

域间 IP 欺骗防御服务净化机制

吕高峰 孙志刚 卢锡城

(国防科学技术大学计算机学院 长沙 410073)

摘 要 IP 地址真实验证成为构建可信网络的基础,基于粗粒度的源-目的自治域标识(密钥)的域间 IP 欺骗报文过滤机制具有处理简单、保护范围广、部署激励高等优点,却存在不能过滤自治域内子网间 IP 欺骗报文等不足.而细粒度的源-目的子网标识能够解决过滤粒度粗的问题,却带来了更严重的处理复杂、计算和存储开销大等问题.针对 IP 欺骗防御机制的计算复杂度和过滤粒度之间的矛盾,提出一种新颖的域间 IP 欺骗防御服务净化机制 RISP. RISP 立足于域间 IP 欺骗防御,根据自治域内拓扑结构的稳定性,引入非对称的细粒度的源子网-目的自治域标识方式,实现对自治域间和自治域内子网间 IP 欺骗报文的检测与过滤.根据主要的 IP 欺骗报文攻击的流特征,引入流异常检测机制,实现细粒度标识的动态触发,进一步降低细粒度标识的计算和存储开销,同时对子网内恶意数据流进行流速限制. RISP 在不增加自治域内防御实体的情况下,使得防御实体能够过滤自治域内子网间 IP 欺骗报文,计算和存储开销小,过滤粒度细,而且具有较高的部署激励.

关键词 IP 欺骗防御;非对称标识;动态标记;可信网络

中图法分类号 TP393

DOI 号: 10.3724/SP.J.1016.2009.00552

Refining the Inter-Domain IP Spoofing Prevention

LU Gao-Feng SUN Zhi-Gang LU Xi-Cheng

(School of Computer Science, National University of Defense Technology, Changsha 410073)

Abstract The validation of source IP addresses becomes the key technique for devising a trustworthy network. Inter-domain IP spoofing preventions based on coarse-grained labels of source-destination ASes protect wide domains of ASes and provide high incentives of deployments, however, have the shortcoming that cann't filter spoofing packets forging other hosts' IP addresses in the same subnet. IP spoofing preventions based on fine grained labels of source-destination subnets solves the above problem, but the complexity of them is very high. Towards the contradiction between the complexity of preventions and the grain of filtering, a novel mechanism to refine the inter-domain IP spoofing prevention service, RISP, is proposed. Based on the stable of the topology of ASes, RISP introduces unsymmetrical fine-grained labels between source subnets and destination ASes, which could filter spoofing packets orienting from ASes or subnets. Based on the characteristics of the mainstream attacks employing IP spoofing, RISP combines the anomaly detection with IP spoofing preventions, which could trigger dynamic marking, reduce the cost of computing and storing of labels and limit the rates of malicious flows.

Keywords IP spoofing prevention; unsymmetrical fine-grained label; dynamic marking; trustworthy network

1 引言

目前 Internet 默认主机将自己的 IP 地址写入报文源 IP 地址域, 然而缺乏安全机制验证该假设^[1]. 攻击者有机可乘, 将伪造的 IP 地址写入报文源 IP 地址域, 从而扮演其他人或隐藏报文的起源, 构成源 IP 地址欺骗. 源 IP 地址欺骗以多种方法破坏了 Internet 安全性和可用性. 首先, 它支持反射攻击, 攻击者发送请求, 将报文源地址伪造为受害者 IP 地址, 欺骗目的端主机向受害者应答并发送数据. 其次, IP 欺骗使得防御机制复杂, 因为源 IP 欺骗报文表现为来源于多个位置, 防御机制不能使用报文源 IP 地址过滤攻击流, 因为这样会对合法主机 (如被伪造的主机) 数据流造成危害. 再次, IP 欺骗使干扰双方通信成为可能, 在加密的安全通道以下通过注入报文, 导致 TCP 连接劫持, DNS Cache 失效. 最后, IP 欺骗破坏了流量控制机制的假设, 使用公平队列在不同流之间分配资源.

IP 欺骗防御机制是网络安全研究重大挑战. 虽然有些大规模 Internet 攻击不一定使用源 IP 欺骗的方法 (如分布式拒绝服务攻击 (DDoS) 以及各种网络蠕虫), 因为这些攻击可以不用 IP 欺骗, 大量分布式攻击代理足够使受害者服务瘫痪. 然而, 忽视 IP 欺骗机制的威胁也是短视的, 因为随着 DDoS 攻击和蠕虫防御机制开始部署, IP 欺骗又将成为具有吸引力的避开已部署的防御机制的方式^[2].

已有的 IP 欺骗防御机制存在众多不足. 基于源-目的自治域标识 (密钥) 的域间 IP 欺骗过滤机制^[3-5]能够过滤自治域间 IP 欺骗报文, 计算和存储开销小, 保护范围广. 由于标识粒度粗, 不能过滤自治域内部子网间 IP 欺骗报文. 基于源-目的子网标识的 IP 欺骗报文过滤机制能够过滤子网间 IP 欺骗报文, 然而标识的数目巨大, 使得计算和存储开销无法满足^[3]. 标识的粒度决定了防御机制的过滤能力, 同时, 也影响了防御机制的复杂度.

设计高效的 IP 欺骗防御机制成为当务之急. 针对防御机制过滤能力和计算复杂度之间的矛盾, 本文提出了一种新颖的域间 IP 欺骗防御结构 RISP (Refining Inter-domain Spoofing Prevention). RISP 立足于域间 IP 欺骗防御机制, 根据自治域内网络拓扑的稳定性, 引入非对称的细粒度源子网-目的自治域标识, 实现对自治域间和自治域内子网间 IP 欺骗报文的过滤. 根据主要的 IP 欺骗报文攻击

的流特征, 引入流异常检测, 实现动态触发细粒度标识, 进一步降低了细粒度标识的计算和存储开销, 而且能够限制子网内恶意数据流的流速. RISP 在不增加域内 IP 欺骗防御实体的情况下, 使得防御实体能够过滤自治域内子网间 IP 欺骗报文, 计算和存储开销小, 过滤粒度细, 而且具有较高的部署激励. RISP 实现了 IP 欺骗报文攻击的检测与过滤机制的联合, 可以作为开放的网络攻击的检测和响应模型.

在 RISP 中, 源端防御实体根据网络拓扑组织子网级源 IP 地址空间, 目的端根据多源数据流特征检测 IP 欺骗报文攻击将会成为关键问题. 源端与目的端防御实体的协同也将是系统设计的难点.

本文第 2 节概述相关研究工作; 第 3 节提出 RISP 系统结构; 第 4 节详细描述了 RISP 的关键技术; 第 5 节通过模拟说明了 RISP 的检测能力和 IP 欺骗报文过滤能力, 并与已有防御机制进行比较; 第 6 节总结全文并指出下一步的研究.

2 相关研究

反向路径转发 RPF (Reverse Path Forwarding)^[6]是 Ingress 过滤的扩展, 使用 IP 路由表丢弃 IP 欺骗的报文. RPF 成为一个可选的主流路由器功能, 只转发具有合法源 IP 地址的报文, 能够减轻 IP 欺骗造成的危害. 如果报文的入口与用报文源 IP 地址查找路由表获得的结果一致, 那么认为该报文具有合法的源 IP 地址. 然而, RPF 有拓扑限制, RPF 只能用于对称路由环境中. 类似于 Ingress 过滤, RPF 不能向部署者提供欺骗报文过滤相关的利益.

基于路由的分布式报文过滤机制 DPF (Distributed Packet Filter)^[7]使用路由信息过滤 IP 欺骗报文, DPF 部署者根据从源到目的转发路径是否经过自己来判断 IP 欺骗报文, 如果不经, 则该报文为 IP 欺骗报文. DPF 过滤器可以部署在枢纽型 AS 中, 因此只需要部分 Internet 部署, 就可以显著过滤大部分 IP 欺骗报文. 但是 DPF 也不能向部署者提供直接的激励, 所有的部署者共享 IP 欺骗防御服务获得的利益.

