软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2014,25(3):642−661 [doi: 10.13328/j.cnki.jos.004407]

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

防范路由劫持的协同监测方法*

王小强, 朱培栋, 卢锡城

(国防科学技术大学 计算机学院,湖南 长沙 410073)

通讯作者: 王小强, E-mail: network.xq@gmail.com

摘 要: 路由劫持是当前 Internet 域间路由系统(BGP)所面临的最严重的安全威胁之一,但目前仍缺乏有效的防护手段.将自治系统(autonomous system,简称 AS)基于 BGP 路由信息自我发现路由劫持的概率定义为对路由劫持的免疫能力,对该免疫能力进行了建模,并给出了 AS 自我免疫的充分条件和必要条件以及该免疫能力的上界.实验结果发现, 80%以上的 AS 对路由劫持完全没有免疫能力,仅不超过 0.26%的 AS 具有大于 85%的免疫能力.对 AS 免疫过程的进一步分析,揭示了造成 AS 免疫能力低下的提供商栅栏现象——提供商优先选择客户路由,从而阻止了劫持路由向被劫持者的传播.为了克服提供商栅栏,提高 AS 的免疫能力,设计了协同监测机制,并提出了一种计算复杂度较低的启发式协同邻居选取策略.该机制无需修改 BGP 协议,可增量部署.实验结果表明,仅与 25 个自治系统进行协同,就可以将对路由劫持的免疫能力提高到高于 95%的水平.

关键词: 域间路由;路由劫持;提供商栅栏;协同;监测

中图法分类号: TP393 **文献标识码**: A

中文引用格式: 王小强,朱培栋,卢锡城.防范路由劫持的协同监测方法.软件学报,2014,25(3):642−661. http://www.jos.org.cn/1000-9825/4407.htm

英文引用格式: Wang XQ, Zhu PD, Lu XC. Securing prefixes against BGP hijacking in a cooperative way. Ruan Jian Xue Bao/ Journal of Software, 2014,25(3):642−661 (in Chinese). http://www.jos.org.cn/1000-9825/4407.htm

Securing Prefixes Against BGP Hijacking in a Cooperative Way

WANG Xiao-Qiang, ZHU Pei-Dong, LU Xi-Cheng

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

Corresponding author: WANG Xiao-Qiang, E-mail: network.xq@gmail.com

Abstract: BGP hijacking is one of the most severe threats facing current inter-domain routing system, but yet there still lack effective countermeasures. This paper models AS (autonomous system) level immunity to BGP hijacking as the possibility of the victim AS learning bogus routes via local BGP routing information, and presents the sufficient condition and necessary condition for an AS to be immune in the presence of BGP hijacking, as well as the upper bound of such immunity. Evaluation results show that more than 80% of ASes have no immunity to BGP hijacking at all and only less than 0.26% of ASes have immunity higher than 85%. Further analysis pinpoints the root cause of such low immunity—provider barrier that victim AS' providers prefer customer routes and prevent the propagation of bogus route to the victim. To tackle this barrier and improve AS level immunity against BGP hijacking, this study designs a cooperation based monitoring mechanism, and proposes a lightweight heuristic approach for each participant to select AS cooperators. This proposed mechanism is completely compatible to BGP, and is incrementally deployable. Experimental results show that by peering with only 25 cautiously selected ASes, one AS can significantly improve its immunity to 95%.

Key words: BGP; route hijack; provider barrier; cooperation; monitoring

* 基金项目: 国家自然科学基金(61170285, 61100223); 国家重点基础研究发展计划(973)(2011CB302600)
收稿时间: 2011-11-04; 定稿时间: 2013-02-06; jos 在线出版时间: 2013-11-28
CNKI 网络优先出版: 2013-11-28 15:15, http://www.cnki.net/kcms/detail/11.2560.TP.20131128.1515.004.html

基于边界网关协议(border gateway protocol,简称 BGP)[1]的域间路由系统是互联网的核心基础设施,路由劫持是 BGP 路由系统当前所面临的最严重的安全威胁之一.当路由劫持发生时,以被劫持网络为目的地的网络流量有可能会被路由到发起路由劫持的攻击者,因此,路由劫持可被用作攻击手段实现多种目的,例如:丢弃所吸附的网络流量,制造路由黑洞,阻断被劫持网络提供的服务;使用属于被劫持网络的 IP 地址发送垃圾邮件,隐藏垃圾邮件的真实来源[2];模拟被劫持网络提供的服务,实现网络钓鱼;将吸附的流量发回到被劫持网络,实现隐蔽的“中间人攻击”[3].在互联网发展的历程中,路由劫持事件时有发生,并严重干扰了互联网的正常运行,影响较大的有 1997 年的 AS7007 事件[4]、2008 年巴基斯坦电信管理局劫持 YouTube[5]等.在这些事件中,被劫持网络提供的服务都被中断两个小时以上,造成了重大的社会影响和经济损失.

业界在防范路由劫持方面做出了大量努力,但迄今仍然缺乏有效的防护手段.造成这种状况的原因包括:

(1) BGP 安全模型的脆弱性.BGP 假设接收到的路由信息是可信和可靠的,使 BGP 对于针对路由内容的攻击特别是路由劫持非常脆弱[6].鉴于当前域间路由系统的巨大规模,更换或升级 BGP 都非常困难,因此,BGP 安全模型上的脆弱性将长期存在;

(2) ISP(Internet service provider,网络运营商)之间缺乏有效的信息共享和协同.每个 ISP 独立地运行自己的网络,客户信息、路由策略均被视为商业秘密,而对路由劫持的防范需要 ISP 之间进行有效的协同.以路由劫持中的前缀劫持为例,其体现为前缀和宣告者自治系统(autonomous system,简称 AS)对应关系的变化.由于当前并不存在一个权威的机构或数据源能够准确地跟踪、提供这种对应关系,仅前缀的拥有者本身(受害者 AS)能够判明这种变化是否合理.但如本文第 2 节所述,这种变化传播到受害者 AS 的概率很低.

本文的贡献包括:

(1) 对 AS 基于 BGP 路由信息自我发现路由劫持的概率(免疫能力)进行建模,给出了 AS 自我免疫的充分条件、必要条件和该免疫能力的上界.实验结果表明,超过 80%以上的 AS 对路由劫持完全没有免疫能力,仅有不超过 0.26%的 AS 的免疫力高于 85%;

(2) 揭示了导致 AS 对路由劫持免疫能力低下的提供商栅栏现象——提供商优选从客户 AS 学到的路由,在路由劫持发生时阻碍了劫持路由向受害者 AS 的传播;

(3) 为了克服提供商栅栏,提高 AS 对路由劫持的免疫能力,设计了协同监测机制.参与协同的每个 AS 从协同邻居学习相关于本 AS 所属网络的路由用于监测,不干扰路由系统的正常功能;向每个协同邻居只输出相关于该邻居的路由,所暴露的路由信息分布在不同邻居之间,保护了参与者 AS 的隐私;由参与者 AS 检测针对于所属网络的路由劫持,回避了第三方难以区分正常路由变化和路由劫持的难题;

(4) 提出了一种启发式协同邻居选取策略,以较低的算法复杂度实现了较高的安全能力.实验结果表明,仅与 25 个自治系统进行协同,就可将对路由劫持的免疫能力提高到高于 95%的水平.

本文第 1 节介绍 BGP 和路由劫持的相关背景.第 2 节对 AS 基于 BGP 路由信息感知路由劫持的能力进行建模,给出 AS 自我免疫的充分条件和必要条件,对该免疫能力的上界进行评估,并揭示导致 AS 对路由劫持免疫力低下的提供商栅栏现象.第 3 节介绍防范路由劫持的协同监测方法和协同邻居选取策略.第 4 节对协同监测方法的部署效果进行评估.最后,第 5 节介绍相关工作并展望未来的研究方向.

