软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(8):2130−2137 [doi: 10.3724/SP.J.1001.2012.04134]

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

基于域间路由的分布式分组过滤有效性研究*

王立军+

(清华大学 信息网络工程研究中心,北京 100084)

Research on the Effectiveness of Distributed Packet Filtering Based on Inter-Domain Routing

WANG Li-Jun+

(Network Research Center, Tsinghua University, Beijing 100084, China)

+ Corresponding author: E-mail: wanglijun@cernet.edu.cn

Wang LJ. Research on the effectiveness of distributed packet filtering based on inter-domain routing. *Journal of Software*, 2012,23(8):2130−2137 (in Chinese). http://www.jos.org.cn/1000-9825/4134.htm

Abstract: Filtering the spoofed packets with a false source addresses is the inherent requirement of the trustworthy and secure Internet. Routing based distributed packet filtering is effective, but its effectiveness has no solid theory analysis. In this paper, based on the inter-domain route distribution and the hierarchy of the Internet topology, the study establishes the route distribution tree model and ideal AS graph model using these two models analyze the effectiveness of maximum filtering and semi-maximum filtering. The analysis results verify the former experimental results and figure out the theoretical explanation. Maximum filtering can filter out most spoofed packets. Though it cannot reach 100%, maximum filtering can limit the number of the successful spoofing AS to the average AS path length of the Internet. On the ideal AS graph, semi-maximum filtering has the same effectiveness as the maximum filtering and its storage and computing overhead is much lower than maximum filtering, which provides the theoretical basis to use it in practice. The model-based analysis points out the inherent features of the inter-domain routing based distributed packet filtering, which conduces to design the subsidiary mechanism and the overall deployment in the whole Internet.

Key words: inter-domain routing; spoofed packet; distributed packet filtering

摘 要: 消除伪造源地址分组是互联网安全可信的内在要求.基于路由的分布式分组过滤具有良好的效果,但是目前对其有效性缺乏严密的理论分析.基于域间路由传播和互联网拓扑的分层特征,建立路由传播数模型和理想AS 图模型,以此为工具分析了基于域间路由的最大过滤和半最大过滤有效性.结论印证并从理论上解释了前人研究中的实验结果.最大过滤能够消除绝大多数的伪造分组,虽然无法达到 100%,但可以将伪造成功的自治系统数量限制为互联网AS路径的平均长度.在理想AS图上,半最大过滤与最大过滤的有效性相同,但是存储和计算开销要小很多,为实际中部署半最大过滤提供了理论依据.理论模型分析揭示了基于域间路由的分布式分组过滤的内在优缺点,有助于设计辅助措施和在整个互联网全面而合理地部署.

关键词: 域间路由;伪造分组;分布式分组过滤

中图法分类号: TP393 **文献标识码**: A

收稿时间: 2011-04-14; 定稿时间: 2011-11-02

传统互联网提供尽力而为的传输服务,路由器根据分组目的地址在转发表中查找对应的转发端口.分组接收方通过分组的源地址判断发送方.从发送方到接收方的传递路径上,没有对分组源地址的检查机制,发送方可以任意指定分组的源地址,以达到伪造和冒充的目的.使用虚假信息的分组被称为伪造分组,携带虚假源地址是伪造分组的最主要类型,以下伪造分组专指携带虚假源地址的分组.接收方不能辨别来自网络的分组是否来自真实的发送方,导致互联网提供的转发服务不可信;多种网络攻击利用伪造源地址的方法,隐藏攻击源头的真实身份以逃避惩罚,成为互联网的安全隐患.随着越来越多安全敏感的应用被部署到互联网上,互联网必须提供更可信的网络服务,以满足其作为国家信息基础设施的要求.增加验证分组源地址真实性的机制,是新一代互联网必须给予解决的关键问题.

基于路由的分布式分组过滤(distributed packet filtering,简称 DPF)[1]被认为是解决伪造分组问题的有效方法.其基本思想是:在互联网自治系统连接拓扑上,路由的传播和选择会形成源头自治系统到目的自治系统的特定的分组转发路径,即分组从源头自治系统到目的自治系统的转发约束,路由器据此约束信息辨别分组源地址的真实性,将伪造分组在转发路径上过滤掉.文献[1]中的实验结果表明,20%的自治系统部署 DPF 能够过滤掉80%的伪造分组.对于分布式分组过滤的有效性研究,目前主要采用在实验性网络拓扑上的模拟实验方法,不能对实验结果做出原理上的分析和解释.本文通过抽象的方法建立了描述互联网域间路由的路由传播树模型和反映互联网层拓扑层次结构的理想 AS 图模型,基于这两个模型分析了域间伪造分组的两种过滤方法(最大过滤和半最大过滤)的有效性,初步揭示了该方法的内在特征,并解释了模拟实验的研究结果.

