $\Delta REVENUE$ 和 $\Delta COST$ 进行展开.

$\Delta REVENUE$ 包含两个部分，一是通过为客户提供更加安全的数据传输服务而带来的收入增加，记作 $\Delta REVENUE_+$；另一部分是方法的假阳性造成的对客户的数据传输的服务质量的下降，从而导致的客户流失和收入减少，记作 $\Delta REVENUE_-$. 那么，$\Delta REVENUE=\Delta REVENUE_+-\Delta REVENUE_-$.

$\Delta REVENUE_+$ 与部署所带来的安全性的增量有关，具体的说，就是与伪造攻击中伪造报文减少比率的增量(也就是部署收益 $benefit$)呈正相关，即弱递增函数，记为 $\Delta REVENUE_+=Rev_+(benefit)$. 类似地，$\Delta REVENUE_-$ 是方法长期运维风险($risk$)的弱递增函数，记为 $\Delta REVENUE_-=Rev_-(risk)$.

而开销的增量 $\Delta COST$ 就是方法总的部署开

销. 我们所定义的部署开销 $cost$ 是指一台边界路由器上的开销，并没有考虑部署自治域自身的属性(如自治域的大小、所需部署的路由器的数量等)，因此，$\Delta COST$ 并不是 $cost$ 本身，而是其弱递增函数，记作 $\Delta COST=Cost(cost)$.

因此，部署源地址验证方法给 ISP 带来的利润增量为

$$\Delta PROFIT=Rev_{+}(benefit)-Rev_{-}(risk)-Cost(cost).$$

从上式可以看出，ISP 的利润增量是我们提出的 3 项评价指标的函数，这也验证了所提出的评价指标的合理性. 但值得注意的是，我们这里并没有给出各个函数的具体形式——实际上，对于不同的 ISP，函数的形式或其中的参数可能是不同的；即使对于同一个 ISP，随着时间的变化其函数也可能变化. 在这里，我们仅说明 Rev_{+}、Rev_{-} 和 $Cost$ 分别是 $benefit$、$risk$ 和 $cost$ 的弱递增函数.

4　评价模型

下面分别介绍 3 项评价指标的评价模型.

4.1　部署收益的评价模型

首先形式化定义 IP 报文. 由于本文主要研究域间场景，因此定义的粒度以自治域为基本单位.

定义 4.　一个报文是一个三元组 $a:(s,d)$，其中 a 为报文发送者所在的自治域；s 为报文的源地址所属的自治域，也即报文的源自治域；d 为报文的目的地址所属的自治域，也即报文的目的自治域. 当不关心报文的发送者时，报文可以简记作 (s,d).

定理 1.　一个伪造报文 $a:(s,d)$ 属于域间源地址验证范围的充要条件是 $a\neq s$ 且 $a\neq d$.

证明.　充分性. 由于 $a\neq d$，报文 $a:(s,d)$ 是跨域传输的，可能经过自治域边界路由器对出域和入域流量的检查；其次，由于 $a\neq s$，报文所携带源地址不属于其发送者所属的自治域，因此，自治域粒度的源地址检查可能识别此伪造. 因此，此报文属于域间源地址验证的范围.

必要性. 由于域间源地址验证只识别自治域粒度的源地址伪造，同一自治域内的伪造无法识别，因此要求 $a\neq s$；其次，域间源地址验证技术部署在自治域的边界路由器上，对穿越自治域边界的报文进行源地址检查，因此要求此报文属于跨域通信，因此 $a\neq d$.

证毕.

下文中，如无特殊说明，当我们提到伪造报文 $a:(s,d)$ 时，默认其满足 $a\neq s$ 且 $a\neq d$.

在之前的章节中，我们介绍了利用伪造源地址发起的两种 DoS 攻击，即直接的(即针对目的地址的)攻击 d-DoS 以及反射式的(即针对源地址的)攻击 s-DoS. 尽管两种攻击的形式有所不同，但在表示方式上却可以做到统一. 我们用如下 3 个符号代表攻击中的 3 种角色(表 2)：

表 2　伪造源地址攻击中的角色

符号	定义
a	伪造报文的发送者：它可能是攻击者本身(attacker)或攻击者所控制的主机(agent).
t	攻击目标(target)：在 d-DoS 中，攻击目标是伪造报文的目的地址；在 s-DoS 中，攻击目标是伪造报文的源地址.
i	无辜者(innocent)，即无辜地被牵扯到攻击中的主机或 IP 地址：在 d-DoS 中，无辜者是伪造报文的源地址，从攻击目标看来，攻击报文是从这些无辜的“替罪羊”发来的；在 s-DoS 中，无辜者是伪造报文的目的地址，被无辜地利用来做反射.

此处，我们定义报文的另一种表达形式：“攻击报文”. 需要说明的是，这里定义的攻击不包括 s-DoS 中从反射点反射出的报文，而只包括由攻击者或攻击者所控制的主机发出的报文.

定义 5.　一个攻击报文被定义为如下形式：(a,i,t)，其中 a 为攻击者即报文的发送者，i 为无辜者，t 为攻击目标.

根据 d-DoS 和 s-DoS 的定义，显然，当攻击为 d-DoS 时，$(a,i,t)=a:(i,t)$；当攻击为 s-DoS 时，$(a,i,t)=a:(t,i)$.

下面定义报文的自治域粒度的转发路径，在本文环境下简称为报文的转发路径.

定义 6.　报文 $a:(s,d)$ 的转发路径是指报文在不被丢弃的情况下，从发送端自治域到目的自治域所经过的自治域序列，记作 $Path[a:(s,d),G^{*}]$，简写作 $Path[a:(s,d)]$ 或者 $Path[a\rightarrow d]$.

定义 7.　我们说自治域 n 在 $a:(s,d)$ 的转发路径上当且仅当 n 是 $Path[a:(s,d)]$ 中的一个节点，记作 $n\in Path[a:(s,d)]$.

定义 8.　方法 f 的过滤函数是指，给定一个部署节点 n 并假设 n 已经部署 f，在不考虑报文 $a:(s,d)$ 在转发时是否经过 n 的情况下，n 对该报文是否为伪造报文的判断函数. 其形式为 $filter(f,G^{*},n,a:(s,d))$. 当判为伪造，函数返回 1；否则，返回 0.