1 BGP 和路由劫持

为了增强可扩展性,互联网采用了层次式的路由体系结构,在自治系统(autonomous system,简称 AS)粒度上分为域内和域间两个层次.自治系统定义为运行在统一策略之下,向外展示出一致的路由策略的一组路由设备[1].AS 内部使用域内路由协议,如 OSPF,IS-IS 和 RIP;AS 之间使用域间路由协议.BGP 是当前域间路由协议事实上的标准,其作用是在 AS 之间交换网络可达性信息.

1.1 互联网AS级路由

为了实现全网范围内的连通性,每个 AS 都必须借助邻居 AS 转发去往/来自非邻居 AS 的数据流量.AS 之间存在 4 种商业关系:提供商-客户关系(provider-customer,简称 p2c),客户-提供商关系(customer-provider,简称

c2p),对等体关系(peer-peer,简称 p2p)和同胞关系(sibling-sibling,简称 s2s).在 p2c 和 c2p 关系中,客户 AS 向提供商 AS 付费购买数据转发服务;建立 p2p 关系的两个 AS 通常具有相当的规模,彼此免费为对方转发数据流量;建立 s2s 关系的双方一般同属于一个机构,不涉及费用结算,通常互为访问外部网络的备份连接.这 4 种关系中,p2c(c2p)关系最为普遍,p2p 次之,s2s 最为少见.以 CAIDA[7]推断的 AS 间商业关系数据为例(基于 2010 年 1 月 20 日的路由表),各种商业关系的数量及比重分为 69191(92.3%),5591(7.4%)和 219(0.3%).鉴于 s2s 关系的比例很小,且和 p2p 关系相似,在很多研究中都被作为 p2p 连接处理[8],本文采取了相同的处理方式.在 Internet 的 AS 级拓扑中,c2p 连接可以看作是一条从客户到提供商的有向边,记为→.类似地,用←表示一条 p2c 连接,用↔表示 p2p 连接.本文中主要用到的符号及其定义见表 1.

Table 1 Symbol definition

表 1 符号定义

符号	描述
p2c, c2p, p2p	AS 间的 3 种商业关系,分别是提供商-客户,客户-提供商,对等体-对等体
$r=(d,v_{k-1}\ldots v_1v_0)$	BGP 路由 r 的简化表示,其中,d 是网络前缀,$v_{k-1}\ldots v_1v_0$ 是 r 的 AS_PATH(AS 路径)属性
r.origin, *r.nexthop*	路由 r 的源 AS(v_0)和下一跳 AS(r 的 AS_PATH 属性从右至左第一个不同于 v_0 的 AS)
$G=\langle V,E,R\rangle$	互联网 AS 级拓扑的图表示,V 是 AS 集合,E 是 AS 之间边的集合,R 是 E 到集合{p2c,c2p,p2p}的映射
$V_{(i)}$	AS i 的影响范围,定义为 V 中选择了 i 发起的路由作为最优路由的 AS 集合
Prov(u), *Cust*(u), *Peer*(u)	AS u 的提供商,客户和对等体的集合
ψ_u	AS u 的提供商闭包,定义为 AS u 仅通过上坡路径(如图 1 所示)就能到达的 AS 的集合
ζ_u	AS u 的客户闭包,定义为 AS u 仅通过下坡路径(如图 1 所示)就能到达的 AS 的集合
$\Im_u$	AS u 对路由劫持的免疫能力
N_v	与 AS v 建立了协同监测会话的 n 个监测邻居 $N_v=\{M_1,M_2,\ldots,M_n\}$
s_v^u	AS v 与 AS u 建立协同监测会话时,u 提供给 v 的安全范围.$\forall a\in s_v^u$,有 $u\in V_{(a)}$,故 v 能从 u 学到攻击路由
S_v	AS v 的安全范围,S_v 是 s_v^u 的并集($u\in N_v$)

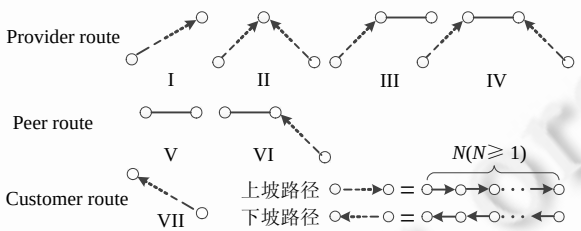

Fig.1 Valley-Free paths learned via neighbors

图 1 “无谷底”限制下从不同类型的邻居可以学到的路由形态

定义 1(客户路由(customer route)、对等体路由(peer route)和提供商路由(provider route)). 一个 AS 从客户、对等体和提供商学到的路由分别称为客户路由、对等体路由和提供商路由.

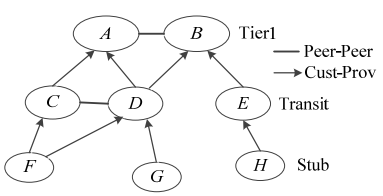

Fig.2 Internet AS level hierarchy structure

图 2 互联网 AS 级的层次结构示意

Internet 的 AS 级拓扑呈现出明显的层次特性.根据在层次结构中所处位置,AS 被分为核心层 AS(*Tier*1 或 *Tier*1 AS),传输层 AS(transit)和边缘层 AS(stub).*Tier*1 AS 之间通过直接的对等连接(p2p)全互联,处在 Internet 路由层次结构的最顶层,是整个 Internet 的核心.*Tier*1 AS 没有提供商,传输层 AS 既有提供商也有客户,而边缘层 AS 没有客户.如图 2 所示,自治系统 *A*,*B* 属于核心层,*C*,*D*,*E* 属于传输层,*F*,*G*,*H* 是边缘层的自治系统.

1.2 AS路由策略

AS 对其域内的路由设备具有完全的控制,因此,每个 AS 可以独立地制定路由策略以实现其利益诉求.尽管这些路由策略从单个 AS 的角度来看是正确的,但多个 AS 之间的路由策略却可能发生冲突,进而在路由系统中造成持续的震荡[9].Griffin 等人研究了 AS 路由策略对 BGP 稳定性的影响,指出 AS 间的路由策略不存在竞争环(dispute wheel)是 BGP 系统稳定的一个充分(非必要)条件[9],但对竞争环进行检测是 NP-Complete 的[10].Gao 和 Rexford 基于前述章节中的 AS 商业关系模型和 Internet 路由结构的层次特性,通过约束 AS 的路由输入、选择和输出策略,给出了一个操作性更强的充分条件,称为 Gao-Rexford 约束[11,12].该约束较好地反映了 ISP 逐利的特性,在刻画 BGP 路由行为方面得到了较为广泛的应用,如文献[13]等.该约束具体包含以下 3 点内容:

- ***GR*1**:严格层次特性.AS 级拓扑不存在 c2p(p2c)的环路,即,任何 AS 都不能间接地成为自己的提供商(客户);
- ***GR*2**:路由选择策略.AS 在进行路由选择时,客户路由优先于对等体路由,进而优先于提供商路由.其原因在于:选择客户 AS 作为下一跳可以赢利,选择对等体 AS 可以实现免费转发,而选择提供商 AS 则需要付费;
- ***GR*3**:路由输入/输出策略.从提供商和对等体 AS 学到的路由只允许向客户 AS 宣告,从客户 AS 学到的路由可以向所有邻居 AS 宣告.