RPF 和 DPF 机制可以归结为基于路由的源端过滤, 在距离攻击者最近的过滤器中过滤 IP 欺骗报文. 优点是能够提前过滤 IP 欺骗报文, 而且没有通信开销, 计算开销也很小. 共同的不足是对动态路由适应能力差, 而且自我保护能力弱, 部署激励差.

SPM^[3]首次提出基于标识的域间 IP 欺骗防御

机制. 通过专有协议在源 AS 与目的 AS 之间共享与源-目的 AS 对关联的标识和源 IP 地址空间, 并将标识通告给域内所有边界路由器, 同时周期性更新该标识. 源端 AS 边界路由器使用源-目的标识标记发出报文, 而目的端 AS 通过验证入报文标记的正确性, 识别 IP 欺骗的报文. SPM 可以识别伪造 SPM 成员 IP 地址的欺骗报文.

BCP38^[8] 允许源地址属于管理员选择的和预定义的前缀的报文进入网络, 如果在 Internet 所有的人点部署, 那么 Internet 中就不存在伪造地址的报文. SAVA (Source Address Validation Architecture) 框架^[9]进一步发展和完善了 BCP38, 克服了其部署动力差等缺陷. SAVA 划分为 3 个层次: 本地子网源地址验证、AS 内部验证和 AS 之间验证, SAVA 解决方法在不同网络规模中都是可行的.

SPM 等是典型的基于标识的目的端过滤 IP 欺骗报文的机制. 与源端过滤机制相反, 他们能够直接向部署者提供激励. 然而, 代价是防御节点之间交互的通信开销、记录标识的存储开销以及标记和验证报文的处理开销增大.

本文提出的面向子网的域间 IP 欺骗防御服务净化机制 RISP, 本着非对称标识的思想, 细化了防御机制的过滤粒度, 同时也减轻了防御机制的计算复杂度; 引入了动态标识的方式, 进一步简化了防御机制的计算负载. 与 SPM 比较, RISP 新颖的标识机制支持了子网间 IP 欺骗报文的过滤, 同时具有较小的计算和存储开销. 另一方面, RISP 继承了 SPM 良好的部署激励. RISP 实现了 IP 欺骗报文攻击的检测与过滤机制的联合, 可以作为开放的网络攻击的检测和响应平台, 为建设新一代可信网络提供了技术支撑.

3 RISP

RISP 立足于域间 IP 欺骗防御机制, 根据自治域内网络拓扑的稳定性, 引入非对称的细粒度源子网-目的自治域标识, 实现对自治域间和自治域内子网间 IP 欺骗报文的过滤. 根据主要的 IP 欺骗报文攻击的流特征, 引入流异常检测, 实现动态触发细粒度标识, 进一步降低了细粒度标识的计算和存储开销, 而且能够限制子网内恶意数据流的流速.

3.1 非对称标识

域间 IP 欺骗防御服务通常部署在运营商的边界路由器中, 而运营商将边界路由器与其他类型路

由器部署在同一电信机房, 构成网络运营商服务呈现点 (Point Of Presence, POP)^[10]. POP 是网络运营商的服务提供点, 它兼有接入网、汇聚网、核心网结点和本地网络服务等重要功能, 是互联网的重要组成部分. 当前网络运营商的 POP 网络一般设计为一组离散路由器的 mesh 结构, 如图 1 所示.

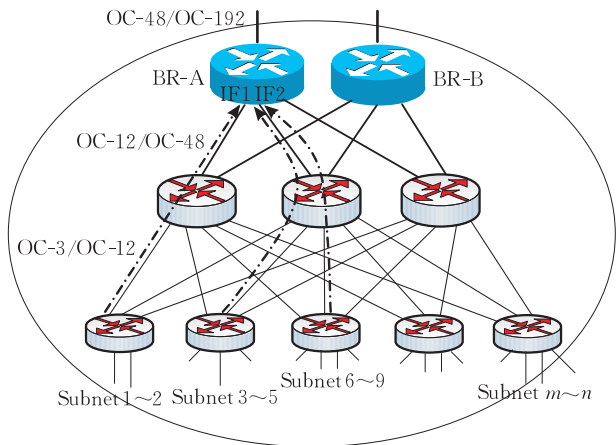


图 1 POP 结构

假设在 POP 内部骨干路由器 BR-A 实现了基于标识的域间 IP 欺骗防御机制, 目的端防御实体在源端防御实体协助下, 就可以过滤源端发送的报文中伪造其他自治域 IP 地址的欺骗报文, 同时防止源端 IP 地址被冒充. 由于标识的粒度是自治域级, 即 $Label_s \rightarrow IPS_s$, $IPS_s = IPS_{Subnet1} \cup IPS_{Subnet2} \cup \dots$, 对于源端内部攻击者伪造内部其他 IP 地址的欺骗报文是没有能力辨别的.

POP 内部节点运行域内路由器, 进行拓扑发现, 维护路由. 骨干路由器 BR-A 根据 POP 拓扑信息, 获得每个端口的源 IP 地址空间信息. 如图 1 所示, BR-A 的接口 IF1 的源 IP 地址空间信息由子网 1 (Subnet 1) 和 2 构成, 接口 IF2 的源 IP 地址空间信息由子网 3~5 以及子网 6~9 构成. BR-A 将 POP 内各个子网的源 IP 地址空间根据入口聚合, 生成若干源 IP 地址空间, 而目的端对等体仍然是自治域级防御实体, 在他们之间形成非对称的细粒度的子网-自治域标识, 即 $Label_{s1} \rightarrow IPS_{s1}$, $IPS_{s1} = IPS_{Subnet1} \cup IPS_{Subnet2}$, $Label_{s2} \rightarrow IPS_{s2}$, $IPS_{s2} = IPS_{Subnet3} \cup IPS_{Subnet5} \cup \dots$. 这种基于域内拓扑结构的标识分配方式, 粒度是端口级, 逼近子网, 也可能对应于多个子网源 IP 地址空间的并集. BR-A 对来源于同一端口的报文分别标记, 实现基于标识的 IP 欺骗报文过滤, 过滤自治域内攻击者伪造自治域内其他子网 IP 地址的欺骗报文. 分辨率和在该路由器中实现

Ingress 过滤的粒度是一样的,与其具有同样的过滤能力.

POP 内网络拓扑结构的稳定性,保证了标识和源 IP 地址空间关联的有效性. 如果 POP 拓扑发生改变,POP 内路由协议也会马上更新映射关系. 域内拓扑结构多样化,在域内路由协议帮助下,自治域级防御实体能够建立该非对称标识.

3.2 动态标识

(1) 攻击检测

SYN flooding 是一种危害性极大的拒绝服务攻击方法,利用 TCP/IP 漏洞实现对目标的攻击,是基于 TCP 协议的攻击手段中使用最频繁的一种^[11]. 在 2000 年 2 月发生的安全事件中,CNN、Yahoo 和 Amazon 在内的众多著名网络都遭受了大规模的 DDoS 攻击,SYN 泛洪是主要攻击方式.

在 SYN 泛洪攻击中,攻击者向服务器发送大量伪造 IP 源地址的 SYN 请求报文,服务器返回 SYN/ACK 应答报文后得不到确认,就不断重传,直至超时丢弃. 超时丢弃速度远远没有新接收到的 SYN 连接请求的速度快,服务器的半连接状态列表很快消耗殆尽,导致客户的正常请求得不到响应,达到拒绝服务的目的. SYN 泛洪攻击的防御比较困难,一方面,该攻击利用 TCP/IP 固有漏洞,正常网络服务都支持 SYN 报文;另一方面,攻击者不需要目标主机的返回信息,所以可以伪造 SYN 报文的源 IP 地址,这使得目标主机无法追查攻击源.