上面定义的过滤函数不考虑报文转发路径、部署节点集合等实际情况，因此无法描述在给定部署节点集的情况下该报文是否真的会被路径上的部署点丢弃掉. 为此，定义丢弃函数如下.

定义 9. 给定方法 f、带有路由信息的拓扑 G^*、部署点集合 D 和报文 $a:(s,d)$，判断该报文在其转发路径上是否会被部署节点识别为伪造而被丢弃. 当被丢弃，函数返回 1；否则，返回 0. 其函数形式为 $discard(f,G^*,D,a:(s,d))$.

给定过滤函数，丢弃函数的计算方法如下（其中，$sgn()$ 是符号函数[28]）：

$$discard(f,G^*,D,a:(s,d))=sgn\left(\sum_{n\in(D\cap Path[a:(s,d)])} filter(f,G^*,n,a:(s,d))\right).$$

为了描述部署收益的期望值，我们假设互联网伪造攻击服从某种概率分布（但并不对具体服从何种分布做假设），在该分布下，每个自治域都有一定的成为攻击者、无辜者和攻击目标的概率. 对于自治域 n，其成为攻击者、无辜者和攻击目标的概率分别记作 PA_n、PI_n 和 PT_n. 本文假设这 3 个概率的分布是相互独立的，此时，

$$E[reduce_{n,D}]=PT_n^{-1}\cdot\sum_{a\neq n}\sum_{i\neq a}PA_aPI_iPT_n discard(f,G^*,D,(a,i,n)),$$

即

$$E[reduce_{n,D}]=\sum_{a\neq n}\sum_{i\neq a}PA_aPI_i discard(f,G^*,D,(a,i,n)).$$

类似地，

$$E[reduce_{n,D\cup\{n\}}]=\sum_{a\neq n}\sum_{i\neq a}PA_aPI_i discard(f,G^*,D\cup\{n\},(a,i,n)).$$

这样，部署开销就可以得到完全展开，如下式：

$$benefit(f,G^*,D,n)=\sum_{a\neq n}\sum_{i\neq a}PA_aPI_i\begin{pmatrix}discard(f,G^*,D\cup\{n\},(a,i,n))\\-discard(f,G^*,D,(a,i,n))\end{pmatrix}.$$

至此，我们完成了在部署节点集合为 D 时、非部署点 n 的部署收益的表达 $benefit(f,G^*,D,n)$. 然而，我们还需要消除因 n 的个体选取差异造成的收益评价偏见，因此要对 N 中所有节点的部署收益进行平均. 我们把平均收益记作 $benefit(f,G^*,D,N)$，由于 N 与 D 互为补集，因此可以简写作 $benefit(f,G^*,D)$.

在计算平均收益时，由于各个自治域遭受伪造攻击的概率不同，因此我们采用加权平均来体现差别，那么平均部署收益的表达式如下：

$$benefit(f,G^*,D)=\sum_{n\in N}PT_n benefit(f,G^*,D,n)\Big/\sum_{n\in N}PT_n.$$

值得说明的是，我们在计算部署收益时涉及到了 3 个参数 PA_n、PI_n 和 PT_n（分别表示 n 成为攻击者、无辜者和攻击目标的概率）. 为了保持评价模型的一般性，我们并不为这 3 个参数假设任何特定的概率分布，模型的应用者可以根据需要及所能获得的数据设定合适的分布. 实际的概率分布应当结合网络测量来确定：一般情况下，普通用户的计算机比内容提供商的服务器更可能被攻击者利用来发送伪造报文（因此 PA_n 可能更大），高性能、开放式的服务器比普通用户的计算机更可能被利用作为 s-DoS 的反射点（因此 PI_n 可能更大），而承载重要服务的服务器比普通用户的计算机更可能成为攻击的目标（因此 PT_n 可能更大）. 然而，在没有足够的实际数据或者只需要进行粗略的评价时，也可以采用简单的概率分布，比如，IP 地址意义上的均一的概率（这也是本领域最为常用的假设分布），此时，$PA_n=PI_n=PT_n=size_n$，其中 $size_n$ 是 n 的地址空间大小占整个可路由地址空间大小的比率.

平均部署收益是在给定部署节点集合 D 的前提下计算出的，为了消除 D 的选取所带来的偏见，我们需要选取不同的 D. 如果要选取所有的 D，则共有 $2^{|V|}$ 种取法. 由于在当今互联网上，$|V|$ 的大小大约为4 万，选取所有 D 的指数级计算复杂度是无法承受的. 因此我们需要采取一些近似的办法去评估部署收益. 基本原则是，选取不同正整数 $k(0\leq k<|V|)$ 作为 D 的大小；在这个大小限制下，随机选取节点作为 D 中的节点，算出平均部署收益，并反复多次，对多次的评价部署收益再做平均，作为当前大小 k 下的部署收益；最后，以 k 为横轴，画出不同部署节点集合大小下的部署收益变化曲线，从而完整地近似方法 f 的部署收益，记作 $benefit(f,G^*)$. 再对不同的互联网拓扑 G^*（比如不同年份的拓扑）分别绘制相应曲线，比较异同和发展趋势，得到 $benefit(f)$.

4.2 部署开销的评价模型

首先定义传统开销向量.

定义 10. 方法 f 的传统开销向量 $\boldsymbol{c}_f$ 的各个分量是其对路由器不同资源的消耗量. 其形式为 $(c_f^c,c_f^s,c_f^n,\cdots)$，这里各个分量分别为计算开销 (c_f^c)、存储开销 (c_f^s)、网络开销 (c_f^n) 等.

定义 11. 传统开销常约束向量 $\boldsymbol{CC}_l$ 是指在当前路由器的条件下，在开销级别 L_l 上对各个传统开销分量的上限限制. 比如，$\boldsymbol{CC}_1$ 是在 L_1 开销级别上的常约束向量，开销为 L_1 的方法的各项传统开销分量值都不能超过 $\boldsymbol{CC}_1$ 的相应分量值.

定义 12. 传统开销向量的比较符号“=”、“≤”、

“$\not\leq$”. 我们说 $\boldsymbol{c}_1=\boldsymbol{c}_2$，当且仅当 $\boldsymbol{c}_1$ 的所有分量值都等于 $\boldsymbol{c}_2$ 的相应分量值. 我们说 $\boldsymbol{c}_1\leq\boldsymbol{c}_2$，当且仅当 $\boldsymbol{c}_1$ 的所有分量值都小于或等于 $\boldsymbol{c}_2$ 的相应分量值；否则，我们说 $\boldsymbol{c}_1\not\leq\boldsymbol{c}_2$.