1 相关研究背景

1.1 互联网路由

路由是互联网的核心功能,负责提供网络可达性信息和计算最优路由,使路由器将分组向目的网络转发.互联网由超过 35 000 个自治系统(autonomous system,简称 AS)组成.每个 AS 由自治系统号码(autonomous system number,简称 ASN)标识.互联网路由分为两个层次:域内路由和域间路由,分别负责在 AS 内部和 AS 之间传递和计算路由信息.常见的域内路由协议有 OSPF,RIP,IS-IS 等,主要基于量度计算最短路由.边界网关协议 BGP[2]是域间路由协议的事实标准.

BGP 路由封装在 Update 消息中传递,包括路由声明和路由取消两种类型.边界路由器发现一条新路由后,通过路由声明将这条路由传播给邻居,其中包括目的网络的 IP 地址前缀和一系列描述路由特征的路由属性.如果边界路由器发现到达某个目的网络的路由不再可用,就向邻居发送路由取消,取消前面发送的到达该目的网络的路由.当边界路由器的路由发生改变时,就向邻居发送新路由的路由声明,同时默认取消前面的发送路由.

BGP 是基于策略的路由,路由策略反映了 AS 间的商业关系和流量选择.主要有两种关系类型[3]:Provider-Customer 和 Peer-Peer.在 Provider-Customer 连接关系中,Provider 为 Customer 提供接入互联网的服务,Provider 将来自其 Provider,Customer,Peer 和自身的路由传递给 Customer,Customer 将来自其 Customer 和自身的路由传递给 Provider;在 Peer-Peer 连接关系中,Peer 将来自其 Customer 和自身的路由传递给对方.基于这两种连接关系形成了互联网 AS 连接的层次结构[4].层次结构的最顶层是大致 20 个国际级的 ISP,通常称作 Tier-1 AS,这些 AS 间几乎形成了 Peer-Peer 关系的全连接.第 2 层次的 Tier-2 AS 是 Tier-1 AS 的 Customer,一般是国家级的 ISP.出于经济和性能方面的原因,Tier-2 AS 会与地理位置相近的其他 Tier-2 间建立 Peer-Peer 关系交换流量.Tier-2 下面的 Tier-3 AS 一般是地区级 ISP.不提供穿越服务的 AS 被称为 Stub AS,通过各级 ISP 接入互联网.

1.2 伪造分组

消除伪造源地址分组的方法主要可分为反应式和预防式两类.反应式方法以 IP 追踪技术[5,6]为代表,在接收方收到伪造分组后采取措施,以减小损害和定位真实发送方.预防式方法主要通过在网络设备部署过滤机制,根据一定的规则检查分组中的某些字段,以判断分组是否来自真实的发送方,在到达目的主机之前发现和消除伪造分组.IP 追踪技术并不能消除伪造分组,而且会给路由器带来很大开销.基于路由的 DPF 被提出之后,多篇文

献设计了为 DPF 提供过滤标准的机制.

SAVE[7]是为支持DPF而设计的新协议,路由器为每个端口维护与之对应的源地址表,表示从该端口进入的分组的真实源地址空间范围.路由器向转发表中的每个目的网络发送含有本地网络地址的 SAVE 更新消息,该消息经过的每个路由器把 SAVE 消息中的网络地址记录在进入端口的源地址表中,由此形成伪造分组的过滤规则.当路由器收到一个分组时,检查分组源地址是否属于进入端口对应的源地址表中的某个网络地址.如果不属于,则判断该分组为伪造分组.SAVE 没有考虑路由系统的层次结构,是一种在域内域间所有路由器间使用的协议.相对不稳定的域内路由会使 SAVE 频繁产生更新消息,增大通信开销,同时降低 SAVE 源地址表的准确程度.另外,新协议也难以在互联网网络设备中逐步部署.

IDPF[8]是应用于域间的伪造分组过滤方案.边界路由器根据来自邻居 AS 的 BGP 消息构建伪造分组过滤规则.根据域间路由策略形成的路由输出约束,可以确定从邻居 AS 到本 AS 可能的上游 AS 集合,以此作为边界路由器对应接口的分组源地址验证规则.但是,由于 IDPF 不是根据发送方到接收方的唯一转发路由验证分组源地址真实性,也就是分组源地址有效范围被扩大,因此,尽管 IDPF 具有简单和开销小的优点,但是降低了识别和过滤伪造分组的效果.IDPF 的有效性评价采用了文献[1]中的软件、拓扑和方法,在有效性研究方法方面没有提高.