TCP 是面向连接的协议,初始化连接所使用的 3 次握手机制是 SYN 泛洪攻击的基础. 如图 2 所示,TCP 会话中 SYN 请求报文和 FIN 报文两种控制报文不是严格的一对一的对应关系(因为 SYN 报文的丢失和重传),但在网络正常运行时,两种报文有很强的关联性,而且数量差异很小. 这种微弱的差异一方面是由于网络中存在少量生存时间长的 TCP 会话,另一方面是由于 RST 报文的存在. RST

报文也能够终止 TCP 会话,而不产生任何 FIN 报文. 研究发现,在网络正常情况下,SYN 报文与 RSTactive 报文之间也有很强的相关性,SYN 报文与 FIN 报文的数量差接近 RSTactive 报文的数量(RSTpassive 报文只占有 RST 报文很少一部分)^[12-14].

$$\Delta n = \text{Number}(\text{SYN}) - \text{Number}(\text{FIN}) - \text{Number}(\text{RST}),$$

判断网络是否正在接收异常的 TCP 连接,可以作为受害者网络 SYN 泛洪攻击检测机制的基本原理.

(2) 攻击检测与报文过滤联合

SYN 泛洪攻击防御方法有两种:一种是在攻击的源端网络(发起攻击的终端网络)检测^[13-14],能及时发现该网络内部的攻击源,对攻击源进行过滤;另一种是在受害者附近进行检测^[14],并追踪到攻击源. 两种方法各有优缺点:在源端网络对分布式 SYN 泛洪攻击检测比较困难,因为攻击者分布范围非常广,数量多,攻击强度不大,所以检测机制往往无法检测到攻击流,或将正常的突发业务误判为攻击. 目的端容易检测,但是无法提前过滤攻击报文.

基于标识的域间 IP 欺骗防御机制,在源端和目的端防御实体协同下实现 IP 欺骗报文的过滤,再在目的端加入攻击检测机制,不仅具有目的端检测机制的灵敏度,而且具有源端检测的粒度,又能够很容易追踪到攻击源,使源端提前过滤攻击报文.

3.3 原理

域间 IP 欺骗防御机制在源端防御实体 p_s 和目的端防御实体 p_d 协同下实现自治域级 IP 欺骗报文过滤. 源端向目的端防御实体通告源 IP 空间信息 IPS_s 以及标识 $Label_s$,即 $p_s \rightarrow p_d : \langle IPS_s, Label_s \rangle$,并对发送给目的端自治域的报文用协商的标识 $Label_s$ 进行标记. 标识的粒度是自治域,那么源端自治域的边界路由器需要维护的标识数与目前网络中自治域的数目相当.

为了满足过滤子网级 IP 欺骗报文的要求,需要建立针对子网的细粒度标识. 如果源端防御实体为每个源-目的子网对分配标识,那么标识的数目将是巨大的. 而且防御实体部署在子网的接入路由器,那么防御实体数也是巨大的.

为了克服过滤能力和防御机制复杂度之间的矛盾,本文建立新颖的非对称标识分配机制,为源自治域子网-目的自治域对分配标识,那么每个自治域内防御实体维护的标识数目只是增长几倍. 进一步优

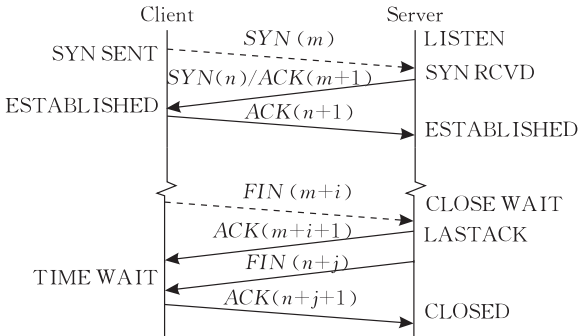


图 2 TCP 会话过程

化该设计,并不要求所有的自治域都建立子网级标识,而只是在目的端(自治域)防御实体的要求下,可疑的自治域建立子网级标识.这是一个动态行为,如果源端行为恢复正常,则不必再进行细粒度标识.

RISP 是在域间 IP 欺骗防御机制的基础上,将标识的粒度由自治域改为子网,建立了新颖的非对称的源端自治域内子网-目的端自治域对的标识,因为防御机制执行体没变,维护防御对等体(自治域)信息,而且维护自己内部拓扑信息,建立非对称的标识机制.为了进一步减少细粒度标识带来的存储和通信开销,RISP 只要求(目的端认为)可疑的源端自治域将标识粒度细化,便于目的端自治域过滤子网级 IP 欺骗报文,同时监测子网的流行为,对于异常的流进行流速限制.RISP 部署在自治域边界路由器中,由 IP 欺骗报文过滤模块、流分类器、异常检测和流速限制等功能模块组成.

(1) IP 欺骗报文过滤器.其利用源端与目的端自治域边界路由器建立的标识以及对应的源 IP 地址空间信息,即 $p_s \rightarrow p_d: \langle IPS_s, Label_s \rangle$, 检验入报文 m 的源 IP 地址是否包含在由报文中携带的标识索引的源 IP 地址空间中,即 $sIP(m) \in IPS_s$, 其中 $label(m) \rightarrow IPS_s$, 如果不是,则说明报文是 IP 地址欺骗报文,予以过滤.

(2) 报文分类器.在 RISP 中,标识分为自治域标识和子网标识,即 $Label = Label_{AS} \cup Label_{subnet}$. 由于自治域级标识标记的报文的处理策略与由子网级标识标记的报文处理策略不同,需对自治域级标识标记的报文流与子网级标识标记的报文流进行分类,分别统计相关流信息.

(3) 异常检测.报文经过 IP 欺骗报文检查,可能存在伪造自治域内其它子网 IP 地址的欺骗报文(针对自治域级标识 $label_{AS}$ 标记的报文),或伪造某子网内其它 IP 地址的欺骗报文(针对子网级标识 $label_{subnet}$ 标记的报文).对于自治域级标识标记的报文流,如果发现异常的流行为,目的端防御实体要求源端防御实体对该标识进行细化,即 $p_d \rightarrow p_s: \langle label_s, Refine \rangle$, 便于目的端更详细地监视流行为.对于子网级标识标记的流,如果发现异常的流行为,由于标识粒度限制,不能再详细区分子网内部 IP 地址,因此无法辨别是否为 IP 欺骗报文,只能进行流速限制,并要求源端过滤,即 $p_d \rightarrow p_s: \langle label_{subnet}, Filter \rangle$.

(4) 流速限制.行为异常的流,对其进行流速限制,减少其潜在的危害,出让资源给其它用户.

(5) 标识管理.域间 IP 欺骗报文过滤机制的主功能模块,与目的端协商会话标识,并通告源 IP 地址空间信息.建立出表,同时维护入表,即建立标识与源 IP 空间的映射关系, $Label_s \rightarrow IPS_s$. 在目的端的要求下,细化自治域级标识为子网级标识,同时更新相应的源 IP 地址空间信息.

RISP 是一种动态的基于细粒度标识的域间 IP 欺骗防御机制,源端根据目的端的要求动态改变标识粒度,与目的端共享子网的源 IP 地址空间,协作实现子网级 IP 欺骗报文过滤,并对源 IP 地址空间提供保护(防止被冒充).同时,目的端自治域根据子网流特性和 TCP 协议握手过程的完整性,监测源端子网流的异常,对于可疑子网流进行流速限制.动态性体现在以下几个方面:受到攻击时才进行细粒度标识;潜在的攻击源才进行细粒度标识.动态性降级了标识计算和存储开销.