部署开销函数的形式化表达如下：

$$cost(f)=\begin{cases}L_0, & \boldsymbol{c}_f\leq\boldsymbol{CC}_0\\ L_1, & \boldsymbol{c}_f\not\leq\boldsymbol{CC}_0,\ \boldsymbol{c}_f\leq\boldsymbol{CC}_1\\ L_2, & \boldsymbol{c}_f\not\leq\boldsymbol{CC}_1,\ \boldsymbol{c}_f\leq\boldsymbol{CC}_2\\ L_3, & \boldsymbol{c}_f\not\leq\boldsymbol{CC}_2\end{cases},$$

其中，$0=\boldsymbol{CC}_0\leq\boldsymbol{CC}_1\leq\boldsymbol{CC}_2$.

下面解释各个分式的具体含义：

L_0：$\boldsymbol{CC}_0$ 的各个分量均为 0，要求 f 的各个传统开销分量都为 0，即什么都不做，包括不做配置和维护. 显然这种方法是不存在的.

L_1：$\boldsymbol{CC}_1$ 的各个分量是指在只改变现有路由器的配置的前提下可以支持的相应传统开销分量的最大值. 以过滤规则的存储开销为例，CC_1^s 是在现有路由器的功能下，通过配置访问控制列表(ACL)能够支持的用户规则数目的最大值.

L_2：$\boldsymbol{CC}_2$ 的各个分量是指在只改变现有路由器的软件和固件(以及可能的配置改变)可以支持的传统开销分量的最大值. 还以过滤规则的存储开销为例，CC_2^s 是在现有路由器的硬件条件下，通过对软件或固件的更新可支持的过滤规则数目的上限.

L_3：当方法 f 的部署开销 $\boldsymbol{c}_f$ 中存在一个分量，使得该分量大于 $\boldsymbol{CC}_2$ 的相应分量时，这个分量无法通过软件、固件和配置来实现，此时需要升级硬件来满足方法在该分量的需要. 仍以过滤规则的存储开销为例，即使升级算法、软固件，所需的过滤规则数仍超过路由器硬件能力，则需更新硬件.

部署开销的评价模型中涉及到了一些参数. L_0、L_1、L_2 和 L_3 表示部署开销的级别，由于我们只关心级别的相对关系，其具体取值并不重要，所以我们只规定 $L_0<L_1<L_2<L_3$. 传统开销常约束向量 $\boldsymbol{CC}_l$ 是指在当前路由器的条件下，开销级别 L_l 上对各个传统开销分量的上限限制. $\boldsymbol{CC}_0$ 的各个分量均为 0 是因为 L_0 要求不产生任何新的开销. 而对于 $\boldsymbol{CC}_1$ 和 $\boldsymbol{CC}_2$ 的各个分量，我们在评价模型中并不设定特定的取值. 这是因为，随着技术的发展，路由器的软件和硬件的功能和性能都在变化，因此 L_1 和 L_2 的开销上限也在变化. 为保持评价模型的一般性意义，我们不能根据今天路由器的形态为 $\boldsymbol{CC}_1$ 和 $\boldsymbol{CC}_2$ 的各个分量赋值——模型的使用者应根据当时的环境为其赋值.

方法部署开销是各个传统开销分量的阶梯函数，图 2 举例说明了开销向量包含计算开销和存储开销两个维度时阶梯函数的一个特例(高维时，整体空间超过三维，难以画出；为简单示意，以二维向量为例)，其中纵轴是部署开销的各个阶梯的取值.

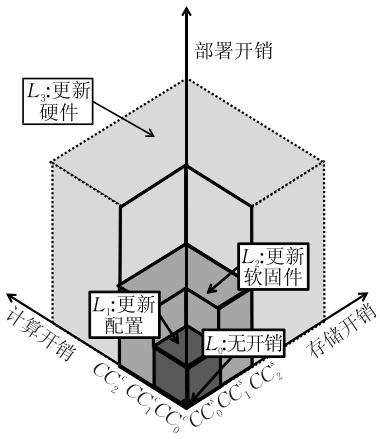

图 2　部署开销阶梯函数示意

与部署收益类似，部署开销也应该反映各个自治域部署的平均开销. 上文所描述的开销是针对每个路由器而言的. 通常，一个 ISP 的规模越大、边界路由器越多、资本越雄厚. 我们假设自治域的经济规模和边界路由器的个数成正比，这样，一个自治域的所有路由器都部署的话，其总开销占该自治域的经济总量的比例是近似的. 因此，方法在一台路由器上的开销反映了在各自治域的平均开销.

本文对部署开销的各个级别的定义描述了 ISP 对技术的实际开销的主要诉求. 在各个级别内部还可以对方法的开销再度进行细分. 比如，同是仅需要配置更新的方法 f_1 和 f_2，如果 f_1 占用 ACL 的条目数比 f_2 少，则在更细的维度上 f_1 优于 f_2. 为保持理论的简洁，除非特别指出，本文主要考虑开销的 4 个级别的离散取值，这也反映了 ISP 的主要诉求.

4.3　运维风险的评价模型

根据前文对于运维风险的分析，传统的假阳性率描述的是“过滤时、过滤处”的假阳性率，即只能够描述“不分时空”(即一直过滤、对所有流量都过滤)的一类方法. 但实际上，存在一些分时或分空的方法，下面对这几类方法进行定义.

定义 13.　“不分时空”的方法是指，不管是否发生攻击而一直过滤，不管谁受攻击而为所有地址空间过滤的域间源地址验证方法，其集合记作 F_{NN}.

定义 14.　“分时不分空”的方法是指，仅在攻击发生时进行过滤，不管谁受攻击而为所有地址空间过滤的域间源地址验证方法，其集合记作 F_{TN}.

定义 15. “分时分空”的方法是指，仅在攻击发生时进行过滤，且仅为遭受攻击的地址空间过滤的域间源地址验证方法，其集合记作 F_{TS}.

之所以不定义“分空不分时”的方法，是因为“遭受攻击的地址空间”本身就具有时间概念，当攻击结束后，它就不再是遭受攻击的地址空间.