路由选择通知[9]通过扩展 BGP 为边界路由器提供 DPF 所需的路由选择信息.基本设计思想是:AS 选择一条路由后,给发送这条路由的邻居 AS 回送一个路由选择通知(selection notification,简称 SN)消息,通知该路由被选择,而且在消息中附带本 AS 的地址空间,这也就是真实源地址应属于的地址范围;如果收到的 SN 消息所响应的路由不是源自本 AS,就将该 SN 消息继续传递给路由的发送方.边界路由器根据 SN 中的地址信息生成域间分组过滤所需的源地址验证规则.路由选择通知的特点是提供完整的路由选择信息,域间伪造分组的过滤规则更加准确,采用 BGP 可选穿越属性传递 SN 消息,支持在互联网中逐步部署.

清华大学提交的 IETF 标准草案和 RFC[10]中设计了 IPv6 源地址认证体系结构 SAVA[11],并在 IETF 成立了专门的研究小组 SAVI.按照互联网的层次结构,SAVA 被设计为本地子网、域内和域间这 3 个层次,分别负责端系统 IP 地址、IP 地址前缀和自治系统粒度的源地址验证.SAVA 包括两种生成域间源地址验证规则的方案:基于端到端轻量级签名和基于路径信息的域间真实地址寻址方案,分别应用在非直接互联和直接互联两种情况.SAVA 首次提出了真实源地址寻址的网络体系结构,但是并没有对其域间方案单独使用和联合使用的有效性做出理论分析.

2 基于域间路由的 DPF

本节给出基于域间路由 DPF 的严格定义和表述[1],作为建立抽象模型和理论分析的基础.将互联网抽象为无向图 $G(V,E)$,其中,V 是节点集合,每个节点表示一个 AS;E 是有向边集合,$e=\langle u,v\rangle$表示节点 v 与 u 之间存在连接关系,方向表示 v 将分组转发给 u.$\{R(d,s)|d\in V,s\in V\}$是图 G 上所有节点的路由集合,$R(d,s)$表示从节点 s 到节点 d 的路由;在不产生歧义的情况下,$R(d,s)$也表示从 s 到 d 的路径.源地址为 s、目的地址为 d 的分组 $P(d,s)$将沿着 $R(d,s)$上的边转发.$F_e:V^2\to\{0,1\}$是定义在 $e=\langle u,v\rangle$上表示分组过滤的函数,节点 u 收到来自边 e 的分组 $P(d,s)$,$F_e(d,s)=1$ 表示丢弃分组,$F_e(d,s)=0$ 表示转发分组.路由器对分组地址信息的检查分为两种:基于源和目的地址联合检查的最大过滤和只基于源地址检查的半最大过滤.

定义 1(最大过滤). 对于来自边 $e=\langle u,v\rangle$的分组 $P(d,s)$,如果存在路由 $R(d,s)$满足 $e\in R(d,s)$,那么节点 u 转发该分组;否则,节点 u 判断该分组使用虚假源地址而将其过滤掉.边 e 上的这种过滤方式称为最大过滤,表示为

$$\tilde{F}_e=\begin{cases}0, & e\in R(d,s)\\ 1, & e\notin R(d,s)\end{cases}.$$

定义 2(半最大过滤). 对于来自边 $e=\langle u,v\rangle$的分组 $P(d,s)$,如果存在路径 $R(t,s)$,$t\in V$ 满足 $e\in R(t,s)$,那么节点 u 转发该分组;否则,节点 u 判断该分组使用虚假源地址而将其过滤掉.边 e 上的这种过滤方式称为半最大过滤,表示为

$$\hat{F}_e=\begin{cases}0, & \exists t\in V, e\in R(t,s)\\ 1, & \text{otherwise}\end{cases}.$$

3 DPF 过滤规则

路由选择通知[9]提供的域间路由选择信息能够生成 $\tilde{F}_e$ 和 $\hat{F}_e$ 所需的验证规则.节点 u 是 V 中任一节点,其边集表示为 $E_u=\{e_u^1,e_u^2,...,e_u^k\}$. u 从 e_u^i 获得的域间路由选择信息记为 $\Omega_{e_u^i}$, u 的全部域间路由选择信息为 $\Omega_u=\bigcup_{i=1}^{k}\Omega_{e_u^i}$.对于 SN 消息 $\omega\in\Omega_{e_u^i}$, s_ω表示发源ω的节点,R_ω表示ω确认的路由,d_ω表示发源路由 R_ω的节点.u 在 e_u^i 上可构造由节点对组成的过滤规则 $\tilde{C}_{e_u^i}=\bigcup_{\omega\in\Omega_{e_u^i}}\{\langle d_\omega,s_\omega\rangle\}$.