3.4 目的端处理

目的端防御实体处理流程:

1. 更新源 IP 地址空间和标识.

接收其他防御实体发送的源 IP 地址空间以及对应的标识,维护入表, $Label_s \rightarrow IPS_s$.

2. 验证报文源 IP 地址.

基于报文标识判断源 IP 地址欺骗的报文 m , 过滤自治域级和子网级 IP 欺骗报文. 检验报文源 IP 地址是否包含在由报文携带的标识标记的源 IP 地址空间中,即判断 $sIP(m) \in IPS_s$ 是否成立,其中 $label(m) \rightarrow IPS_s$, 如果是,则让报文通过.

3. 提取流特征.

基于标识对报文分类,为每一类流(自治域级标识标记的报文和子网级标识标记的报文)分配流状态记录表项.分别统计流的 TCP 协议特征,即 $Number(SYN)$, $Number(FIN)$, $Number(RST)$, 记为 $s(t)$, $f(t)$ 和 $r(t)$.

4. 检测异常.

分布式 DoS 攻击中,各个源的流量都很小,如果根据单独的源流量特性,不容易检测异常.此时,即使每个源的流量很小,异常很小,但是已经超过目的端的负载,那么目的端很容易从总流量的异常变化判断是否被攻击,并从流的标识判断是哪些源发送的报文.

主要针对应用伪造源 IP 地址的 SYN 泛洪攻击,根据当前时刻统计的流状态信息以及 TCP 协议特征,判断目的端网络状态是否异常,是否受到攻击.

5. 触发动态标识.

对于自治域标识标记的报文流,若检测到异常,向报文源(由标识确定)通告细粒度标识请求,即 $p_d \rightarrow p_s: \langle label_s, Refine \rangle$.

对于子网级标识标记的报文流,若流行为恢复正常,向报文源(由标识确定)通告细粒度表示撤销,即 $p_d \rightarrow p_s: \langle label_{subnet}, Resume \rangle$.

6. 流速限制.

减小为可疑的子网级标识标记的报文流分配的网络带宽.

根据 MIT spoofer 项目^①统计结果,80%已部署的 IP 欺骗报文过来机制不能过滤子网内部 IP 欺骗报文,可以认为子网内攻击者可以伪造子网内任何 IP 地址,因此对子网级标识标记的流中发现的异常,采用流速限制的措施.

3.5 源端处理

源端防御实体处理流程:

1. 维护源 IP 地址空间.

与目的端防御实体协商源端自治域(或子网)-目的端自治域级防御实体对的会话标识 $Label_s$, 并共享源端防御实体的源 IP 地址空间信息 IPS_s , 构造出表, $Label_s \rightarrow IPS_s$. 同时,收集其它防御实体相关信息,构造入表.

2. 动态标识报文.

当网络出现异常,收到目的端防御实体发送的告警通知, $\langle label_s, Refine \rangle$, 则源端防御实体根据子网标识对进入端口的报文分别标记.

当网络状态恢复正常,收到目的端发送的正常通告, $\langle label_{subnet}, Resume \rangle$, 源端防御实体根据网络状态恢复情况,检查各个子网级源 IP 地址空间是否完全不存在异常行为.如果是,则可以恢复自治域级标识.

动态细粒度标识已经不是单纯意义上的 IP 欺骗报文过滤机制,而是一种网络攻击检测与防御机制,是域间 IP 欺骗防御机制功能的扩展,向网络攻击防御的扩展. RISP 能够统计细粒度流相关协议特征,很容易扩展到对其他利用 IP 欺骗报文的攻击.

4 关键技术

4.1 消息传递

RISP 是在源端防御实体与目的端防御实体之间传递源 IP 地址空间信息和会话标识.

消息传递方式有 BGP 带外传递和专用协议分发. RISP 选择应用专用协议^[15]传递的方式,减少了 BGP 的影响.

4.2 流 Cache

RISP 在域间 IP 欺骗防御机制中融入了数据平面的信息,增强域间 IP 欺骗防御机制的过滤能力. 数据平面的信息主要是数据流状态特征信息,引入流 Cache 存储流状态信息.

流是由报文携带的标识确定的,同时分别为自治域级标识标记的报文和子网级标识标记的报文设置流 Cache.

(1) 结构

RISP 用流 Cache 记录 TCP 流的时间戳 t , 特征值的统计量 $s(t)$, $f(t)$ 和 $r(t)$ 以及流相关的属性 c 等信息. $s(t)$, $f(t)$ 和 $r(t)$ 是在 $(t-\Delta t, t)$ 时间槽内来自某个自治域的报文流中 SYN、FIN 和 RST 报文统计.

流 Cache 使用 n 路动态组相联结构,如图 3 所示. 组中各 Cache 项是由 n 个 Hash 函数 h_1, h_2, \dots, h_n 确定,这些函数满足如下的性质,对于任意给定的变量 X , $h_1(X), h_2(X), \dots, h_n(X)$ 是独立同分布的随机变量. 这类 Hash 函数称为 n -universal Hash 函数.

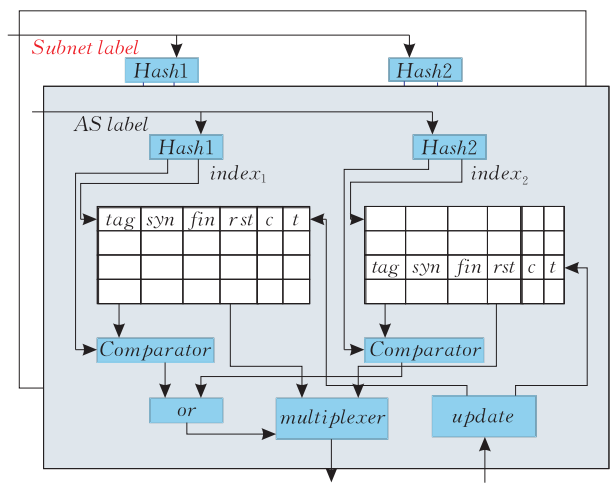


图 3 动态组相联流 Cache(2 路)

Cache 项由流的 $s(t)$, $f(t)$, $r(t)$ 以及流属性 c 和时间戳 t 等信息组成. 如果需要记录新的 Cache 项,从 $h_1(X), h_2(X), \dots, h_n(X)$ 确定的 Cache 组中选出一项. 如果这一组中有无效的 Cache 项,那么就写入该项. 否则,按照一定的策略,如选择 Cache 项的时间戳与当前时间差最大的 Cache 项,进行替换(即近似 LRU 的替换策略).

子网级 IP 欺骗报文需要特殊的处理,IP 欺骗报文过滤器根据自治域级标识过滤伪造其他自治域 IP 地址的 IP 欺骗报文,根据子网级标识过滤伪造自治域内其他子网 IP 地址的 IP 欺骗报文,现在还有子网内部的 IP 欺骗报文,即伪造子网内部 IP 地址的 IP 欺骗报文,无法根据标识过滤,只能进行流速限制. 因此 RISP 设置单独的空间保存子网级标识标记的流状态信息.

(2) Hash 函数

每个 Hash 函数可以作为一个线性变化 $B^T = HA^T$, 将具有 i 比特的二进制向量 $A = a_1 a_2 \dots a_i$ 映射

① MIT Spoofer project. <http://momo.lcs.mit.edu/spoofer>

到 k 比特的二进制向量 $\mathbf{B} = b_1 b_2 \cdots b_k$. 在流 Cache 中, 报文携带的标识对应于二进制向量 \mathbf{A} , 则 $i = 32$ (标识长度). 然后将经过 Hash 计算得到的结果作为查找流 Cache 的索引 $index_i$ 和标签 tag_i .