4.3.1 不分时空的方法的运维风险

由上面的定义可以得出，F_{NN} 中的方法 f 的运维风险就是该方法的假阳性率，记作 FP_f. FP_f 由两部分组成，一部分是方法从原理上的固有假阳性率，记作 FPT_f；另一部分是在实现中算法的近似、资源的限制等产生的实践假阳性率，记作 FPP_f.

定理 2. 如果方法 f 的固有假阳性与实践假阳性相互独立，则其假阳性率 $FP_f=FPT_f+FPP_f-FPT_f\cdot FPP_f$.

证明. 由于理论的假阳性率为 FPT_f，则理论的真阳性率为 $1-FPT_f$；同理，实践真阳性率为 $1-FPP_f$. 由于实践假阳性与固有假阳性相互独立，那么最终的真阳性率为理论真阳性率与实践真阳性率的乘积，即 $(1-FPT_f)(1-FPP_f)$. 因此，最终的假阳性率为 $FP_f=1-(1-FPT_f)(1-FPP_f)$，展开得 $FP_f=FPT_f+FPP_f-FPT_f\cdot FPP_f$. 证毕.

由于方法的假阳性率与方法所部署的网络状况、已部署的节点集和所考虑的具体节点都有关，因此其形式应为 $FP(f,G^*,D,n)$，计算公式为

$$FP(f,G^*,D,n)=FPT(f,G^*,D,n)+FPP(f,G^*,D,n)-FPT(f,G^*,D,n)\cdot FPP(f,G^*,D,n).$$

在给定假阳性率的情况下，不分时空的方法的运维风险可以直接得出，如下式：

$$risk(f,G^*,D,n)=FP(f,G^*,D,n),$$

其中，$f\in F_{NN}$.

4.3.2 分时不分空的方法的运维风险

设在相当长的一段时间里共发生了与 n 相关、需要 n 过滤的 NA_n 次攻击，设这段时间的总长度为 1，第 k 次攻击的发生的时间区间为 $RI_{n,k}=[begin_{n,k},end_{n,k}]$，其中 $0\le k\le NA$ 且 $0\le begin_{n,k}\le end_{n,k}\le 1$. 那么，过滤发生的时间的总长度、也即过滤时间占总时间的比率为 $\left|\bigcup_k RI_{n,k}\right|$，其中 $\bigcup_k RI_{n,k}$ 表示将所有攻击的时间区间合并为一些互不相连、互不重叠的区间的集合，而 $\left|\bigcup_k RI_{n,k}\right|$ 表示 $\bigcup_k RI_{n,k}$ 中所有区间的长度的和.

对于分时不分空的方法 f 来说，其运维风险等于其假阳性率 $FP(f,G^*,D,n)$ 乘以其进行过滤的时间比率，即

$$risk(f,G^*,D,n)=FP(f,G^*,D,n)\cdot\left|\bigcup_k RI_{n,k}\right|,$$

其中，$f\in F_{TN}$.

4.3.3 分时分空的方法的运维风险

设第 k 次攻击影响到的合法流量占总合法流量的比率为 $RV_{n,k}$. 假设如果两个攻击由攻击的时间区间的重叠，其所影响的合法流量不重叠，即攻击事件在时空双维度上是互斥的. 在互斥的前提下，不同攻击所带来的运维风险就可以直接进行加运算而不需考虑集合重叠带来的重复计算. 此时，分时分空的方法 f 的运维风险可用下式计算：

$$risk(f,G^*,D,n)=FP(f,G^*,D,n)\cdot\sum_k RI_{n,k}\cdot RV_{n,k},$$

其中，$f\in F_{TS}$.

4.3.4 平均运维风险

前面所描述的运维风险 $risk(f,G^*,D,n)$ 是在已部署节点为 D 的情况下非部署节点 n 上的风险. 该风险是有意义的，因为它正是直接描述节点 n 的部署风险、是 n 最为关心的. 但从方法评价的角度来说，一个节点的风险可能由于该节点的特殊性具有偏见，因此，我们采用部署收益评价模型中的手段，对 N 中所有节点的运维风险进行加权平均；再对同样大小的不同 D 进行平均；再对不同大小的 D 的平均值画出发展曲线，作为该方法的运维风险. 其中，对于确定的 D，平均运维风险表达式如下：

$$risk(f,G^*,D)=\sum_{n\in N} size_n risk(f,G^*,D,n)\Big/\sum_{n\in N} size_n.$$

基于 $risk(f,G^*,D)$，方法 f 最终的运维风险函数 $risk(f)$ 的计算方式与基于 $benefit(f,G^*,D)$ 计算 $benefit(f)$ 的方式一致，前文有详细介绍，此处不再赘述.

5 评价模型的应用示例

前一节介绍了可部署性指标的理论评价模型. 为了展示模型的实用性，我们在本节以部署收益为例介绍模型的具体应用方法. 我们给出了部署收益评价的具体步骤、数据的采集、评价结果和对结果的分析等. 值得说明的是，本示例中所采用的数据和参数并不一定是唯一的或最优的——如果有更精确的实际数据和参数，评价结果也会更具说服力.

5.1 评价步骤

步骤 1.

输出：$\{benefit(f)\}$

输入：$\{f\}$

对于$\{f\}$中的每个方法 f，由步骤 2 计算出 $benefit(f)$，得到所有方法的部署收益$\{benefit(f)\}$.

步骤 2.

输出：$benefit(f)$

输入：$f,\{G^*\}$

对于$\{G^*\}$中的每个拓扑G^*，由步骤 3 求得 $benefit(f,G^*)$，从而得到$\{benefit(f,G^*)\}$. 分析$\{benefit(f,G^*)\}$随拓扑的变化趋势，得到 $benefit(f)$.

步骤 3.

输出：$benefit(f,G^*)$

输入：$f,G^*,\{PA_n\},\{PI_n\},\{PT_n\}$

对每个正整数 k，随机生成 N_{avg} 个大小为 k 的 D，由步骤 4 计算出 $benefit(f,G^*,D)$. 对同一大小的 D 的 $benefit(f,G^*,D)$进行平均获得平均部署收益，并以 k 为横轴，绘制出平均部署收益随 k 的变化曲线，获得 $benefit(f,G^*)$.

步骤 4.

输出：$benefit(f,G^*,D)$

输入：$f,G^*,\{PA_n\},\{PI_n\},\{PT_n\},D$

对于每个 $n\in N$，由步骤 5 计算出 $benefit(f,G^*,D,n)$，并对 N 中各个节点的$benefit(f,G^*,D,n)$以 PT_n为权重进行加权平均，获得 $benefit(f,G^*,D)$.