如果 u 从 e_u^i 收到分组 $P(d,s)$,则 $\langle d,s\rangle\in\tilde{C}_{e_u^i}$ 满足.$\langle d,s\rangle\in\tilde{C}_{e_u^i}$ 表示存在 SN 消息 $\omega\in\Omega_{e_u^i}$,即 s 收到若干条到达节点 d 的路由后,选择了经过边 e_u^i 的路由,这样ω才会经过 e_u^i,即 $e_u^i\in R(d,s)$. 因此,$P(d,s)$经过 e_u^i 符合域间路由选择形成的约束,可以判断其源地址 s 是真实的.

如果 u 从 e_u^i 收到分组 $P(d,s)$,则 $\langle d,s\rangle\notin\tilde{C}_{e_u^i}$ 满足.根据路由选择通知原理:选择新路由向发送该路由的节点回送 SN 消息;收到 SN 消息后判断其响应的路由不是源自本节点,则向发送被响应路由的邻居节点转发该 SN 消息.节点 s 选择经 e_u^i 到达 d 的路由后,发送的 SN 消息ω一定会经过 e_u^i 传递给 u,总有 $\omega\in\Omega_{e_u^i}.\langle d,s\rangle\notin\tilde{C}_{e_u^i}$ 与 $\omega\in\Omega_{e_u^i}$ 相矛盾.于是,$P(d,s)$经过 e_u^i 不符合域间路由选择形成的约束,可以判断其源地址 s 是伪造的.

根据 $\tilde{C}_{e_u^i}$ 构造 $\hat{C}_{e_u^i}=\{s\mid\langle d,s\rangle\in\tilde{C}_{e_u^i},d\in V,s\in V\}$, 节点 u 可依据 $\hat{C}_{e_u^i}$ 实现 $\hat{F}_e$:u 从 e_u^i 收到分组 $P(d,s)$:若 $s\in\hat{C}_{e_u^i}$,则表示存在 $\langle t,s\rangle\in\tilde{C}_{e_u^i}$,此即 $e_u^i\in R(t,s)$,可以判断分组源地址真实并转发;否则,判断 $P(d,s)$为伪造分组并丢弃.

定理 1. 最坏情况下,节点 $u\in V$ 上 $\tilde{F}_e$ 的过滤规则数量是 $\hat{F}_e$ 的 N 倍,即 $|\tilde{C}_{e_u^i}|=N\cdot|\hat{C}_{e_u^i}|$, N 是 u 的路由数量.

证明:假设节点 u 共得到 N 条路由 $r_1,r_2,\ldots,r_N$.S_k 表示这样的节点集合,其中的节点选择了 r_k,发送的 SN 消息经过边 e_u^i 到达节点 u,则有 $|\tilde{C}_{e_u^i}|=\sum_{k=1}^{N}|S_k|$,$|\hat{C}_{e_u^i}|=\left|\bigcup_{k=1}^{N}S_k\right|$,最坏情况下,$|\tilde{C}_{e_u^i}|=N\cdot|\hat{C}_{e_u^i}|$.定理得证. □

存储开销和操作复杂度与验证规则数量成正比,最坏情况下,$\tilde{F}_e$ 也是 $\hat{F}_e$ 的 N 倍,因此实际中应尽量采用 $\hat{F}_e$.

4 最大过滤 $\tilde{F}_e$ 的有效性分析

定义 3(路由传播树). 节点 d 的网络可达性信息在 AS 拓扑上以 BGP 路由 R_d 传播,R_d 被 V 中节点发送和选择的过程,形成以节点 d 为根的有向树 T_d,定义 T_d 为路由传播树.$e=\langle m_1,m_2\rangle$是 T_d 上的有向边,表示节点 m_2 选择了来自邻居 m_1 的 R_d 作为到达 d 的转发路由.

AS1 和 AS7 的路由传播树如图 1 所示.T_d 的信息分布于 V 中所有节点,每个节点具有 T_d 的部分信息.节点 u 使用标准 BGP 协议获得 u 到 d 的路由,即 T_d 上从根节点 d 到 u 的树枝,分组 $P(d,u)$在 T_d 从 u 到 d 的树枝上沿着与边相反的方向转发.如果节点 u 支持 $\tilde{F}_e$,节点 u 除了获得转发分组所需的路由以外,还需要获得路由选择信息 Ω_u.由于目的地址固定为 d,Ω_u 简化为 $T_{d,u}-\{u\}$,其中,$T_{d,u}$ 是 T_d 上以 u 为根的子树.

$T_{d,u}-\{u\}$可被划分为 $\{T_{d,m_1},T_{d,m_2},...,T_{d,m_k}\}$,其中,$m_i$ 是与边 e_u^i 对应的 u 的子节点;$T_{d,m_i},i=1,...,k$ 是与 e_u^i 对应的子树,即在路由选择树模型中 $\tilde{C}_{e_u^i}=T_{d,m_i},i=1,...,k$.