(3) Cache 更新

时间戳. Cache 项中的时间戳记录该流最新的报文到达时刻, 即当属于该流的报文到达时, 用当前时刻更新时间戳域. 该项表明了流的活跃程度.

流特征统计量. Cache 中的统计量记录了在 $(t - \Delta t, t)$ 时间片内到达的该流束的特定报文的总数. 当该流的相关报文到达时, 对应的特征统计量计数器加 1. 在每个时间槽结束时, 清零.

Cache 项有效性. 在初始化 Cache 时, 每个表项都是无效的. 当某个流的特征统计量存储在该表项时, 该表项置为有效.

流属性. RISP 将流分为统计源和观察源, 统一存放, 设置属性位 c 进行区分. 统计源记录是当前网络中流量最大的流, SYN 统计量最大, 能够充分反映网络流状态. 观察源记录了最新的数据流, 时间戳最大, 作为候选的统计源.

替换策略. 对两种类型的数据分别处理. 对于统计源数据按照时间戳选择替换项, 即最久未更新的流, 对当前网络状态影响减弱. 对于观察源数据按照 SYN 统计量选择替换项, 即流量最大的, 可以进入统计源. 被替换出的观察源数据加入统计源, 按照统计源替换策略选择替换项. 观察源中流量最大的进入统计源, RISP 根据统计源中流特性就可以判断当前网络状态.

4.3 多源特征融合

流 Cache 记录时刻 t 网络中来自不同源的 TCP 流的特征值, 即 $s_i(t)$ 、 $f_i(t)$ 和 $r_i(t)$. 为了满足异常检测要求, 使用 $x_i(t) = (s_i(t) - f_i(t) - r_i(t)) / s_i(t)$ 表示该流的异常程度. 正常情况下, $x_i(t)$ 的取值趋近于 0; 攻击发生时, $x_i(t)$ 的取值趋近于 1.

对 n 个 TCP 流(流 Cache 中统计源表项)的异常程度进行融合, 以平均值 μ 表示当前网络的异常程度. 为了提高计算实时性, 对 n 个统计量 $x_i(t)$ 采

用分批估计算法处理, 即对同一时刻来自不同自治域的流的异常程度进行分批处理^[16] 以求得到更高精度和实时性的结果.

设 n 个流的异常度为 x_1, x_2, \cdots, x_n , 则每个流的异常度可表示为 $x_i = \mu + \xi_i$, $i = 1, 2, \cdots, n$, ξ_i 为随机误差, 相互独立, 且 $\xi_i \sim N(0, \sigma^2)$.

将 n 个流的异常度分为 k 批, 其中第 j 批为 $x_{j1}, x_{j2}, \cdots, x_{jn_j}$, $j = 1, 2, \cdots, k$, 且 $\sum_{j=1}^k n_j = n$, $n_j \geq 2$.

第 j 批的均值和方差分别为

$$\bar{x}_j = \frac{1}{n} \sum_{i=1}^{n_j} x_{ji}, \quad j = 1, 2, \cdots, k, \quad \bar{\sigma}_j^2 = \hat{\sigma}_{x_j}^2 = \frac{\bar{s}_j^2}{n_j},$$

其中 $\bar{s}_j^2 = \frac{1}{n_j - 1} \sum_{i=1}^{n_j} (x_{ji} - \bar{x}_j)^2$.

若将 $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_k$ 作为网络异常度 μ 的 k 个观测值, 则每个 \bar{x}_j 都可以表示为

$$\bar{x}_j = \mu + \xi'_j \quad (j = 1, 2, \cdots, k),$$

其中 ξ'_j 为随机误差, 他们相互独立, 且 $\xi'_j \sim N(0, \bar{\sigma}_j^2)$.

对应于 $\bar{x}_1, \bar{x}_2, \cdots, \bar{x}_k$ 的似然函数为

$$L = \prod_{j=1}^k f(\bar{x}_j; \hat{\sigma}_j; \mu),$$

其中 $f(\bar{x}_j; \hat{\sigma}_j; \mu) = \frac{1}{\sqrt{2\pi\hat{\sigma}_j}} \exp\left[-\frac{(\bar{x}_j - \mu)^2}{2\hat{\sigma}_j^2}\right]$.

由极大似然函数估计法, 应使 $\frac{d \ln L}{d \mu} = 0$.

由此可求得当前时刻 t 网络状态的异常程度 μ 的估计值为

$$\hat{\mu} = x = \left[\sum_{j=1}^k \frac{1}{\hat{\sigma}_j^2} \bar{x}_j \right] \left[\sum_{j=1}^k \frac{1}{\hat{\sigma}_j^2} \right]^{-1}.$$

用 $u(t)$ 记录当前时刻 t 网络的异常程度 $\hat{\mu}$, 即 $u(t) = \hat{\mu}$. 异常检测单元根据时间序列 $u(t)$ 判断网络是否发生异常, 是否发生攻击.

4.4 异常检测

根据经过特征融合处理后的网络状态异常程度 $u(t)$, 应用 CUSUM 基本方法^[13-14, 17] 检测网络异常, 如图 4 所示. 在观察窗口内, 不同时刻网络异常度 $u(t)$, 构成序列 u_1, u_2, \cdots, u_n .

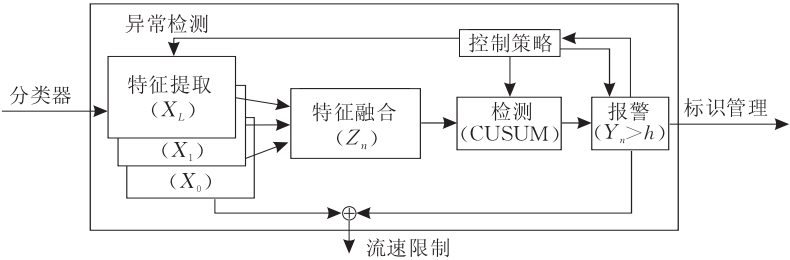


图 4 异常检测

首先,在正常情况下,采用指数加权滑动平均算法对 u_n 的均值进行估计: $\hat{u} = \beta \hat{u}_{n-1} + (1-\beta)u_n$, 其中 \hat{u}_{n-1} 为第 $n-1$ 次检测结束后对 u_n 均值的估计, β 为加权系数. 在发现异常后, 暂停对 u_n 的估计, 并以当前的估计值作为告警期间 \hat{u}_n 的参考值.

其次,在正常情况下, 对 u_n 的方差进行估计:

$$\hat{\sigma}_n = \sqrt{\frac{\sum_{i=1}^n (u_i - \hat{u}_{i-1})^2}{n-1}}.$$

在发现异常后, 暂停对 u_n 方差的估计, 并以当前的估计值作为告警期间 $\hat{\sigma}_n$ 的参考值.

为了降低网络数据流突发对攻击检测所造成的干扰, 设置了一个累积变量 y :

$$y_n = (y_{n-1} + z_n)^+,$$

其中 $z_n = u_n - \hat{u}_{n-1} - \eta \times \hat{\sigma}_{n-1}$.

如果 $y > (1+\lambda) \times \hat{u}_{n-1}$, 则发现异常.

当 DDoS 攻击发生后, 会出现大量的 SYN 报文, 即大量的 SYN 和 FIN 不对称的报文流, 因此序列 z_n 由非正数转为一个正数, 经过 CUSUM 计算, 其累积值 y_n 会快速增加, 当超过一定的阈值时, 则发现网络异常.

4.5 流速限制

对自治域级标识标记的报文流的状态信息和子网级标识标记的报文流的状态信息分别应用异常检测机制, 计算该类流的异常程度.