步骤 5.

输出：$benefit(f,G^*,D,n)$

输入：$f,G^*,\{PA_n\},\{PI_n\},\{PT_n\},D,n$

对于每个伪造报文(a,i,n)，根据方法的过滤函数求出 $discard(f,G^*,D\cup\{n\},(a,i,n))-discard(f,G^*,D,(a,i,n))$. 再乘以 PA_aPI_i，求和得到 $benefit(f,G^*,D,n)$.

需要说明的是，对于 d-DoS 和 s-DoS，方法给出的部署收益是不同的，因此需要分别评价.

5.2　数据集

5.2.1　自治域级的互联网拓扑

我们从 UCLA 的 Internet Topology Collection 项目的公开数据集中获得互联网的自治域级拓扑①. 该数据集中不仅包括各个节点、节点之间连接的边，还标注了各条边对应的自治域之间的经济关系，包括对等关系、客户到提供商和提供商到客户 3 种关系，后面我们会依据这些关系推断互联网域间路由.

该数据集包括 2008 年 10 月 8 日至今每天的拓扑数据，我们采用了 2008 年至 2012 年每年 10 月 11 日的拓扑，共有 5 个，代表 5 年来互联网的成长和拓扑的变化.

5.2.2　自治域的地址空间大小

本文所采用的自治域的 IP 地址空间是从 CAIDA② 获得. 该数据集从 RouteViews③ 采集 BGP 更新的数据，产生 IP 地址前缀到自治域号码的映射. 所提供的数据的时间范围是从 2005 年至今. 本文采用了其中 2008 年至 2012 年每年 10 月 11 日的数据，以与拓扑数据相配合.

通过最长前缀匹配的方式，我们将前缀的有效地址空间映射到相应的自治域，从而得到每个自治域的地址空间大小. 如果有自治域的地址空间大小为 0，将其设为 1，以避免后面计算部署激励时除数为 0 的情况. 最后，计算出所有自治域的总的可路由地址空间大小，进而计算出每个自治域的地址空间大小占总空间大小的比例，即$\{size_n\}$.

5.3　路由的生成

自治域级别的路由在评价中有两个主要的用途. 一是用于确定报文的转发路径，已确定哪些节点在路径上、可以参与过滤；二是用于为基于路径的方法提供必要的信息. 本文采用 C-BGP④ 来推测路由信息. C-BGP 是一个 BGP 路由的模拟器，它以带有自治域关系的拓扑为输入，每个自治域按照自治域之间的关系、以 Valley-Free[29] 为原则进行 BGP 的宣告、传播和路径选择，当传播过程收敛以后，每个节点都形成一个完整路由表.

5.4　模拟参数

模拟参数如表 3 所示.

表 3　模拟参数

参数	取值
$\{f\}$	{BASE[18]，DPF[14]，HCF[25]，IDPF[15]，IEF[21]，PiIP[26]，SAVE[30]，SPM[16]，uRPF[22]}
$\{G^*\}$	{topo-2008，topo-2009，topo-2010，topo-2011，topo-2012}
N_{avg}	50
$\{PA_n\}$	$\{size_n\}$
$\{PI_n\}$	$\{size_n\}$
$\{PT_n\}$	$\{size_n\}$

5.5　评价结果

模拟结果显示，不同年份、不同拓扑下各个方法的部署收益曲线及其相互关系基本不变，因此，为节约篇幅，我们只展示 2012 年的数据得出的模拟结果. 图 3 和图 4 分别展示了$\{f\}$中的方法针对 d-DoS 和 s-DoS 两种攻击所产生的部署收益曲线. 初始收益大的方法有利于吸引早期的部署，而后期部署收益较高的方法则有利于长期持续部署.

① Internet AS-level Topology Archive[EB/OL]. http://irl.cs.ucla.edu/topology/

② The Cooperative Association for Internet Data Analysis (CAIDA) [EB/OL]. http://www.caida.org/

③ University of Oregon Route Views Project (Route Views) [EB/OL]. http://www.routeviews.org/

④ C-BGP[EB/OL]. http://c-bgp.sourceforge.net

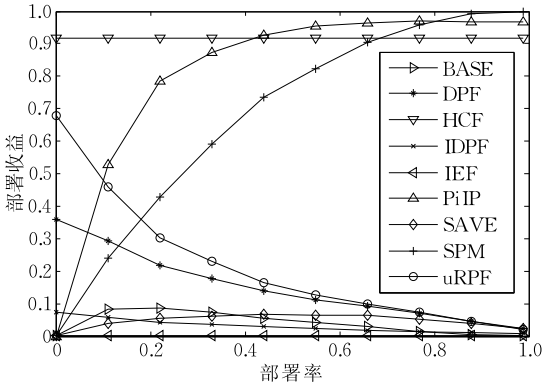

图 3 方法针对于 d-DoS 的部署收益

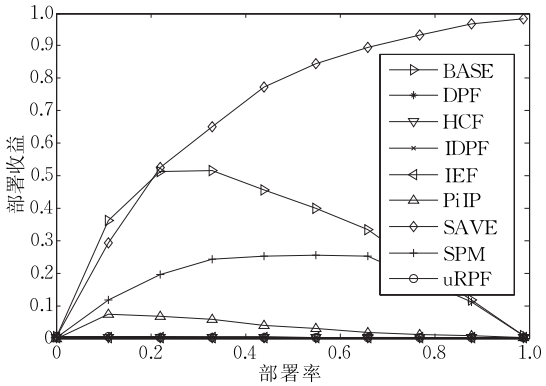

图 4 方法针对于 s-DoS 的部署收益

针对 d-DoS,DPF、HCF、IDPF 和 uRPF 都具有较好的初始部署收益,因为其过滤表的建立过程不依赖于其他自治域,即独立部署就可以获得较好的自我保护.但是除了 HCF 之外,其他方法的收益曲线都逐渐降低.其原因是,随着部署率的上升,被已有部署者过滤掉的伪造流量越来越多,而非部署者通过自己的部署能够得到的额外的过滤保护就越来越少,从而造成后期部署收益不足.而采取基于目的的域间协作的方法(SPM 和 PiIP)都展示出较好的针对于 d-DoS 的后期收益.随着部署率上升,部署者之间相互协作,通过共享信息增强彼此的过滤能力或帮助彼此过滤伪造流量,使部署者相比非部署者能得到更多的保护,因此具有更高的部署收益.