如果一条 AS 路径经过的所有 AS 都遵循 *GR*3,那么该路径满足“无谷底”(valley-free)特性[11].即,AS 路径穿过一条 p2c 或 p2p 连接后,不能再穿过 c2p 或 p2p 连接.例如,图 2 中的 AS 路径 $C\rightarrow A\leftarrow D\leftarrow G$ 符合无谷底特性,而 $C\rightarrow A\leftarrow D\rightarrow B$ 不符合,因为该路径在穿过 $A\leftarrow D$(p2c 连接)之后又穿过了 $D\rightarrow B$(c2p 连接).由于在 Internet 路由层次结构中提供商所处层次一般要高于客户,我们将一个 AS 经过连续的 c2p/p2c 连接(1 条或多条)到达另一个 AS 的过程称为“上坡/下坡”,相应的路径序列称为“上坡路径/下坡路径”.“无谷底”特性对客户路由、对等体路由和提供商路由的存在形式做出了限制,如图 1 所示.

1.3 BGP路由和路由决策

一条 BGP 路由包含两组属性:目的地标识(网络前缀,prefix)和去往该目的地的路径属性(path attribute)[1].路径属性包括 ORIGIN,MULTI_EXIT_DISC,LOCAL_PREF 和 AS_PATH 等.BGP 利用 AS_PATH 属性来避免 AS 级的路由环路:每个 AS 将路由传播给邻居 AS 之前,需要把自己的 AS 号添加到该路由的 AS_PATH 列表的左端.接收方 AS 通过检查自己的 AS 号是否出现在路由的 AS_PATH 列表中来判明本 AS 是否已处理过该路由.

定义 2(源 AS、下一跳 AS). 考虑到与本文内容的相关性,BGP 路由 r 被简化为二元组 $r=(d,v_{k-1}\ldots v_1v_0)$,其中:$d$ 是网络前缀,表示一块连续的 IP 地址;$v_{k-1}\ldots v_1v_0$ 是 r 的 AS_PATH 属性的 AS 列表.最右侧的 v_0 是网络前缀 d 的所有者,称为源 AS($r.origin$);路由 r 经过的不同于源 AS 的第 1 个 AS,称为下一跳 AS($r.nexthop$).例如,若 $v_1\neq v_0$,则 v_1 是 r 的下一跳 AS.

BGP 是单路径协议.对于任意 AS,去往一个目的网络可能会存在多条路由,但是只有最优路由才被用于数据转发和向 BGP 邻居通告.BGP 的最优路由选择(以下简称路由选择)是一个复杂的过程,更多细节可参见文献[1].在理论分析中,我们仅考虑选择:

(1) 具有最高的 LOCAL_PREF 值的路由(*GR*2);

(2) 具有最短 AS_PATH 长度的路由.

RouteViews[14]和 RIPE-RIS[15]是分别由美国俄勒冈州立大学和欧洲网络协调中心(RIPE Network Coordination Centre)设立的 BGP 路由数据发布服务.它们与数百个 AS 建立了 BGP 会话,并周期性地发布从这些 AS 获得的路由表和路由更新数据.根据这些数据,我们可以获知这数百个 AS 的路由决策结果,即,这些 AS 去往各个目的网络的 AS 级路径及变化.

1.4 路由劫持

为了劫持到前缀 d 的路由,攻击者自治系统 X 通常伪造并向邻居 AS 宣告一条到特定前缀 d'的长度为 k 的

AS 路径,记为 p.不失一般性,令 $p=v_{k-1}\dots v_0$.为了避免攻击行为被邻居 AS 察觉,v_{k-1} 通常是攻击者 X 本身.注意到,当 $k>1$ 时,宣告路由的 AS(X)并不等于路由的源 AS(v_0).更一般地,定义路由的发起者如下:

定义 3(路由 r 的发起者 AS(initiator AS)). 在路由 r 传播所经过的 AS 中,若某 AS 向邻居传播的路由并非学自于其他邻居,称该 AS 为 r 的发起者.

根据 d'和 d 之间的关系以及 k 的长度,对路由劫持的分类可以从两个维度上进行:

- 在一个维度上,根据 d'是 d 的父前缀($d'\supset d$)、子前缀($d'\subset d$)还是 d 本身($d'=d$),路由劫持可分为“父前缀劫持”、“子前缀劫持”和“确切前缀劫持”.由于 BGP 中路由的传播在前缀粒度上独立进行,“父前缀劫持”或“子前缀劫持”中的劫持路由会传播到受害者 AS 而被发现,攻击效果易于预测,因此,本文中主要讨论对“确切前缀劫持”的防范.但如本文第 3 节所示,本监测方法也具备对“父前缀劫持”和“子前缀劫持”的防范能力;
- 在另一个维度上,k=1 对应于“非法的源 AS”攻击,也就是通常所说的“前缀劫持”;k=2 对应于“下一跳劫持”.前缀劫持在 BGP 中表现为“多源 AS(multiple origin ASes,简称 MOAS)”冲突[16],易于被鉴别;相比而言,通过伪造长度大于 1 的 AS 路径进行路由劫持具有更强的隐蔽性,因为仅有被伪造的邻接关系所涉及的 AS 才能鉴别该攻击.理论上,攻击者可以伪造长度任意的 AS 路径进行路由劫持,但攻击效果(如吸附的流量)会随 k 的增加而迅速衰减.本文中只考虑 k=1,2 时的路由劫持,这也是已报道的路由劫持事件中最常见的情形.

2 AS 自我免疫能力模型

将 Internet 在 AS 级的拓扑表示为无向图 $G=\langle V,E,R\rangle$,其中,V 是 AS 集合,E 是 AS 节点之间的边的集合,R 是 E 到集合{p2c,c2p,p2p}的映射.由于 AS 级 Internet 拓扑的演化相对缓慢[17],本文假定在一定时间内 G 相对不变.G 中仅有 AS u 宣告了一个网络前缀 d.本文中用 $Neigh(u)$表示 u 在 G 中所有邻居 AS 的集合,$Neigh(u)=\{v|\forall v\in V\wedge(u,v)\in E\}$,并用 $Prov(u)$,$Cust(u)$和 $Peer(u)$分别表示 u 的提供商、客户和对等体邻居 AS 的集合.以图 1 为例,$Neigh(C)=\{A,D,F\}$,$Prov(C)=\{A\}$,$Cust(C)=\{F\}$,$Peer(C)=\{D\}$.

本文在对 AS 自我免疫能力建模的过程中,除了引入 Gao-Rexford 约束,还作如下假设:

假设 1(唯一性假设). 每个 AS 到一个前缀只能选择一条最优路由,一对 AS 之间只存在一种商业关系.

假设 2(攻击策略假设). 为了最大化攻击效果,AS 发起路由劫持时,向自己所有的邻居宣告伪造的路由.

假设 3(连通性假设). 在路由劫持发生之前,V 中任意两个自治系统之间相互可达.

定义 4(影响范围 $V_{(i)}$). AS i 是前缀 d 的一个发起者,待 BGP 收敛后,AS i 的影响范围定义为 V 中选择了 i 发起的路由作为最优路由的 AS 集合,记为 $V_{(i)}$.当前缀 d 在整个路由系统中只有一个发起者 i 时,基于连通性假设(假设 3),$V=V_{(i)}$;但是当存在多于一个发起者时,$V_{(i)}$取决于这多个发起者发起的路由在路由系统中扩散、传播和相互作用.在下文中,如果 AS $x\in V$ 且 $x\in V_{(a)}$(a 为攻击者 AS),则称 x 被污染.

路由劫持发生时,若劫持路由传播到了受害者 AS,称受害者 AS 对此路由劫持免疫(也称为自我免疫).此定义基于两个假设:

(1) 绝大多数 AS 都在域内部署了用于网络管理、测量和信息采集的设施,只要劫持路由传播到了受害者 AS 的路由器,无论该劫持路由是否被选为最优路由,我们都认为受害者 AS 能感知到该路由劫持;

(2) 之后,受害者 AS 可以采取反制措施以消除路由劫持的影响,如宣告被劫持网络的子前缀等.