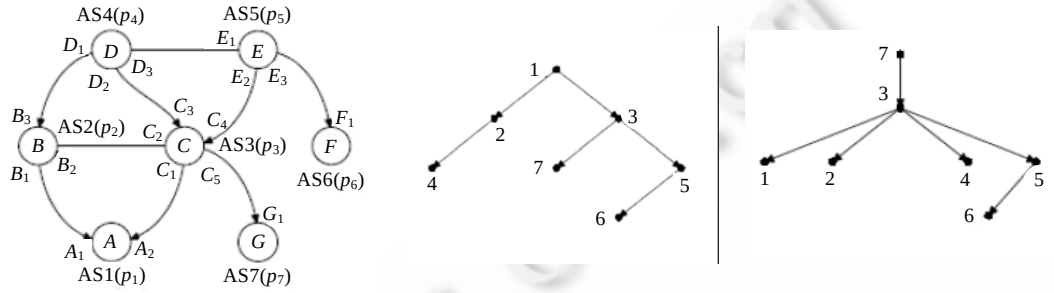
路由传播树简化了基于路由的 DPF 问题,$\tilde{F}_e$ 的过程为:节点 u 收到来自边 $e_u^i=\langle u,m_i\rangle$ 的分组 $P(d,s)$,首先根据目的地址 d 确定路由传播树 T_d.如果 $s\notin T_{d,m_i}$,那么判断 $P(d,s)$为伪造分组而将其过滤掉;如果 $P(d,s)$源自节点 $s'\neq s$,伪造的源地址 $s\in T_{d,m_i}$,那么节点 u 将不能判断出 $P(d,s)$是伪造分组,从而将其漏过.

定理 2. 如果 T_d 上存在长度大于等于 3 的树枝,那么 $\tilde{F}_e$ 不可能过滤掉所有伪造分组.

证明:以 V_F 表示图 G 上执行 $\tilde{F}_e$ 的节点集合,源自 s'的伪造分组 $P(d,s)$被 T_d 上节点的 $\tilde{F}_e$ 漏过有两种情况:

- 情况 1:从 s'到 d 的树枝上没有节点执行 $\tilde{F}_e$,s'发出的伪造分组 $P(d,s)$可被顺利地转发到 d.
- 情况 2:假设 u 是从 s'到 d 的树枝上执行 $\tilde{F}_e$ 的第 1 个节点,并有 $s'\in T_{d,m_i}$,所有 s'发出的伪造分组 $P(d,s)$,$s\in T_{d,m_i}$ 都不会被节点 u 的 $\tilde{F}_e$ 过滤掉.

情况 1 可以通过增大 V_F 来解决,使得从任意 s'到 d 间,至少有 1 个节点执行 $\tilde{F}_e$.情况 2 若要避免,则必须满足 $|T_{d,m_i}|=1$,否则,$s'\in T_{d,m_i}$ 可以成功地伪造任意 $s\in T_{d,m_i}, s\neq s'$ 的地址.$|T_{d,m_i}|=1$等价于 T_d 上树枝的最大长度为 3.定理得证. □



(a) 简单网络拓扑,AS1~AS7 是自治系统,A~G 为边界路由器 (b) 以 AS1 为根的路由传播树 T_1 (c) 以 AS7 为根的路由传播树 T_7

Fig.1 Route distribution tree model

图 1 路由传播树模型

图 2 可以给出比较直观的解释,实线连接表示该边执行 $\tilde{F}_e$,虚线连接表示只作分组转发,不执行 $\tilde{F}_e$.情况 1 如图 2(a)所示,增大 V_F,例如节点 u 部署 $\tilde{F}_e$,这样即转化为情况 2.情况 2 如图 2(b)所示,在树枝 $u\rightarrow m_i\rightarrow s'$上,节点 u 对来自$\langle u,m_i\rangle$的分组执行 $\tilde{F}_e$.若 $T_{d,m_i}=\{m_i,s',s\}$,则 s'发出的伪造分组 $P(d,m_i),P(d,s), s\in T_{d,m_i}$,不能被过滤掉;若 $T_{d,m_i}=\{m_i,s'\}$,则 s'发出的伪造分组 $P(d,m_i)$不能被过滤掉.

(a) 伪造分组 $P(d,s)$没有经过部署 $\tilde{F}_e$ 的节点 (b) $\tilde{F}_e$ 不能判断出伪造分组 $P(d,s)$

Fig.2 A case of packet $P(d,s)$ with forged source address not filtered by $\tilde{F}_e$

图 2 伪造源地址的分组 $P(d,s)$不能被 $\tilde{F}_e$ 过滤掉的情况

定理 2 表明,基于域间路由的 DPF 存在内在缺陷:如果一个节点伪造 T_d 上孩子的源地址发送分组给 d,则伪造分组将会成功到达目的节点 d.例如,在图 1(b)上,如果 V_F={2,3,5},则从任意节点到目的节点 1,中间都至少有 1 个节点执行 $\tilde{F}_e$.如果节点 5 向节点 1 发送源地址为 6 的伪造分组 $P(1,6)$,$\tilde{F}_e$ 会将其漏掉.基于域间路由的 DPF 本身无法弥补这个缺陷,只能采用其他辅助措施.