针对 s-DoS 的部署收益与 d-DoS 的最大不同是,所有方法的初始部署收益都几乎为 0.这是因为 s-DoS 中的伪造发生在攻击者和反射主机之间,这些报文绝大多数都不经过受害者,使得受害者自治域即使部署了某种方法也没有机会去过滤,因此初始部署收益很低.为了实现高部署收益,部署者之间必须采取基于源的域间协作,帮助彼此过滤伪造报文.我们可以看到,采取基于源的域间协作的方法(SPM、BASE 和 SAVE)相较其他方法具有更高的针对 s-DoS 的部署收益.

5.6 评价结果的进一步分析

从以上的评价结果可以总结,技术上采取了域间协作的方法具有较高的部署收益.实际上,自治域之间的协作主要起到两个作用.首先,域间协作可以传递和共享用于源地址验证的信息,增强部署者的过滤能力,加强对部署者的保护;其次,部署者还可以有针对性地将路由器上有限的资源仅用于对自己和其他部署者的保护,避免将资源用于为非部署者提供免费的保护.这样,一方面部署者的保护得到提升,另一方面又使得非部署者因得不到或仅得到很少的保护,从而为自治域提供了更强的部署动机.当然,全面的方法可部署性分析还需要考虑部署开销和运维风险,但由于本文的重点是评价模型,我们就不在此介绍这两个指标的评价示例,感兴趣的读者可以参见我们的在线技术报告①.

6 讨 论

6.1 可部署性与互联网整体安全性的关系

本文提出并建立了域间源地址验证方法的可部署性评价模型,意在通过引导方法从设计上注重对 ISP 的经济激励来促进方法在互联网上的广泛部署.而广泛部署则是彻底消除互联网域间伪造攻击的基础和必要条件.

定理 3. 假设 $\forall(a,d)\in E, Path[a\rightarrow d]=\{a,d\}$,那么,能够完全过滤互联网域间伪造流量的部署者的集合 D 组成了拓扑上的一个点覆盖.

证明. 对于任意伪造报文 $a:(s,d)$,它能被过滤掉仅当 $\exists n\in Path[a\rightarrow d], n\in D$,即伪造报文的转发路径上至少需要存在一个部署者.特别地,当 $(a,d)\in E$ 时,根据假设 $Path[a\rightarrow d]=\{a,d\}$,有 $a\in D$ 或者 $d\in D$.也就是说,拓扑上每一条边都至少有一个端点在 D 中,所以 D 组成了拓扑上的一个点覆盖. 证毕.

本定理中的假设 $\forall(a,d)\in E, Path[a\rightarrow d]=\{a,d\}$ 是指,如果两个自治域直接相连,那么他们之间的流量就会通过直接相连的链路传输,而不会再经其他自治域穿越传输.这个假设是很弱的,在当前互联网上很容易被满足(根据 Valley-Free 原则及最短路径选择).

① 互联网域间源地址验证方法的评价模型与比较评价[EB/OL]. http://netarchlab.tsinghua.edu.cn/~junbi/THU-NetArchLab-SAV-InterAS-Model-v1-20130501.pdf

由于寻找拓扑中的最小点覆盖是 NP 难问题，计算最优解需要消耗大量时间和计算资源，因此我们并没有计算当前互联网域间拓扑的最小点覆盖.但根据文献[14]，1999 年互联网的最小点覆盖包含大概 18.9%的自治域.而随着互联网拓扑结构的扁平化[31]，此比例可能仍在增加.即使仍以此比例计算，当前互联网上共有 45977 个自治域①，那么最小点覆盖也包含 8690 个自治域.显然，哪怕假设所有自治域都有识别任何域间伪造报文的能力，完全消除域间伪造攻击仍需要 8690 个自治域的部署.在当前去中心化的互联网上，只能通过各个自治域内生的激励去部署.因此，研究方法可部署性的问题是解决互联网整体安全问题的关键；而方法具备高部署性则是其得到广泛的部署并最终解决互联网域间源地址伪造问题的必要条件.

6.2　方法设计的优化目标

第 3.3 节给出了利润增量的表达式 $\Delta PROFIT=Rev_+(benefit)-Rev_-(risk)-Cost(cost)$，其中，$Rev_+$、$Rev_-$ 和 $Cost$ 分别是 $benefit$、$risk$ 和 $cost$ 的弱递增函数.显然，若以 $\Delta PROFIT$ 最大化为方法的优化目标，我们需要分别最大化 $benefit$、最小化 $risk$ 和 $cost$.最理想的情况是，$benefit=1$、$risk=0$ 且 $cost=L_0$.但实际上，不产生任何开销就能完全过滤伪造报文且没有任何假阳性的方法是不存在.也就是说，$benefit$、$risk$ 和 $cost$ 可能相互约束，解空间中的一部分是不可行的.我们把描述这些约束、寻找可行解空间作为一项未来工作.

如果我们可以给出 Rev_+、Rev_- 和 $Cost$ 的具体形式，即最优化的目标函数表达式，那么结合约束条件，我们就可以通过解此最优化问题找到最优方法.然而，正如我们在第 3.3 节所提到的，即使目标函数的形式得以确定，函数的形式或其中的参数也可能因不同 ISP 而不同、随时间而变化.因此，针对某一表达式所求出的最优方法未必具有长久、普遍的意义.

确定方法优化目标的另一个思路是，通过增加限制条件缩小可行解的空间，并在较小的空间内寻找针对 3 个指标的多个帕累托最优方法(未必是 $\Delta PROFIT$ 最优的方法).比如，由于数据传输是 ISP 的主营业务，假阳性往往是无法忍受的.这样我们就可以增加约束条件 $risk=0$，仅对 $cost$ 和 $benefit$ 进行优化.由于 $cost$ 的取值是有限离散的，我们可以限定不同的 $cost$ 的取值后分别最优化 $benefit$.对于在两个不同的 $cost$ 取值 $cost_1$ 和 $cost_2$ 下求得的方法 f_1 和 f_2，设它们的部署收益分别为 $benefit_1$ 和 $benefit_2$，一般来讲，如果 $cost_1<cost_2$，则有 $benefit_1<benefit_2$，那么 f_1 和 f_2 都是约束条件 $risk=0$ 下的帕累托最优方法.这些帕累托最优方法尽管未必能够最大化 ISP 的利润增量，但是可以在一些限定条件下给出最适合 ISP 的方法(比如在 ISP 不能容忍假阳性且对开销非常敏感的时候，可以采用 $risk=0$、$cost=L_1$ 时的帕累托最优方法)，因此仍然是很有意义的.