假设 $V\backslash\{u\}$中的每个 AS 对 u 发起路由劫持的概率相同,定义 u 对路由劫持的免疫能力 $\mathfrak{I}_u$ 如下:

定义 5(免疫能力 $\mathfrak{I}_u$). AS u 的自我免疫能力 $\mathfrak{I}_u=|C_u|/(|V|-1)$,其中,$C_u$ 是一个 AS 集合,u 对从该集合中的每个 AS 发起的路由劫持都免疫.

根据 BGP 路由决策模型,一个 AS 是否会被污染,不仅取决于它接收到的攻击者 a 发起的劫持路由,还取决于它到受害者 AS u 的路由.下面首先对路由劫持发生前 V 中 AS 使用的去往 u 的路由进行讨论.

2.1 无路由劫持的BGP系统

定义 6. 提供商闭包ψ_u是u仅通过上坡路径就能到达的自治系统的集合.换言之,ψ_u中的AS可以通过下坡路径到达u.以图1为例,$\psi_F=\{C,D,A,B\}$,$\psi_E=\{B\}$.

定义 7. 客户闭包ζ_u是u仅通过下坡路径就能到达的自治系统的集合,换言之,ζ_u中的AS可以通过上坡路径到达u.以图1为例,$\zeta_C=\{F\}$,$\zeta_F=\varnothing$.

根据上述定义,对于去往u的最优路由选择,ψ_u中的AS选择的一定是客户路由;相反,ζ_u中的AS选择的一定不是客户路由.证明过程见推论1和推论2.

推论 1. 仅ψ_u中的AS有到达u的客户路由,且ψ_u中的AS选择的去往u的路由一定是客户路由.

证明:首先证明充分性.根据定义,$\forall x\in\psi_u$,存在从u到x的一条上坡路径$u\rightarrow\ldots\rightarrow y\rightarrow x$($y$是到$x$前的最后一跳);相应地,存在一条从$x$到$u$的下坡路径$x\leftarrow y\leftarrow\ldots\leftarrow u$.因此,$x$有通过客户$y$去往$u$的客户路由.然后证明唯一性.假设$\exists x\notin\psi_u$,$x$从其客户$y$学到一条到$u$的路由.根据图2列举的7种模式,$y$宣告给$x$的去往$u$的路由只能属于模式VII,是一条下坡路径,记为$y\leftarrow\ldots\leftarrow u$,故$x\leftarrow y\leftarrow\ldots\leftarrow u$也是一条下坡路径,故$x\in\psi_u$,与题设矛盾. □

根据充分性证明,ψ_u中的AS一定有到u的客户路由.根据*GR*2,它们选择的去往u的路由一定是客户路由.

推论 2. $\psi_u\cap\zeta_u=\varnothing$,即$u$的提供商闭包和客户闭包之间不存在交集.结合推论1,u的客户闭包中的AS都没有去往u的客户路由.该推论事实上是*GR*1的外延.

证明:假设$\exists x\in\psi_u$且$x\in\zeta_u$,根据提供商闭包的定义,从u到x存在一条上坡路径$u\rightarrow\ldots\rightarrow x$;根据客户闭包的定义,从$u$到$x$存在一条下坡路径$u\leftarrow\ldots\leftarrow x$.若这两条路径除$u$和$x$外不存在交点,则它们在$u$和$x$之间形成一个闭合环路,与*GR*1矛盾;若存在交点,不失一般性,记其中一个交点为y,则至少形成两条回路,$u\rightarrow\ldots\rightarrow y\rightarrow u$和$x\rightarrow\ldots y\rightarrow x$,与*GR*1矛盾.题设得证. □

假设 4. $\psi_u\cap\zeta_{Peer(u)}=\varnothing$,其中,$\zeta_{Peer(u)}$表示$u$的对等体的客户闭包.假设4指$u$的提供商闭包和$u$的对等体的客户闭包不存在交集,进而$u$的对等体的客户闭包中的AS没有到$u$的客户路由.

虽然Gao-Rexford约束中强调不允许p2c(c2p)连接构成环路,但未对p2p连接做限定.理论上,p2c连接涉及的两个AS中,服务商的网络规模要大于客户,而p2p连接只存在于两个网络规模相当的AS之间,因此,ψ_u中AS的网络规模要大于u的对等体的规模以及u的对等体的客户的规模.据此,我们假设u的提供商闭包和u的对等体的客户闭包之间不存在交集.结合推论1和本假设可知,$\zeta_{Peer(u)}$中的AS没有去往u的客户路由,但是在实验评估中我们注意到,该假设对于有些自治系统并不成立.

2.2 自我免疫的条件

由于BGP中每个ASu只能从邻居AS学习路由,直观上,ASu对ASa发起的路由劫持免疫当且仅当:$\exists x\in Neigh(u)\cap V_{(a)}$,$x$向$u$输出了到前缀$d$的路由.即至少存在一个邻居AS,该邻居选择了攻击者发起的劫持路由作为最优路由,且该邻居的路由策略允许它将劫持路由向源AS通告,称为自我免疫的前提.

为了判明u能对何种形态的攻击路由实现自我免疫,我们以u的邻居为研究对象,首先分析它们是否会被攻击路由污染(*C*1),然后分析若是被污染,它们是否会向u输出攻击路由(*C*2).具体分析过程见表2:首先,通过与现有的去往u的路由(existing route to victim)进行比较,依据BGP路由决策模型列举了使u的邻居满足*C*1的攻击路由的可能形态(route to attacker);然后,根据这些邻居与u之间的商业关系判断*C*2是否成立,最终得到了能够使u自我免疫的攻击路由的具体形态.

表2根据与u的商业关系,我们将u的邻居分为提供商、对等体和客户等3类,然后分别讨论这3类邻居能否使*C*1和*C*2成立:

(1) $\forall x\in Prov(u)$,x从u学到长度为1的客户路由.根据BGP路由决策模型,只有劫持路由也是客户路由且长度为1时,x才有可能被污染,此时,x用于去往u和a的路由具有同等优先级.注意,x是可能而非一定被污染,因此,表2中的条件(Bi)只是u自我免疫的可能性条件;

(2) $\forall x\in Peer(u)$,x从u学到长度为1的对等体路由,仅当劫持路由是长度为1的对等体路由或任意长度

的客户路由时,x 才被污染.前者是使 x 被污染的可能条件,后者是充分条件.由于 $GR3$ 不允许将对等体路由向另一个对等体转发,因此,只有后者同时使 $C1$ 和 $C2$ 满足,得到充分条件(Bii);

(3) $\forall x\in Cust(u)$,x 从 u 学到长度为 1 的提供商路由.当劫持路由是长度为 1 的提供商路由时,x 有可能被污染.当劫持路由是对等体或客户路由时,x 一定被污染.根据 $GR3$,每个 AS 只能向提供商输出客户路由,因此,仅当劫持路由是客户路由时 $C2$ 才被满足,得到充分条件(Biii).

Table 2 Conditions for AS to be immune to BGP hijacking

表 2 AS 实现自我免疫的条件

	Existing route to victim		$C1$ (route to attacker)		$C2$ (export to u)	Index	Attacker location (AS a)
Peer group	Route type	Length	Route type	Length			
$Prov(u)$	Customer route	1	Customer route	1	√	(Bi)	$a\in Cust(Prov(u))\backslash\{u\}$
$Peer(u)$	Peer route	1	Peer route	1	×		
			Customer route	Any	√	(Bii)	$a\in\zeta_{Peer(u)}$
$Cust(u)$	Provider route	1	Provider route	1	×		
			Peer route	Any	×		
			Customer route	Any	√	(Biii)	$a\in\zeta_u$

当攻击者 AS 发起下一跳劫持时(宣告长度为 2 的 AS 路径),表 2 中的条件(Bi)不能使 $C1$ 得到满足,因此,(Bi)不适用于下一跳劫持;条件(Bii)和(Biii)都与劫持路由的 AS 路径长度无关(any),因此对于下一跳劫持也成立.