对于子网级标识标记的报文流, 若异常程度超过平均水平, 即 $x_i(t) > \hat{\mu}$, 根据该流的异常程度确定报文的通过率:

$$p = 1 / (1 - x_i(t) / \ln(x_i(t))).$$

对于自治域级标识标记的报文流, 若异常程度超过平均水平, 即 $x_i(t) > \hat{\mu}$, 则向源端发送细粒标识请求.

5 性能评估

5.1 衡量标准

为了量化和评估 RISP 防御效果、过滤能力和追踪能力, 引用文献[18]定义的防御性能衡量标准: $\phi_1(\tau)$ 和 $\phi_2(\tau)$, 并与 IDPF 进行比较.

定义 1. 覆盖率. 网络实体中 RISP 防御节点所占比例, 记为 γ .

定义 2. 伪造的 IP 地址集合. 攻击者 a 攻击 t 时可以伪造的 IP 地址集合 $S_{a,t}$. 利用 $S_{a,t}$ 中地址伪

造报文源 IP 地址, 该报文可以到达 t , 不会被 RISP 防御机制过滤, 根据定义知 $a \in S_{a,t}$.

定义 3. 攻击者集合. 攻击 t 时能够伪造 s 中 IP 地址的攻击者集合 $C_{s,t}$, 从这些节点中发送伪造 s 中的 IP 地址的报文, 攻击 t , 在转发过程中不会被 RISP 防御机制过滤, 根据定义知 $s \in C_{s,t}$.

$\phi_1(\tau)$ 从受害者 t 角度描述过滤能力衡量标准, 任意攻击者能够伪造至多 τ 个 AS 中的 IP 地址攻击 t 的比例, 表明抵御欺骗 DoS 攻击的能力.

$$\phi_1(\tau) = \frac{|\{t: \forall a \in V, |S_{a,t}| \leq \tau\}|}{|V|}, \tau \geq 1.$$

$\phi_2(\tau)$ 从攻击者 a 角度描述过滤能力衡量标准, 能够伪造至多 τ 个 AS 中的 IP 地址的攻击者 a 的比例, 表明 RISP 防御机制对攻击者欺骗能力的限制.

$$\phi_2(\tau) = \frac{|\{a: \forall t \in V, |S_{a,t}| \leq \tau\}|}{|V|}, \tau \geq 1.$$

5.2 参数设置

(1) 模拟器

基于 dpf2^[18] 实现了 RISP 模拟. dpf2 由 3 个模块组成: cover、dpf 和 stats. cover 根据不同的输入规则如随机选择、顶点覆盖(vertex cover)和排名顺序选择 RISP 节点. dpf 是主要模块, 计算 $S_{a,t}$ 和 $C_{s,t}$, 它的输入包括过滤类型和路由算法. stats 根据 dpf 的输出计算性能衡量标准.

从 Oregon 大学的 RouteViews^① 位于美国 ISC (isc. routeviews. org)、日本 DIXIE (wide. routeviews. org) 的 2 个无缺省路由域 DFZ(Default-Free Zone)中 BGP 路由器获得 RIB, 并构造了 Internet 拓扑结构, 分别记为 G_{USA} 和 G_{Japan} . 表 1 总结了它们的拓扑结构的属性, 列举了节点、边和 VC 的节点数. 由于 BGP 路由器位置不同, 获得的 Internet 拓扑结构 G_{USA} 和 G_{Japan} 也不完全相同. 在模拟中分别使用, 分析不同拓扑对 IP 欺骗防御机制的影响.

表 1 Internet 拓扑结构属性

Graph	# of node	# of AS path	VC size
G_{USA}	28018	9154266	3954
G_{Japan}	27024	751041	3331

网络中防御节点数和位置对 IP 欺骗防御机制的性能有一定的影响, 因此防御节点的选择也是关键. 分析随机选择防御节点, 从网络节点中随机选取

① University of Oregon Route Views Project. <http://www.routeviews.org/>

直到目标大小(如覆盖率为 30%和 50%,相应的防御节点集合记为 $Rnd30$ 和 $Rnd50$)以及根据设计规则选取(如防御节点形成顶点覆盖). VC 覆盖了 Internet 结构中所有的边,文献[18]提出了用启发式算法计算最小的 VC .

表 2 流属性

Trace	Duration Time/s	Avg. packet length/B	Number of flows	TCP ratio by bytes/%	TCP ratio by packets/%
IPLS-CHIC	7.814371	10488	631217	95.38	90.05
IPLS-KSCY	7.814371	10822	594144	88.35	84.65

表 2 中,IPLS-CHIC(Abilene III)trace 是美国 Internet2 Indianapolis (IPLS) Abilene Router Node (Abilene III)到 Kansas (CHIC)的 OC-192 链路,其采样时间约是 8s. IPLS-KSCY (Abilene III) trace 是美国 Internet2 Indianapolis (IPLS) Abilene Router Node (Abilene III)到 Kansas (KSCY)的 OC-192 链路,其采样时间约是 8s.

流 Cache 只要能够容纳时间槽内活跃流数目即可.由于 Internet 网络流量中大部分的流都是短期流,因此在小时间尺度下的固定时间槽内活跃的流数目一般较小^[19].图 5 表示活跃报文流数随测量时间尺度的变化.

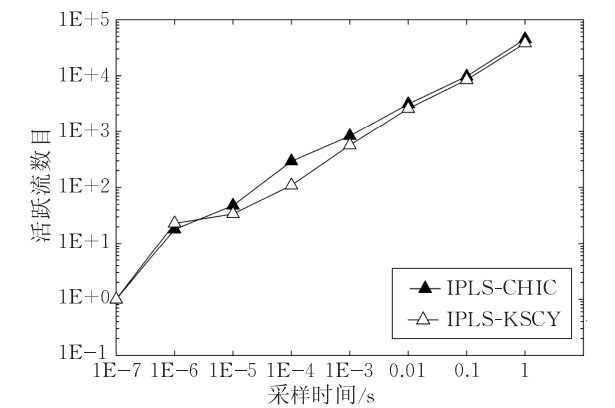


图 5 活跃流统计

选择 $\Delta t = 1\text{ms}$,可知流 Cache 需要 1024 个 Cache 表项(Cache 中每一路为 512 项).每个表项记录包含标签 tag (3B),SYN、FIN 和 RST 计数器 (6B),属性 (1B),共需要存储空间 10kB.自治域标识标记的报文与子网级标识标记的报文流状态分别存储,需 2 个流 Cache,则共需存储空间为 20kB.在每个流 Cache 中,观察源表项为 128 个,其余为统计源表项.

(3) 阈值

在检测过程中,无误报时间和检测延时是相互矛盾的.为了缩短检测延迟,需提高检测的灵敏度,

(2) 流 Cache

采用的网络流量数据是 NLANR^① 组织在 Internet 的 2 个被动测量站点中捕获的真实报文 trace 数据,如表 2 所示,分析实时的流特性,指导流 Cache 设计.

即降低阈值,但这样就会带来较多的误报,即无误报时间就会缩短.

在设置参数时,通常在这两个目标间进行折中,选取一个恰当的值.算法通过选择最佳参数 η, λ 来降低误报率和缩短检测时间.设定的 η 越大,在 z_n 中出现负值的可能性就越大,因此测试统计量 y_n 累积到一个较大值来显示攻击的可能性就越小,设 $\eta = 0.2$. λ 决定了 y_n 的报警门限, λ 越大,误报的率就越低,但检测时间会越长,设 $\lambda = 1.5$.

5.3 检测能力

(1) 特征序列

为了评测 RISP 的有效性,使用 DARPA 的离线数据集^②作为评测数据,对 RISP 进行测试.根据 DARPA 描述,选择了一个包含 SYN 泛洪攻击的数据集,该数据集使用 tcp dump 格式存储.

在检测试验中,将评测数据按照源 IP 地址空间划分为 3000 组,分别表示来自不同自治域的报文.同时配置 IP 欺骗报文过滤器,放行所有的报文.