本文所提出的评价指标与评价模型，为设计不同场景下的最优方法提供了分析框架和理论依据.但如何求出最优解、并根据理论解设计出实际可行的方法，仍需要进一步的工作.

6.3　模型指导方法设计的应用实例

本节中，我们介绍利用可部署性评价模型指导方法设计的应用实例.

首先要确定方法的优化目标.在本实例中，我们的目标是约束条件 $risk=0$ 下的帕累托最优方法.根据上一节的分析，基于评价模型，我们需要在保证运维风险为 0 的前提下，针对部署开销为 L_1、L_2 和 L_3，分别以最优化部署收益为目标设计 3 个方法.

在确定了优化目标之后，下面的问题是如何通过方法的设计来实现这些目标.我们利用评价模型，对现有方法的 3 项指标进行定量评价，并对评价结果进行分析，总结出方法设计的基本规律.具体包括：基于路径的方法都存在或多或少的运维风险，而基于端(在域间场景下，“端”指自治域)和端到端的方法则可以避免运维风险；独立部署的方法部署收益较低，而采取域间协作则可以提升甚至最大化部署收益；通过按需防御则可以降低部署开销.

以此为指导，我们分别设计了 Mutual Egress Filtering(MEF)[32] 和 Inter-domain Collaboration System(ICS)这两个域间源地址验证方法.其中 ICS 包括两个模式——标签模式(ICS-tag)和消息验证码模式(ICS-mac).MEF、ICS-tag 和 ICS-mac 都采用端或端到端的验证来避免运维风险，其部署开销等级分别为 L_1、L_2 和 L_3，评价结果显示它们的部署收益在同等开销级别的方法中最高.

我们依托于国家项目的支持，实现了 ICS-tag，并将其部署在中国下一代互联网骨干网上，至今已成功运营两年多.在 ICS-tag 中，自治域两两之间协商用于生成确定性标签序列的状态机，两端的状态机同步变迁来生成标签，将其插入到报文头部，用于

① CIDR Report [EB/OL]. http://cidr-report.org/2013/12/29

端到端的验证.由于状态机的逻辑简单、标签插入和验证的开销较低,现网上的路由器只需要更新固件(更新报文的处理流程)就可以支持相应功能,而无需进行硬件升级,因此部署开销为 L_2.

在现网运行期间,尽管 ICS-tag 并未检测到大规模的伪造攻击,但却帮我们发现了一些软件缺陷和网管漏洞.比如,该系统曾在运行中报告了某自治域的部分出口报文使用了其他自治域的源地址.调查发现,原因是该自治域提供了一个开放式 IPv6 隧道服务,但却没有进行完善的前缀检查,而是将来自其他自治域的报文解封装后直接发送出去.这些报文本应使用隧道提供的源地址前缀,但由于某网络软件的缺陷,错误地使用了其他自治域的原生 IPv6 地址.软件缺陷和网管漏洞共同导致了伪造报文的出现.ICS-tag 系统捕获了这些报文,并帮助发现和修复了这些漏洞.篇幅所限,关于方法设计、分析和部署的详情请参见在线技术报告①.

7 总结与展望

源地址伪造是当前互联网的重要安全隐患和亟待解决的问题,而域间源地址验证可以通过较少的设备部署来实现有效的伪造防御.本文的特色和创新之处是首次从部署者的利益角度出发,提出将部署收益、部署开销和运维风险作为域间源地址验证方法的可部署性评价指标;从理论上证明了指标的合理性;针对这 3 项指标,我们分别建立了完整的理论评价模型;通过对现有方法的部署收益的评价,介绍了模型应用的具体流程,并通过对评价结果的深入分析提炼出具有高部署收益的方法的技术特征;讨论了方法可部署性与互联网整体安全性的关系、方法设计的优化目标以及模型指导方法设计的应用实例.

本文所提出的评价指标和模型,为域间源地址验证方法的横向比较提供了准则和方法,为方法的设计指明了方向.该指标和模型的应用,将有利于设计出更加易于部署的域间源地址验证方法,进而推进域间源地址验证的部署,最终通过改善网络的安全可信环境来促进互联网的创新和健康发展.

参 考 文 献

[1] Dobbins R, Morales C. Worldwide infrastructure security report. Arbor Networks, Chelmsford, Massachusetts, USA: Technical Report WISR/EN/0110, 2009

[2] Dobbins R, Morales C. Worldwide infrastructure security report. Arbor Networks, Chelmsford, Massachusetts, USA: Technical Report WISR/EN/0111, 2010

[3] Dobbins R, Morales C. Worldwide infrastructure security report. Arbor Networks, Chelmsford, Massachusetts, USA: Technical Report SR/WISR/EN/0212, 2011

[4] Arbor Networks. The business value of DDoS protection. Arbor Networks, Chelmsford, Massachusetts, USA: Technical Report WP/BVDDoSP/0211, 2010

[5] Beverly R, Berger A, Hyun Y, Claffy K. Understanding the efficacy of deployed internet source address validation filtering //Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC). Chicago, USA, 2009: 356-369

[6] Labovitz C. Botnets, DDoS and ground-truth//Proceedings of the 50th Conference of North American Network Operators' Group (NANOG). Atlanta, USA, 2010: 58

[7] Liu B, Bi J, Zhu Y. Deployable approach for inter-as anti-spoofing//Proceedings of the IEEE International Conference on Network Protocols (ICNP). Vancouver, Canada, 2011: 19-24

[8] Pang R, Yegneswaran V, Barford P, et al. Characteristics of internet background radiation//Proceedings of the ACM SIGCOMM Conference on Internet Measurement (IMC). Taormina, Italy, 2004: 27-40

[9] Sun C, Liu B, Shi L. Efficient and low-cost hardware defense against DNS amplification attacks//Proceedings of the IEEE Global Telecommunications Conference(GLOBECOM). New Orleans, USA, 2008: 1-5

[10] Wu J, Bi J, Li X, et al. A source address validation architecture (SAVA) testbed and deployment experience. RFC 5210, 2008