条件(Bi/Bii/Biii)是(提供商/对等体/客户)向 u 输出攻击路由时攻击路由的形态.在(Bi)中,u 的提供商学到了去往 a 的长度为 1 的客户路由,此时 $a\in Cust(Prov(u))\backslash\{u\}$,即 u 的提供商除 u 之外的直接客户;在(Bii)中,u 的对等体学到了去往 a 的客户路由,根据 $GR3$ 对应的 7 种模式,客户路由的形式仅包含模式 VII,因此从该对等体到 a 必定存在一条下坡路径,此时 $a\in\zeta_{Peer(u)}$,即 u 的对等体的客户闭包;在(Biii)中,u 的客户学到了去往 a 的客户路由,同(Bii),此时 $a\in\zeta_u$.

注意到,$a\in\zeta_{Peer(u)}$是(Bii)成立的必要而非充分条件,但结合假设 4,则演化为充分必要条件.例如,不考虑假设 4,虽然从 u 的一个对等体(不妨记为 x)到 a 之间存在一条下坡路径,但若该下坡路径上有的 AS 优选 u 而非 a 发起的路由,那么 x 可能不被 a 发起的路由污染,从而不会向 u 输出 a 发起的劫持路由.但假设 4 中$\zeta_{Peer(u)}$中的 AS 都没有去往 u 的客户路由,因此能保证从 x 到 a 的下坡路径上的所有 AS 都优选去往 a 的客户路由,故 u 能从 x 学到 a 发起的客户路由.同理,$a\in\zeta_u$ 也只是(Biii)成立的必要而非充分条件,结合推论 2 后成为充分必要条件.

2.2.1 对前缀劫持自我免疫的充分条件和必要条件

定理 1. 自治系统 u 对前缀劫持自我免疫的充分条件是攻击者 AS $a\in Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}$.即当 a 是 u 的直接邻居,或是 u 和 u 的对等体的客户闭包中的 AS 时,u 对 a 发起的前缀劫持免疫.

证明:

(1) 当 $a\in Neigh(u)$时,根据假设 2,每个攻击者都向其所有的直接邻居宣告伪造的攻击路由,因此 u 可以检测到 a 发起的前缀劫持;

(2) 当 $a\in\zeta_{Peer(u)\cup\{u\}}\backslash Neigh(u)$时:

- 若 $a\in\zeta_{Peer(u)}\backslash Neigh(u)$,根据客户闭包的定义,$a$ 和 u 的一个对等体 $x\in Peer(u)$之间存在一条上坡路径 p,沿着 p 的所有 AS 都属于ζ_x.根据假设 4,ζ_x 中的 AS 都没有去往 u 的客户路由,因此,沿着 p 的所有 AS 都会选择 a 发起的客户路由.故 x 可以沿 p 这条路径学到去往前缀 d(发起者为 a)的客户路由,并通过 $u\leftrightarrow x$ 这条 p2p 连接宣告给 u;
- 若 $a\in\zeta_u\backslash Neigh(u)$,$a$ 和 u 之间存在一条上坡路径 p,沿着 p 的所有 AS 都属于ζ_u.由于ζ_u 中的 AS 都没有去往 u 的客户路由(推论 2),因此,沿着 p 的所有 AS 都没有去往 u 的客户路由,却都可以选择沿 p 学到的客户路由去往 a.根据 $GR2$,在选择去往前缀 d 的路由时,它们都会选择 a 发起的路由,最终,u 沿着 p 学到 a 发起的劫持路由. □

定理 2. 自治系统 u 对前缀劫持自我免疫的必要条件是攻击者 AS $a\in Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}\cup Cust(Prov(u))$.

即 u 对 a 发起的前缀劫持免疫时,攻击者 a 或者是 u 的直接邻居,或者是 u 和 u 的对等体的客户闭包中的 AS,或者是 u 的提供商的直接客户.

证明:假设攻击者 $a\notin\{Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}\cup Cust(Prov(u))\}$,且 u 学到了 a 发起的劫持路由.由于 $a\notin Neigh(u)$,故 a 不是 u 的直接邻居,则至少存在邻居 $x\in Neigh(u)$有 $x\in V_{(a)}$,且 x 将 $a(x\neq a)$发起的攻击路由宣告给了 u.下面对 x 与 u 的商业关系展开讨论:

(1) 若 $x\in Cust(u)$,由于无谷底原则只允许客户 AS x 输出形入 $a\to\ldots\to x$ 的路径到提供商 u(模式 VII),根据客户闭包的定义,$a\in\zeta_u$,与题设矛盾;

(2) 若 $x\in Peer(u)$,同情形(1),由于无谷底原则只允许 x 输出形入 $a\to\ldots\to x$(模式 VII)的路径到 u,根据客户闭包的定义,$a\in\zeta_x$,考虑到$\zeta_x\subseteq\zeta_{Peer(u)}$,因此 $a\in\zeta_{Peer(u)}$,与题设矛盾;

(3) 若 $x\in Prov(u)$,x 从 u 学到的长度为 1 的客户路由,根据 BGP 路由决策原理,x 必定有去往 a 的长度为 1 的客户路由,否则,x 不会被劫持路由污染.此时,a 必为 x 的客户,即 $a\in Cust(Prov(u))$,与题设矛盾.

综上,题设得证. □

2.2.2 对下一跳劫持自我免疫的充分必要条件

类似于对前缀劫持自我免疫的充分、必要条件的推导,可以得到如下结论:

定理 3. 自治系统 u 对下一跳劫持自我免疫的充分必要条件是攻击者 AS $a\in Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}$.

证明:分为充分性证明和必要性证明.充分性证明与定理 1 完全相同,略去.

必要性证明与定理 2 基本类似,假设 $a\notin\{Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}\}$,仅在情形(3)有所区别:若 $x\in Prov(u)$,x 从 u 学到的长度为 1 的客户路由.虽然 a 是 x 的客户,由于 a 宣告的是 AS 长度为 2 的劫持路由,因此,x 仍然优选 u 发起的正确路由.在这种情形下,u 不会从 x 学到劫持路由,与题设矛盾.

综上所述,题设得证. □

2.3 自我免疫能力上界及评估

根据定理 1、定理 2,前缀劫持下的 AS 级自我免疫能力满足以下不等式:

$$\Im_u\geqslant\frac{|Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}|}{|V|-1} \tag{1}$$

$$\Im_u\leqslant\frac{|Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}\cup Cust(Prov(u))|}{|V|-1} \tag{2}$$

根据定理 3,下一跳劫持下的 AS 级自我免疫能力满足以下等式:

$$\Im_u=\frac{|Neigh(u)\cup\zeta_{Peer(u)\cup\{u\}}|}{|V|-1} \tag{3}$$

结合公式(1)~公式(3),无论是针对前缀劫持还是下一跳劫持,公式(2)都是 $\Im_u$ 的上界.另外,推论 2 和假设 4 并不一定适用于所有的 AS,进一步降低了 AS 对路由劫持的免疫能力.例如,若 $\psi_u\cap\zeta_{Peer(u)}\neq\varnothing$(假设 4 不成立),即使攻击者 AS $a\in\zeta_{Peer(u)}$,AS u 也不一定能够实现自我免疫.不妨假设 AS $Y\in\psi_u\cap\zeta_{Peer(u)}$,当$\exists x\in Peer(u)$使攻击者 $a\in\zeta_x$ 时,Y 恰好在从 a 到 x 的上坡路径上,由于 Y 有去往 u 的客户路由,它并不一定优选 a 发起的劫持路由,因此,x 不一定能学到劫持路由,进而 u 的自我免疫失败.此外,实际情况中,攻击者 AS 试图劫持邻居 AS 的网络前缀时,它们不大可能将伪造的、用于实施攻击的路由宣告给邻居 AS.因此,将公式(2)作为 $\Im_u$ 的上界是合理的.接下来,我们基于公式(2)对当前 Internet 中的 AS 级免疫能力的上界进行评估.