在回放过程中只提取 TCP 握手中使用的控制报文,进行攻击检测.

(2) 检测序列

当 SYN 泛洪攻击发生以后,将会有比 FIN 多许多的 SYN 报文通过路由器,他们的对称关系被打破,网络异常程度将会迅速地增大.

在正常情况下,由于 $\eta = 0.2, z_n$ 保持负值.在攻击下,异常程度增大, z_n 出现正值,如图 6 所示,4 个时刻 A, B, C, D 均出现了网络异常.

(3) 攻击检测

在正常情况下,CUSUM 计算结果 y_n 都保持 0 值.当由于网络其他原因造成网络异常, z_n 变成正值时,其 CUSUM 的值 y_n 变化不大,而且会迅速地恢

① Passive Measurement and Analysis (PMA). <http://pma.nlanr.net>
② MIT Lincoln Laboratory. DARPA intrusion detection evaluation data set. <http://www.ll.mit.edu/IST/ideval/>, 1999

复为 0, 修正由网络错误所造成的误报, 如图 7 所示 A, B, C 时刻. 对于网络中正在进行的 SYN 泛洪攻击, CUSUM 结果 y_n 会变得很大, 如图 7 所示的 D 时刻. 因此, 一旦发生攻击后, CUSUM 检测方法可以迅速发现正在进行的 DDoS 攻击.

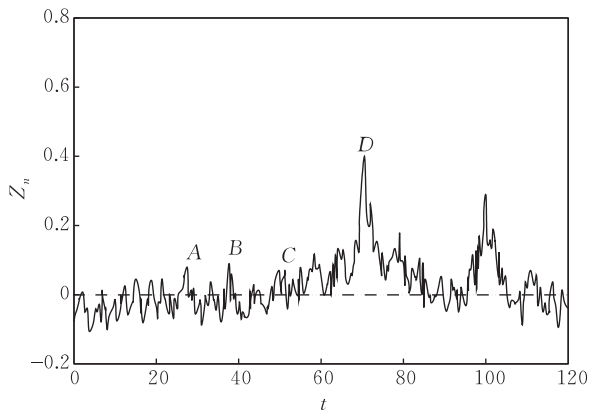


图 6 流特征检测序列

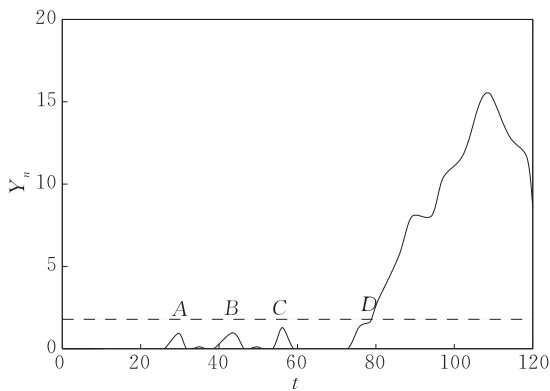


图 7 攻击检测

目前, 检测 DDos 攻击的方法, 有基于统计分析的方法和基于规则检测的方法. 对于小规模网络检测比较有效, 对于大流量背景下的检测, 尤其是在攻击流量被背景流量淹没的情况下, 这些算法有其固有的局限性, 即依赖于攻击流量是否达到一定规模. RISP 是基于细粒度标识的异常检测方法, 统计微观的自治域级流特征, 融合为宏观的网络状态异常程度, 进行判断, 灵敏度更高、更准确. 而且 RISP 能比较方便地实现不同的流协议特征的提取和处理, 实现针对多种类型的攻击的检测.

5.4 过滤能力

从受害者角度分析 RISP 过滤能力. $\phi_1(\tau)$ 表示了可能受到攻击的节点 τ 的比例, 此时攻击者能够伪造最多 τ 个节点的 IP 地址, 其中 $\phi_1(1)$ 表示攻击者只能伪造最多 1 个 AS 的 IP 地址攻击 t , 说明了 t 对欺骗攻击的免疫能力. 图 8 表示了在了 G_{USA} 中 3 种

覆盖 $Rnd30$ 、 $Rnd50$ 和 VC 下 IDPF 和 RISP 过滤能力. IDPF 不能够完全防止 IDPF 节点受到欺骗攻击, $\phi_1(1) < \gamma$, 除非网络中所有的节点支持 IDPF. 而且 IDPF 节点放置对于 IDPF 的性能有严重的影响, 在 VC 下的性能超越了 $Rnd30$ 和 $Rnd50$. 而 RISP 节点通过标识能够过滤联盟成员发送的 IP 欺骗报文或非联盟成员伪造联盟成员 IP 地址的 IP 欺骗报文, $\phi_1(1) > \gamma$.

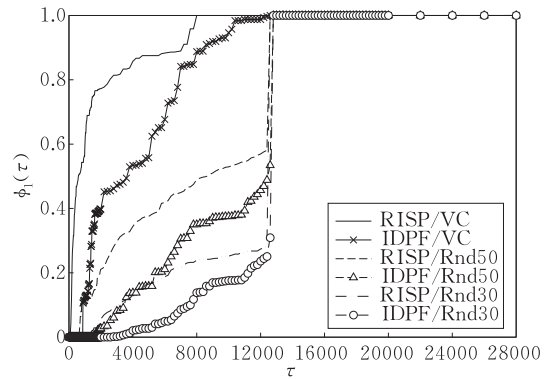


图 8 过滤能力 $\phi_1(\tau)$ 的比较

从攻击者角度分析 RISP 过滤能力. $\phi_2(\tau)$ 表示了防御机制限制攻击者欺骗能力的效果, 其中 $\phi_2(1)$ 描述了只能使用自己 IP 地址不能伪造其他 AS 的 IP 地址发起欺骗攻击的攻击者 a 的比例. 图 9 表示了在了 G_{Japan} 中 3 种覆盖 $Rnd30$ 、 $Rnd50$ 和 VC 下 IDPF 和 RISP 的 $\phi_2(\tau)$ 值. IDPF 不能完全防止网络受到欺骗攻击, 则突出了对攻击者能力的限制. IDPF 在 $Rnd30$ 、 $Rnd50$ 和 VC 覆盖下, $\phi_2(1)$ 分别是 0.292、0.487 和 0.805. RISP 机制在相同配置下, $\phi_2(1)$ 分别是 0.312、0.498 和 0.821.

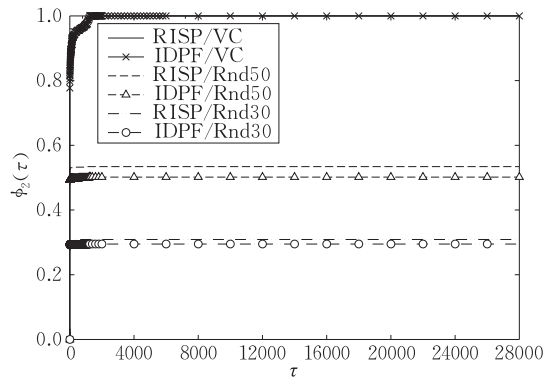


图 9 过滤能力 $\phi_2(\tau)$ 的比较

6 总结和展望

RISP 立足域间 IP 欺骗防御, 根据自治域内网

络拓扑的稳定性,引入非对称的细粒度源子网-目的自治域标识,实现对自治域间和自治域内子网间 IP 欺骗报文的过滤.根据主要的 IP 欺骗报文攻击的流特征,引入流异常检测,实现动态触发细粒度标识,降低了细粒度标识的计算和存储开销,而且能够限制子网内恶意数据流的流速. RISP 在不增加域内 IP 欺骗防御实体的情况下,使得防御实体能够过滤自治域内子网间 IP 欺骗报文,计算和存储开销小,过滤粒度细,而且具有较高的部署激励.