[11] Wu J, Bi J, Bagnulo M, Baker F. Source address validation improvement (SAVI) framework. RFC 7039, 2013

[12] Feng T, Bi J, Hu H, et al. InSAVO: Intra-AS IP source address validation solution with OpenRouter//Proceedings of the IEEE International Conference on Computer Communications (INFOCOM). Orlando, USA, 2012: 33-34

[13] Bi J, Liu B, Wu J, Shen Y. Preventing IP source address spoofing: A two-level, state machine based method. Tsinghua Science & Technology, 2009, 14(4): 413-422

[14] Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets//Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM). San Diego, USA, 2001: 15-26

[15] Duan Z, Yuan X, Chandrashekar J. Controlling IP spoofing through interdomain packet filters. IEEE Transactions on

① ICS. An Inter-domain Collaboration System for Defense against IP Spoofing based DDoS Attacks [EB/OL]. http://netarchlab.tsinghua.edu.cn/~junbi/THU-NetArchLab-SAV-ICS-v2-20130430.pdf

Dependable and Secure Computing (TDSC), 2008, 5(1): 22-36

[16] Bremler-Barr A, Levy H. Spoofing prevention method//Proceedings of the IEEE International Conference on Computer Communications (INFOCOM). Miami, USA, 2005: 536-547

[17] Liu X, Li A, Yang X, Wetherall D. Passport: Secure and adoptable source authentication//Proceedings of the USENIX Symposium on Networked Systems Design and Implementation (NSDI). San Francisco, USA, 2008: 365-378

[18] Lee H, Kwon M, Hasker G, Perrig A. BASE: An incrementally deployable mechanism for viable IP spoofing prevention //Proceedings of the ACM Symposium on Information, Computer and Communications Security (CCS). Alexandria, USA, 2007: 20-31

[19] Liu B, Bi J, Yang X. FaaS: Filtering IP spoofing traffic as a service//Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM). Helsinki, Finland, 2012: 113-114

[20] Mirkovic J, Kissel E. Comparative evaluation of spoofing defenses. IEEE Transactions on Dependable and Secure Computing (TDSC), 2011, 8(2): 218-232

[21] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC2827, 2000

[22] Baker F, Savola P. Ingress filtering for multihomed networks. RFC 3704, 2004

[23] Soon L, Othman M, Udzir N. IP spoofing defense: Current issues, trend and challenges. MASAUM Journal of Reviews and Surveys, 2009, 1(1): 110-115

[24] Ehrenkranz T, Li J. On the state of IP spoofing defense. ACM Transactions on Internet Technology (TOIT), 2009, 9(2): 6

[25] Wang H, Jin C, Shin K. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Transactions on Networking (ToN), 2007, 15(1): 40-53

[26] Yaar A, Perrig A, Song D. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. IEEE Journal on Selected Areas in Communications (JSAC), 2006, 24(10): 1853-1863

[27] Mankiw N G. Principles of Economics. 6th Edition. Mason, OH, USA: Cengage Learning, 2011

[28] Bracewell R. The Sign Function, In the Fourier Transform and Its Applications. 3rd Edition. New York, USA: McGraw-Hill, 1999

[29] Gao L. On inferring autonomous system relationships in the Internet. IEEE/ACM Transactions on Networking (ToN), 2001, 9(6): 733-745

[30] Li J, Mirkovic J, Wang M, et al. SAVE: Source address validity enforcement protocol//Proceedings of the IEEE International Conference on Computer Communications (INFOCOM). New York, USA, 2002: 1557-1566

[31] Ager B, Chatzis N, Feldmann A, et al. Anatomy of a large European IXP//Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM). Helsinki, Finland, 2012: 163-174

[32] Liu B, Bi J, Vasilakos A. Towards incentivizing anti-spoofing deployment. IEEE Transactions on Information Forensics and Security (TIFS), 2014, (99): 1-15

LIU Bing-Yang, born in 1985, Ph.D., postdoctoral researcher. His research interests include Internet architecture, IP source address validation, software defined networking, and Internet economics.

BI Jun, born in 1972, Ph. D., professor, Ph. D. supervisor. His research interests include Internet architecture and protocols, future Internet (SDN and NDN), Internet routing, and source address validation and traceback.

Background

With the rapid development in the last decades, the Internet has become a critical information infrastructure, which deeply impacts people's daily life and economic activity. Thus, the security of the Internet attracts more and more attention since it concerns the property safety in the real world. Recently, IP spoofing is frequently used by attackers in denial of service (DoS) attacks, which cause immense economic loss. IP spoofing makes these attacks harder to trace and prevent, and also harms the trustworthy, accountability, manageability, and measurability of the Internet. Hence, IP spoofing has become one of the most critical security threats to the Internet.

Inter-domain source address validation methods mitigate IP spoofing by identifying and filtering cross-domain spoofing packets. The academia proposes the evaluation criteria for these methods, and designs many methods according to the

criteria. However, although these methods meet the criteria, they are not sufficiently deployed by Internet service providers (ISPs). The reason is that the current criteria mainly focus on the security of the global Internet, but considers little about the ISPs' profit.

This paper proposes the first deployability evaluation criteria for inter-domain source address validation from the ISPs' perspective. The criteria include deployment benefit, deployment cost and operational risk. We theoretically prove that these criteria completely meet the ISPs' economic appeal. Thus the methods which conform to the criteria can motivate the ISPs to deploy them and hopefully eliminate the IP spoofing problem in the long run.

This paper also establishes the theoretical evaluation model, which specifies the comprehensive quantitative evaluation mechanism, for each criterion. The model is feasible in the sense that it can be practically applied to evaluating the existing methods based on publicly available Internet data.

This work is supported by the National High Technology Research and Development Program (863 Program) of China (No. 2013AA013505) and the National Natural Science Foundation of China (No. 61472213). This work is the fundamental theory of the inter-domain source address validation problem, which is one of the key problems to be studied by the projects.

Our group has been working on source address validation since 2005. The previous work includes architecture design, method design, method implementation and deployment, and comparative evaluation. Some papers have been published or accepted by SIGCOMM, INFOCOM, ICNP, IEEE Transactions on Information Forensics and Security (TIFS), IEEE Network, Computer Networks, ACM CCR and other international conferences and journals. Our group is the co-founder of IETF Source Address Validation Improvements (SAVI) WG. We published RFC 5280 (Source Address Validation Architecture Testbed) and three RFC drafts which have been approved as future RFCs.