2.3.1 数据集

鉴于实际采集的 Internet 拓扑的不完整性[18]以及商业关系推断算法的不准确性[19,20],评估中采用了两个不同的拓扑图:拓扑 1 简称为 CAIDA,基于 CAIDA 发布的 2010 年 1 月 20 日的互联网 AS 级拓扑和对 AS 间商业关系的推断[7];拓扑 2 简称为 Gao,基于同一天从 RouteViews 以及 RIPE-RIS 项目采集到的路由表(主要是路由的 AS_PATH 属性),然后采用 Gao 算法[11]推断 AS 间的商业关系.两个拓扑的基本参数见表 3,两者在 p2c,p2p 连接所占比例上有明显的差异,体现了一定程度上的数据多样性.

Table 3 Data set of Gao and CAIDA topologies

表 3 Gao 和 CAIDA 拓扑数据

	# of ASes	# of AS links	# of p2c	# of p2p	# of s2s
Gao	34 182	97 485	77 172, 79.2%	17 935, 18.4%	2 378, 2.4%
CAIDA	33 508	75 001	69 191, 92.3%	5 591, 7.4%	219, 0.3%

对于推论 2,CAIDA 中有 127 个(0.38%),Gao 中有 199(0.58%)个 AS 的提供商闭包和客户闭包产生了重叠,即超过 99%的自治系统满足推论 2;对于假设 4,CAIDA 中有 1 333 个(3.98%),Gao 中有 1 533 个(4.48%)个 AS 的提供商闭包和对等体的客户闭包产生了重叠,即超过 95%的自治系统满足假设 4.总体而言,违反推论 2 和假设 4 的自治系统所占比例很小,公式(2)作为$\mathfrak{I}_u$的上界能够反映绝大多数 AS 对于路由劫持的免疫能力.

评估同时考虑了 Internet 拓扑的层次特性和流量特性.在层次特性方面,我们将 AS 分为 *Tier*1,*Transit* 和 *Stub* 这 3 层,具体的方法是:

(1) 从一个预先选定的、公认的、小规模的 *Tier*1 集合出发(8 个),每次将 *V**Tier*1 中与当前 *Tier*1 中所有 AS 均有连接、度数最大的 AS 加入到 *Tier*1 集合中,直到再也找不到这样的 AS 为止.算法终止时,一共得到了 18 个 *Tier*1;

(2) 根据从 RouteViews 和 RIPE-RIS 收集的 AS 路径,只出现在路径最右边的 AS 被定义为是 *Stub*(28 691 个);

(3) 剩下的 AS 被划分为 *Transit*(5 486 个).

同时,为了更准确地刻画 Internet 的流量特性——一少部分稳定的前缀承载了 Internet 中绝大部分流量[21],内容服务提供商(Internet content provider,简称 ICP)所在的自治系统受到了重点关注.具体方法如下:

首先,从 Alexa[22]的站点排名中选取访问流量排名前 300 的网站的网址;然后,通过本地的 DNS 服务器以及 GoogleDNS[23]和 OpenDNS[24]将这些网址解析成 IP 地址;之后,使用 RouteViews 的 BGP 路由表将这些 IP 地址关联到宣告它们的 AS;最后,借助于 Whois 数据库[25]和搜索引擎查询这些 AS 号所属 ISP 的名字,只有名字与网址存在一定关联的 AS 才被认为属于 ICP.

使用这种方式,300 个网址中有 283 个网址解析得到的 IP 地址成功地与 AS 号建立了关联,最终得到了 182 个被认定为 ICP 的 AS,称为 *Traffic-Set*.解析得到的 AS 号远少于网址数是因为一些跨国企业往往使用一个 AS 号来服务多个站点,例如,Google 使用 AS 号 15169 提供服务的站点包括 google.com,google.com.hk,google.de,google.co.uk 等.

2.3.2 评估结果

图 3 展示了 CAIDA 和 Gao 拓扑下 AS 对路由劫持的免疫能力的补充累积分布(complementary cumulative distribution function,简称 Ccdf).尽管表 3 显示了 CAIDA 和 Gao 拓扑之间存在着显著的差异,但如图 3 所示,两种拓扑中 AS 对路由劫持的免疫力的分布却非常接近.得益于更多的连接数、更高的 p2p 连接比例,Gao 拓扑中 AS 的免疫力略高于 CAIDA 拓扑中的情形.但就整体而言,两个拓扑中,AS 对路由劫持的免疫能力都很低.CAIDA 中仅有 16.8%的自治系统的免疫力大于 0,这个比例在 Gao 中是 17%.换言之,超过 80%以上的自治系统对路由劫持完全没有免疫力;免疫力超过 85%的 AS 的比例在 CAIDA 中是 0.23%,在 Gao 中是 0.26%.

图 4 展示了 Gao 拓扑中不同类型的 AS 对路由劫持的免疫能力,可以得到以下结论:

(1) *Tier*1 表现出了最强的免疫力,所有 *Tier*1 AS 的免疫力都高于 95%,其原因在于,*Tier*1 AS 及其对等体 AS(也是 *Tier*1 AS)有庞大的客户闭包;

(2) *Transit*,*Stub* 和 *Traffic-Set* 中的 AS 均表现出了很低的免疫能力,且 *Stub* 的免疫力最差.其中,43.4%的 *Traffic-Set* 以及几乎全部的 *Stub* 对路由劫持没有免疫能力.免疫力超过 85%的自治系统在 *Transit* 和 *Traffic-Set* 中所占的比重分别为 1.28%和 6.59%;

(3) 虽然 *Traffic-Set* 中的 AS 在整体上表现出了略强于 *Transit* 中 AS 的免疫能力,但仍然达不到保证其承载的 Internet 内容服务的安全性的要求.

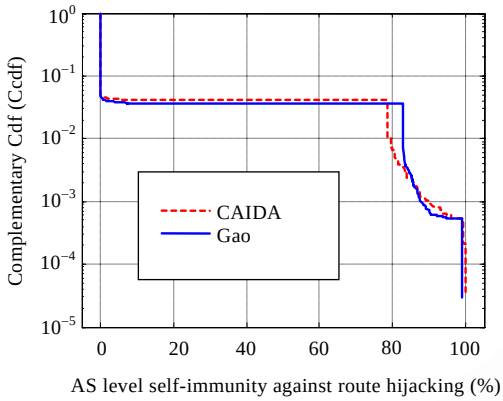

Fig.3 Ccdf of AS-level immunity under two topologies

图 3 两种拓扑下,AS 对路由劫持的自我免疫能力

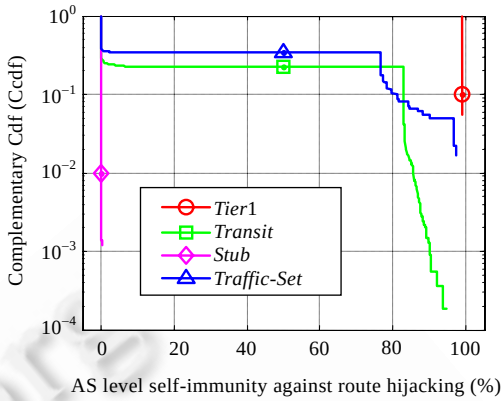

Fig.4 Ccdf of AS-level immunity of tiered ASes

图 4 不同类型的 AS 对路由劫持的自我免疫能力

2.4 AS自我免疫力低下的根源——提供商栅栏

为了直观地展示 AS 对路由劫持免疫力低下的原因,图 5 标记了 AS 0 的免疫范围的上界.该范围具体包括:AS 0 的直接邻居 AS 5,AS 8,AS 13;AS 0 的提供商(AS 5,AS 8)的直接客户 AS 6,AS 7,AS 9;AS 0 及其对等体 AS 13 的客户闭包中的 AS.同时,图 5 也展示了 AS 14 劫持 AS 0 的网络前缀时网络中 AS 的状态.