定理 3. 在 $\tilde{F}_e$ 充分部署情况下,成功伪造任意节点 $s\in V$ 作为源地址的节点集合记为 W_s,则有 $|\overline{W_s}|=A-1$,其

中,A 为互联网 AS 路径的平均长度.

证明:记 T_d 上从 s 到 d 树枝上的中间节点为 $u_1,u_2,\ldots,u_k$,如果节点 $u_1,u_2,\ldots,u_k$ 和 d 都支持 $\tilde{F}_e$,则根据 $\tilde{F}_e$ 的过滤规则,任意节点 $n\in V,u\neq s,u\neq u_i,i=1,\ldots,k$ 伪造的 $P(d,s)$都会被过滤掉.根据定理 1,只有 $u_1,u_2,\ldots,u_n$ 伪造 $P(d,s)$不会被过滤掉,即成功发送伪造分组 $P(d,s)$的 AS 数目为 $k.d$ 是任意选取的,所以有 $|\overline{W_s}|=A-1$. □

定理 2 表明,$\tilde{F}_e$ 能够大大降低 AS 的地址被其他 AS 伪造的可能,但不能消除所有伪造源地址分组,必须配以辅助措施补足这种方法的内在缺陷.这为后续工作有针对性地设计辅助措施和配合方案,以及研究分组过滤在网络中的部署方案提供依据.文献[1]的实验结果中,在 $\tilde{F}_e$ 充分部署覆盖集合节点的情况下,基于路由的 DPF 将伪造分组的真实源 AS 限定在数量很小的范围,而定理 3 对此给出了原理解释.

5 理想 AS 图模型

以 $Z=\{t_1,t_2,t_3\}$表示邻居 AS 间的关系类型.把经济关系考虑进来后,描述 AS 拓扑的图 $G(V,E)$被扩展为带有注释边的图 $G(V,E,f)$,其中,f 是定义在所有边上的函数:

$$f(\langle u,v\rangle)=\begin{cases}t_1, & u\text{是}v\text{的Provider}\\ t_2, & u\text{是}v\text{的Customer}\\ t_3, & u\text{是}v\text{的Peer}\end{cases}.$$

定义 4(理想 AS 图). 理想 AS 图 $G(V,E,f)$是考虑 AS 间关系类型的图,V 是表示 AS 的节点集合;E 是表示 BGP 连接的边集;f 是边集 E 上的注释,表示节点间表现为路由策略的关系类型,并且具有如下要求:

1) 存在节点集合 $Tier^1=\{c_1^1,c_2^1,\ldots,c_k^1\}\subseteq V$, 对任意 $c_i^1,c_j^1\in Tier^1,i\neq j,\langle c_i^1,c_j^1\rangle\in E$ 和 $f(\langle c_i^1,c_j^1\rangle)=t_3$ 同时满足.
2) 对于任意节点 $x\in V$,最多存在 1 个节点 $y\in V$,满足 $f(\langle y,x\rangle)=t_1$.
3) 对任意边$\langle x,y\rangle\in E$,如果 $x\notin Tier^1$ 或者 $y\notin Tier^1$,那么 $f(\langle x,y\rangle)\neq t_3$.
4) 对任意边$\langle x,y\rangle\in E$:
   a) 如果 $x\in Tier^1,y\notin Tier^1$,并且 $f(\langle x,y\rangle)=t_1$,那么可以得到节点集合:
   $$Tier^2=\{y|f(\langle x,y\rangle)=t_1,x\in Tier^1,y\notin Tier^1\}.$$
   b) 如果 $x\in Tier^i,y\notin Tier^{i-1}\cup Tier^i,i=2,3,\ldots$,并且 $f(\langle x,y\rangle)=t_1$,那么可以得到节点集合:
   $$Tier^{i+1}=\{y|f(\langle x,y\rangle)=t_1,x\in Tier^i,y\notin Tier^{i-1}\cup Tier^i\}.$$

在上述定义中,第 1 条要求理想 AS 图模型中的点集存在一个子集 $Tier^1$,其中的任意两个节点之间都建立 Peer-Peer 类型的关系.也就是说,该子集中的点建立 Peer-Peer 关系的全连接,对应着互联网拓扑中顶层 ISP.第 2 条要求每个节点如果有 Provider,那么最多只有 1 个,排除了理想 AS 图上存在多宿主的情况.第 3)条要求 $Tier^1$ 以外的节点间不存在 Peer-Peer 关系.第 4 条指出理想 AS 图的层次结构,存在节点集合 $Tier^i,i=2,3,\ldots$,所以理想 AS 图理想化的互联网拓扑可以看作是将多棵树的树根两两相连得到:树根之间建立 Peer-Peer 关系的全连接,形成互联网的核心;根节点没有 Provider,非根节点只有 1 个 Provider;在同一棵树上只有 Provider-Customer 关系,并且与树根节点较近的节点是 Provider.