RISP 继承了基于标识的防御机制的可部分部署性,能够很好地支持动态路由和非对称路由.应用 Routeview 提供的 RIB 进行评估, RISP 增强了 IP 欺骗防御节点的能力,是一种高效的域间 IP 欺骗防御机制,为建设新一代可信网络提供技术支撑.

未来会有更多的研究集中于如何将自治域级和端系统级 IP 欺骗防御机制融合的方法.同时 IP 欺骗防御逐渐受到 IETF 的关注.我们相信 RISP 能够推动 IP 欺骗防御机制的标准化,这也是我们进一步研究的方向.

参 考 文 献

- [1] Hastings N E, McLean P A. TCP/IP spoofing fundamentals//Proceedings of the 15th Annual International Phoenix Conference on Computers and Communications. 1996: 218-224
- [2] Schuba C L, Krsul I V, Kuhn M G. Analysis of a denial of service attack on TCP//Proceedings of the IEEE Symposium on Security and Privacy. 1997: 208-223
- [3] Bremner-Barr, Levy H. Spoofing prevention method//Proceedings of the IEEE INFOCOM 2005. Miami, USA, 2005: 2809-2814
- [4] Liu X, Yang X W, Wetherall D. Passport: Secure and adoptable source authentication//Proceedings of the 5th USENIX NSDI. San Diego, CA, 2008
- [5] Lee Heejo, Kwon M, Hasker G, Perrig A. BASE: An incrementally deployable mechanism for viable IP spoofing prevention//Proceedings of the ASIACCS 2007. Singapore, 2007: 20-31
- [6] Baker F. Requirements for IP version 4 routers. Internet Engineering Task Force. RFC 1812, June 1995
- [7] Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets//Proceedings of the ACM SIGCOMM 2001. California, USA, San Diego: ACM Press, 2001: 15-26
- [8] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, 2000
- [9] Paul Ferguson, Wu Jianping, Bi Jun, Li Xing, Ren Gang, Williams M I. Source address verification architecture problem statement. Internet Draft, draft-sava-problem-statement-01.txt, June 2007
- [10] Guan Jian-Bo, Su Jin-Shu. The aggregation switching of heterogeneous routers for single POP application. Journal of National University of Defense Technology, 2005, 27(5): 12-17(in Chinese)
(管剑波, 苏金树. 面向 SPR 的异构路由器聚合交换技术. 国防科技大学学报, 2005, 27(5): 12-17)
- [11] Zhu Wen-Tao, Li Jin-Sheng, Hong Pei-Lin. A router agent based distributed flooding detection system. Chinese Journal of Computers, 2003, 26(11): 1585-1590(in Chinese)
(朱文涛, 李津生, 洪佩琳. 基于路由器代理的分布式湮没检测系统. 计算机学报, 2003, 26(11): 1585-1590)
- [12] Gong Jian, Peng Yan-Bing, Yang Wang, Liu Wei-Jiang. Macroscopical quantitative balance of TCP packets. Chinese Journal of Computers, 2006, 29(9): 1562-1571(in Chinese)
(龚俭, 彭艳兵, 杨望, 刘卫江. TCP 流的宏观平衡性. 计算机学报, 2006, 29(9): 1562-1571)
- [13] Chen Wei, He Yan-Xiang, Peng Wen-Ling. A light weight detection method against DDoS attack. Chinese Journal of Computers, 2006, 29(8): 1392-1400(in Chinese)
(陈伟, 何炎祥, 彭文灵. 一种轻量级拒绝服务攻击检测方法. 计算机学报, 2006, 29(8): 1392-1400)
- [14] Wang H N, Zhang D L, Kang G S. Detecting SYN flooding attacks. IEEE Computer and Communication Society, 2002, 3(6): 1530-1539
- [15] Lv Gao-Feng, Sun Zhi-Gang. Towards spoofing prevention based on hierarchical coordination model//Proceedings of the IEEE Workshop on High Performance Switching and Routing. New York, USA, 2007: 1-6
- [16] Liao Xi-Chun, Qiu Min, Mai Han-Rong. The study on data fusion algorithms of multi-sensor based on parameter estimation. Chinese Journal of Sensors and Actuators, 2007, 20(1): 193-197(in Chinese)
(廖惜春, 丘敏, 麦汉荣. 基于参数估计的多传感器数据融合算法研究. 传感技术学报, 2007, 20(1): 193-197)
- [17] Sun Zhi-Xin, Tang Yi-Wei, Cheng Yuan. Router anomaly traffic detection based on modified-CUSUM algorithms. Journal of Software, 2005, 16(12): 2117-2123(in Chinese)
(孙知信, 唐益慰, 程媛. 基于改进 CUSUM 算法的路由器异常流量检测. 软件学报, 2005, 16(12): 2117-2123)
- [18] Duan Z H, Yuan X, Chandrashekar J. Constructing Inter-domain packet filters to control IP spoofing based on BGP updates//Proceedings of the IEEE INFOCOM 2006. Barcelona, SPAIN, 2006: 13-25
- [19] Stevens W. TCP slow start, congestion avoidance, fast retransmit, and fast recovery algorithms. IETF RFC 2001, January 1997



LU Gao-Feng, born in 1980, Ph.D., assistant researcher. His current research interests include high performance routing and switching, trustworthy network.

SUN Zhi-Gang, born in 1973, Ph. D., associate professor. His current research interests include high performance router and next generation network architecture.

LU Xi-Cheng, born in 1946, professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His current research interests include parallel and distributed computing and computer network.

Background

DDoS defenses are thwarted by IP spoofing, and by IP spoofing attackers can evade detection and put a substantial burden on destination networks for filtering attack packets. IP spoofing prevention becomes a kind of important network security facility, which detects attacks based on spoofing packets and filters malicious traffic. Although many IP spoofing prevention techniques have been proposed, none of them is widely used in the Internet. IP spoofing prevention mechanisms proposed could not prevent all of network equipments from being attacked and could not filter spoofing packets before their flooding on middle networks. IP spoofing prevention mechanisms are not efficient, and have high cost and low incentive of deployment, which restricts ISPs to deploy IP spoofing prevention mechanisms and causes a serious flaw of Internet.

The contradiction between the allocation of IP addresses and the use, such as multihoming and hijacking, increases the complexity of getting the state of domains, and the conflict among management policies of domains enhances the difficulty of cooperating with other domains. End-hosts are vulnerable to spoofing attacks and the cooperating attack employing IP spoofing has a serious influence on Internet, so designing an efficient IP spoofing prevention mechanism turns out to be an important approach to building a trustworthy network.

The work of this paper is supported by the National

Grand Fundamental Research (973) Program of China (2009CB320503 and 2005CB321801). The research team of this paper has developed some creativity and published many technique papers in journals and proceedings. As a part of the source IP addresses validation, this paper presents a novel approach to refine the IP spoofing prevention service for filtering spoofing packets orienting from the subnets with little overhead of computing and communicating. Based on the stable of the topology of ASes, RISP introduces unsymmetrical fine-grained labels between source subnets and destination ASes, which could filter spoofing packets orienting from ASes or subnets. Based on the characteristics of the mainstream attacks employing IP spoofing, RISP combines the anomaly detection with IP spoofing preventions, which could trigger dynamic marking, reduce the cost of computing and storing of labels and limit the rate of malicious flows. RISP acts as an open platform for detecting and response of attacks, which would support the building of the next generation trustworthy network. Ahead of the work, the authors the mechanism to extend the IP spoofing prevention servercie towards non-members of alliance of spoofing preventions and the mechanism to enhance the the ability of spoofing preventions towards members of alliance of spoofing preventions, which are efficient and scalable mechanisms of inter-domain spoofing preventions.