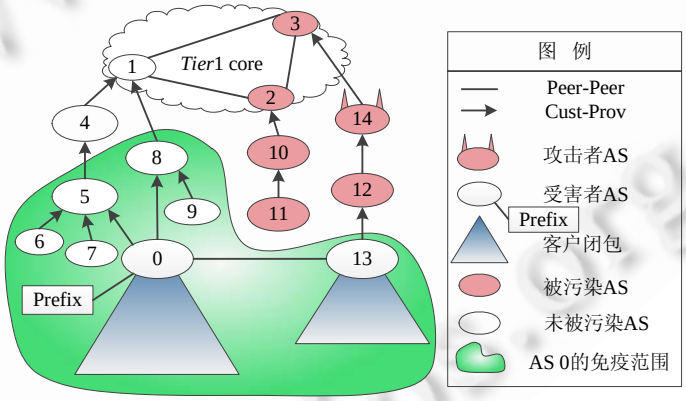

Fig.5 An AS's immunity against route hijacking

图 5 AS 的免疫范围示例

对于 AS 0 的服务提供商,BGP"只传播最优路由"和 *GR*2 是造成 AS0 难于从它们学到劫持路由的主要原因.以 AS 0 的间接服务提供商 AS 1 为例,AS 1 从它的两个 *Tier*1 对等体(AS 2 和 AS 3)接收到了 AS 14 发起的劫持路由,但由于 AS 0 发起的客户路由具有更高的优先级(*GR*2)和 BGP 只传播最优路由的特性,它并不会优选劫持路由,自然也不会向其客户 AS 4 和 AS 8 传播此劫持路由.基于同样的原因,仅当攻击者 AS 是 AS 5 或 AS 8 的直接客户时,AS 5 或 AS 8 才有可能优选劫持路由并向 AS 0 通告此劫持路由.

除了上述的 BGP"只传播最优路由"和 *GR*2,*GR*3 是阻止 AS 0 的对等体和客户向其输出劫持路由的又一重要原因.根据 *GR*3,对等体/客户只能向对等体/提供商输出客户路由,这使得仅当攻击者 AS 来自于 AS 0 本身的客户闭包或者 AS 0 的对等体的客户闭包时,AS 0 才有可能通过对等体或客户学到劫持路由.以 AS 0 的一个对等体 AS 13 为例,即便 AS 13 优选从 AS 12 学到的劫持路由,受限于路由输出策略,它也不会向 AS 0 输出此劫持路由.

一个典型的 AS(非 *Tier*1 自治系统)依赖其提供商 AS 来实现到网络中其他自治系统的可达性.当针对于它的路由劫持发生时,其提供商出于自身利益优选客户路由,导致攻击路由不能传播到受害者 AS.这种提供商阻碍了自治系统自我感知路由劫持的现象称为提供商栅栏(provider barrier)现象.

提供商栅栏的存在,使自治系统仅能感知自身的客户闭包、对等体的客户闭包中的自治系统发起的路由劫持,以及以一定概率感知提供商的直接客户发起的路由劫持(定理 1~定理 3).对应于以上分析,为了提高 AS 对路由劫持的自我免疫能力,可以采取以下措施:

第 1 种方法是改变 BGP 中只传播最优路由的行为,将 BGP 改造成类似 OSPF 的路由协议,但这样违背了 BGP 的设计初衷,会显著降低 BGP 的可扩展性;

第 2 种方法是改变 AS 的路由选择和输出策略,但这与 AS 的利益诉求相矛盾,不会得到运营商的支持;

第 3 种方法是通过提升自己在 Internet 路由结构中的层次来扩展自身和对等体的客户闭包的范围,但此方法经济代价高昂,在实践中并不可行.

第 4 种方法是采用协同监测,越过提供商栅栏,从提供商之外的 AS 学习路由用于对路由劫持的检测.实验评估显示,Internet 中绝大多数 AS 对路由劫持的免疫力都很低,具备了广泛的协同基础,但该方法能否成功还取决于对以下几个问题的解决:

(1) 兼容性.BGP 是 Internet 的核心基础设施,如何保证协同监测交换的路由不扰乱现有的路由功能;

(2) 隐私保护.ISP 视路由策略为商业秘密,协同需要 ISP 向协同伙伴透漏一部分路由信息,如何保证 ISP 对信息交换的控制并在不损害安全能力的前提下尽可能少地泄漏 ISP 的隐私;

(3) 有效性和准确性.由于缺乏准确的前缀-源 AS 对应关系和 AS 邻接关系,检测前缀劫持和下一跳劫持一直是公认的难题,如何降低路由劫持检测过程中的“漏检率”和“误检率”?此外,方法中应使用较成熟的技术,避免引入新的技术风险.

3 防范路由劫持的协同监测方法

为了克服提供商栅栏,在 AS 级提高对路由劫持的免疫能力,我们提出了防范路由劫持的协同监测方法:参与协同的每个 AS 与它的协同邻居 AS 交换各自感兴趣的路由更新,并基于接收到的路由更新信息检测路由劫持.该方法的要点包括:

① 每个成员 AS 在域内设立一个监测器,定义相关于本 AS 的前缀集(一般是属于本 AS 的网络);

② 监测器在 AS 内部使用“只收不发”的 BGP 会话学习路由用于和协同邻居交换;

③ 在监测器之间,每个监测器从协同邻居只能学习到相关于本 AS 网络的路由,向每个协同邻居只输出相关于该邻居的路由;

④ 监测器基于从邻居接收到的、相关于本 AS 所属网络的路由更新检测路由劫持.

由于每个参与者 AS 从协同邻居 AS 学到的路由并不能用于数据转发,因此本方法不会产生兼容性问题.具体地,监测器与域内路由器之间的 BGP 会话具有“只收不发”的特性,从监测邻居学到的路由不会在域内传播;监测器从协同邻居学到的路由相关于本 AS 所属网络,不存在将其用于转发数据的动机.此外,根据 BGP 规范,一个 IP 地址可用作转发数据的下一跳仅当该 IP 在 IGP 中可达,因此,将远端监测邻居的 IP 地址设为转发数据的下一跳并不可行.

本方法能够较好地保护参与者的隐私.在 RouteViews 和 RIPE-RIS 项目中,每个参与者被建议输出整个路由表,使得对参与者路由策略的推导相对容易.在本方法中,一方面参与者具有相当的灵活性,可以自主地决定向协同邻居暴露相关于哪些网络前缀的路由信息;另一方面,暴露的路由信息以多个片段的形式分布在不同的监测邻居之间,使得外界难于推断参与者的路由策略.

本方法使用源认证的思想由网络的拥有者本身对路由劫持进行检测,保证了检测的有效性和准确性,绕开了第三方难以区分正常路由变化和路由劫持的难题.同时我们认为,这种利己特性将有助于本方法的推广和应用.此外,本方法采用成对协同方式,每个参与者获得的安全能力并不取决于本方法的部署范围,而是取决于与

之协同的 AS 的数量和分布.

下面,我们从协同监测体系结构、对路由劫持的检测和协同邻居选择这 3 个方面介绍本方法的设计和实现.