定理 4. 理想 AS 图上任意两个节点之间只有 1 条无环路由.

证明:将理想 AS 图看作是多棵树的根节点两两建立 Peer-Peer 关系而形成的,对于任意节点 $x,y\in V$:

1) 如果 x 和 y 都在以 $c\in Tier^1$ 为根的同一棵树上,则根据图论可知,x 与 y 之间只有 1 条无环路由.
2) 如果 x 和 y 分别在以 $u\in Tier^1,v\in Tier^1$ 为根的树上,$Tier^1$ 节点间只有 Peer-Peer 关系,则根据 Peer-Peer 关系节点间传播路由的规则,节点 u 只能从节点 v 得到 y 的可达性信息.根据情形 1)可知,y 到 v 和 u 到 x 之间都只有 1 条路由,于是 x 与 y 之间只有 1 条无环路由. □

定理 5. $\hat{F}_e$ 和 $\tilde{F}_e$ 在理想 AS 图上过滤伪造分组的有效性相同.

证明:假设节点 $u\in V$ 基于域间路由选择信息生成分组过滤规则,执行基于域间路由的 DPF,其边集记为 $\{e_u^1,e_u^2,\ldots,e_u^k\}$,与边 e_u^i 对应的邻居记为 $m_i,i=1,2,\ldots,k.d_l\in V,l=1,2$ 是任意两个目的节点,到达 $d_l,l=1,2$ 的路由表示为

R_{d_l}.假设 u 选择的到达 d_l 的最优路由从边 e_n^l 收到,那么在 d_l 的路由传播树 T_{d_l} 上,T_{d_l,m_l} 必为空集,否则会形成路由环路.

若 $e_u^1 \neq e_u^2$,即 u 选择作为转发路由的 R_{d_1} 和 R_{d_2} 来自不同的邻居.如前文所述,路由传播树上 $\tilde{F}_e$ 的验证规则 $\tilde{C}_{e_u^i}=T_{d,m_i}$,所以 u 在路由传播树 T_{d_1} 上的验证规则是 $\{\Phi,T_{d_1,m2},...,T_{d_1,m_k}\}$,在 T_{d_2} 上的验证规则是 $\{T_{d_2,m_1},\Phi,...,T_{d_2,m_k}\}$.如果 $T_{d_1,m_i}\neq T_{d_2,m_i}$,$i$=3,4,…,$k$,即存在 x 满足 $x\in T_{d_1,m_i}, x\notin T_{d_2,m_i}$,那么假设 $x\in T_{d_2,m_j}$,$j\neq i$,x 到 d_1 和 d_2 的路径分别为 $x,\ldots,m_i,u,\ldots,d_1$ 和 $x,\ldots,m_j,u,\ldots,d_2$,而 $m_i\neq m_j$.也就是说,从 n 到 x 在理想 AS 图上有两条不同路由,这与定理 4 不符,因此必有 $T_{d_1,m_i}=T_{d_2,m_i}$,i=3,…,k.

若 $e_n^1=e_n^2$,则节点 u 在 T_{d_l},l=1,2 上的子树集合为 $\{\Phi,T_{d_l,m2},...,T_{d_l,m_k}\}$.与以上证明相同,$T_{d_1,m_i}=T_{d_2,m_i}$,$i$=2,3,…,$k$ 总是满足.

e_u^i 是 u 的任意边,对于所有的目标节点 d_j,j=1,…,n,若 u 从边 e_u^i 收到 R_{d_i},那么不存在分组 $P(d_i,s)$从 m_i 转发向 u.由此,若 u 从 e_u^i 收到的分组 $P(d_i,s)$,其路由 R_{d_i} 都来自 e_u^i 以外的边,那么如前所述,这些 T_{d_i,m_i} 都相同,所以 e_u^i 上 $\hat{F}_e$ 与 $\tilde{F}_e$ 过滤效果相同.节点 u 是理想 AS 图上的任意节点,由此定理得证. □

定理 5 解释了文献[1]的实验结果中 $\hat{F}_e$ 与 $\tilde{F}_e$ 过滤效果几乎相同的原因:实验采用 1997 年的互联网拓扑连接稀疏;更重要的是,从路由表很难发现 Peer-Peer 关系,从而存在大量被漏掉的 Peer-Peer 连接,拓扑生成算法得到的互联网拓非常扑近似于理想 AS 图.前文已经指出,$\tilde{F}_e$ 的存储开销和过滤操作复杂度远远大于 $\hat{F}_e$,这为在实际部署中应尽量使用 $\hat{F}_e$ 提供了依据.

6 结束语

本文通过建立理论模型的方法分析了基于域间路由的 DPF 的有效性.基于路由传播树模型的分析揭示,分布式分组过滤本身存在固有缺陷,即使在充分部署 DPF 的情况下,单独采用这种方法也不能在域间消除所有的伪造源地址分组,必须设计辅助措施.这也说明很有必要在整个互联网设计包括多个层次的真实源地址寻址方案,例如 SAVA 体系结构.基于路由的 DPF 能够过滤大部分伪造分组,因此可以作为此体系结构中的重要组成部分.为了降低过滤给边界路由器带来的开销,实际中应主要采用半最大过滤.本文基于理想 AS 图模型的分析揭示,在理想 AS 图上,最大过滤与半最大过滤的有效性相同.二者有效性的差别决定于互联网实际拓扑与理想 AS 图的差别,这为部署半最大过滤提供了理论依据.随着互联网的发展,更多的自治系统采用 Peer-Peer 和多宿主连接方式.互联网连接拓扑特性的变化对基于域间路由的 DPF 的有效性都会产生重要影响,对其影响的评价及相关的解决办法将是进一步的研究方向.

References:

[1] Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. In: Proc. of the ACM SIGCOMM. San Diego, 2001. 15−26. [doi: 10.1145/964723.383061]

[2] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC 4271, 2006.

[3] Huston G. Interconnection, peering and settlements—Part I. Internet Protocol Journal, 1999,2(1):2−16.

[4] Subramanian L, Agarwal S, Rexford J, Kartz RH. Characterizing the Internet hierarchy from multiple vantage points. In: Proc. of the 21st INFOCOM. New York, 2002. 618−627.

[5] Savage S, Wetherall D, Karlin A, Anderson T. Network support for IP traceback. IEEE/ACM Trans. on Networking, 2001,9(3): 226−237. [doi: 10.1109/90.929847]

[6] Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F, Schwartz B, Kent ST, Strayer WT. Single-Packet IP traceback. IEEE/ACM Trans. on Networking, 2002,10(6):721−734. [doi: 10.1109/TNET.2002.804827]

[7] Li J, Mirkovic J, Wang M, Reiher P, Zhang L. SAVE: Source address validity enforcement protocol. In: Proc. of the 21st INFOCOM. New York, 2002. 1557−1566.

[8] Duan Z, Yuan X, Chandrashekar J. Constructing inter-domain packet filters to control IP spoofing based on BGP updates. In: Proc. of the 25th INFOCOM. Barcelona, 2006.

[9] Wang L, Xu K, Wu J. BGP route selection notice. In: Proc. of the Int'l Conf. on Information Network (ICOIN). LNCS 3961, 2006. 440−449. [doi: 10.1007/11919568_44]

[10] Wu J, Bi J, Li X, Ren G, Xu K. A source address validation architecture (SAVA) testbed and deployment experience. IETF, RFC5210, 2008.

[11] Wu J, Ren G, Li X. Source address validation: Architecture and protocol design. In: Proc. of the IEEE ICNP. 2007. [doi: 10.1109/ICNP.2007.4375858]

王立军(1978－),男,河北唐山人,博士,助理研究员,主要研究领域为互联网域间路由,医疗卫生信息化.

2012 CCF 中国计算机大会

征 文 通 知

第 9 届 CCF 中国计算机大会(2012 CCF China National Computer Congress, CCF CNCC2012)将于 2012 年 10 月 18 日–20 日在大连世博广场举行,承办单位为大连大学.CCF CNCC 是由中国计算机学会 2003 年创建的系列性学术会议,已在不同的城市成功举办 8 届,现每年一次.

CCF CNCC 旨在探讨计算机及相关领域最新进展和宏观发展趋势,展示中国学术界、企业界最重要的学术、技术事件和成果,使不同领域的专业人士能够获得探讨的机会并获得所需信息.CCF CNCC2012 将有约 2 000 人到会,有逾 100 项成果进行展览展示,是中国计算机界的又一次盛会.

CCF CNCC2012 现公开征集会议论文,征文范围涵盖计算机领域各专业.本次大会拟不出版论文集,有不超过 50 篇的优秀论文将刊登在《计算机学报》上,其他所有大会入选论文也将发表在 CCF 会刊《小型微型计算机系统》和《计算机应用与软件》上.

投稿方式

此次将采取网上投稿方式,请作者将稿件通过以下地址提交:http://conf.ccf.org.cn/

如果是 CCF 会员,请在投稿时注明“CCF 会员”.

重要日期

录用通知发出日期: 2012 年 8 月 1 日