3.1 协同监测体系结构

本方法在组织形式上以 AS 为基本单位,每个成员 AS 在域内设立一个协同监测器(cooperative monitor,下文中简称监测器).概念上,监测器由两个功能部件组成:路由组件和检测路由劫持的引擎组件.监测器使用路由组件运行 BGP 协议与其他成员交换路由变化,检测引擎基于路由组件接收到的 BGP 路由更新检测路由劫持.

3.1.1 监测器的域内实现

监测器从所在的 AS 学习实时的路由视图,以便能够向与之协同的其他监测器提供路由更新,但并不将从其他监测器学来的路由输出到所在 AS.前者通过路由组件与 AS 内的路由器(内部邻居)建立 iBGP 会话实现,后者通过配置监测器的路由输出策略实现.这种只收不发的 BGP 会话可以保证监测器输入的路由不会传播到监测器所在自治系统的内部,不影响原有的路由和数据转发功能.实际上,这种配置方式在现有的路由采集项目如 RouteViews 和 RIPE-RIS 中已经得到了广泛应用.也就是说,参与了 RouteViews 和 RIPE-RIS 项目的 AS 无需对域内的设施做任何改动,就可直接重用于协同监测方法的部署.

出于备份的目的,我们建议每个监测器与两个或两个以上的内部邻居互联.随着 AS 内 iBGP 拓扑组织形式的不同,监测器所连接的内部邻居也略有不同:

(1) 对于采用全互联拓扑的 AS,监测器需要与其中任意两个或两个以上的路由器建立 iBGP 会话.例如,图 6 中 AS *v* 的 4 个路由器 *R*1,*R*2,*R*3 和 *R*4 通过 iBGP 实现了全互联,AS *v* 的监测器与 *R*1 和 *R*4 建立了 iBGP 会话;

(2) 对于采用路由反射来组织 iBGP 拓扑的 AS,监测器需要与其中任意的两个或以上的路由反射器(RouteReflector,简称 RR)建立 iBGP 会话,并将监测器配置为路由反射器的客户(RouteClient,简称 RC).例如,图 6 中 AS *u* 有两个 *RR*(*RR*1 和 *RR*2)和 3 个 *RC*(*R*1,*R*2,*R*3),AS *u* 中的监测器与两个路由反射器 *RR*1 和 *RR*2 建立 iBGP 会话;

(3) 对于采用 BGP 联邦部署方式的 AS,监测器只需加入其中任意一个联邦,并与该联邦内任意两台或以上的路由器建立 iBGP 会话即可.

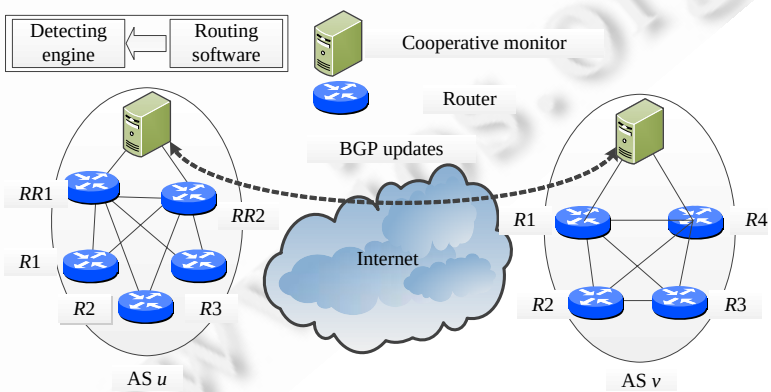

Fig.6 Cooperative monitoring architecture

图 6 协同监测体系结构

3.1.2 监测器的域间实现

属于不同 AS 的监测器之间,通过协同监测会话互联.协同监测会话本质上就是多跳步的 eBGP 会话.与 BGP 会话一样,协同监测会话使用 TCP 以实现可靠的通信,会话双方均采用 MD5 算法[26]防止消息被篡改.

监测器之间选择性地输出对方感兴趣、且符合本地策略的路由.考虑处在不同自治系统中的两个监测器 *u*

和 v,每个监测器都需要定义相关于本 AS 的前缀集,记为 I_u 和 I_v.一般而言,I_u 中的前缀要么属于 u,要么属于 u 的客户.协同检测会话(u,v)能够建立当且仅当双方均同意向对方发送对方感兴趣的路由更新,即 u 同意向 v 发送关于 I_v 中前缀的路由更新且 v 同意向 u 发送关于 I_u 中前缀的更新.当一方(u)提出建立协同监测会话的请求时,另一方(v)需要验证 u 是否合法地拥有 I_u 中的网络前缀.例如,通过查看 RouteViews 和 RIPE-RIS 项目发布的历史路由数据,检查 I_u 中前缀是否属于 u;在反方向上,u 也需要对 I_v 做同样的验证.

监测器 u 仅向 v 输出到相关于 I_v 中前缀(包括父前缀和子前缀)的路由,该策略可以通过 prefix-list 实现.例如,“ip prefix-list name permit *A.B.C.D* le 8 ge 32”表示 *A.B.C.D*/8~*A.B.C.D*/32 范围内的所有前缀.

3.2 路由劫持检测

按照 AS u 的管理员预定义的策略 P_u,检测引擎对从监测邻居学到的路由变化进行检测以发现路由劫持.P_u 定义为一个三元组 $P_u=\langle I_u,O_u,L_u\rangle$.对于任意前缀 $d\in I_u$,$O_{u,d}$ 是 u 认为有资格宣告前缀 d 的自治系统集合,$L_{u,d}$ 是 u 认为有资格充当到前缀 d 的路由的下一跳 AS 的集合.给定任意前缀 x,在 P_u 中查找最相关于 x 的前缀的过程记为 $Lookup_u(x)$,该过程类似于“最长前缀匹配”,步骤如下:

(1) 若$\exists d\in I_u$ 使 $x=d$,存在精确匹配,返回 d;

(2) 若$\exists d\in I_u$ 且 $x\subset d$,即 I_u 中存在 x 的父前缀,返回具有最大前缀长度的 x 的父前缀;

(3) 若$\exists d\in I_u$ 且 $d\subset x$,即 I_u 中存在 x 的子前缀,返回具有最小前缀长度的 x 的子前缀;

(4) 返回$\varnothing$.当 $Lookup_u(x)$返回$\varnothing$时,说明 x 与 AS u 不相关.

监测器 u 从监测邻居 M_i 接收到的路由更新反映了从 M_i 去往 u 所属网络的路由及变化.为了防范路由劫持,我们主要关注两类变化:

(1) 源 AS 的变化是否合理;

(2) 下一跳 AS 的变化是否合理.

在实现上,当接收到相关于前缀 x 的路由更新 r 时,只需将该路由的源 AS 和下一跳 AS 与 $O_{u,d}$ 和 $L_{u,d}$ 对比即可(其中,$d=Lookup_u(x)$).

3.3 协同邻居选择策略

受限于计算资源、网络带宽等约束,参与者 AS 只能选取有限数量的协同邻居(假设最多只能有 K 个邻居).因此,每个参与者 AS 必须按照一定的邻居选取策略来选取协同邻居以获得最大的收益.我们主要考虑以下两种收益:安全能力和容错能力.

3.3.1 安全能力

给定监测器 v 以及和它建立了协同监测会话的 n 个监测邻居 $N_v=\{M_1,M_2,\ldots,M_n\}(n\leqslant K)$.为了测量一个 AS 参与协同监测所获得的安全能力,定义该 AS 的安全范围 S_v.S_v 是一个自治系统的集合,从 S_v 中的自治系统发起的针对于 v 的路由劫持事件都会被 v 通过协同监测网络所感知.该定义类似于之前自治系统免疫能力的定义,不同点在于:此时,v 的协同邻居会扩展 v 的感知范围.为了刻画受害者 $AS(v)$、攻击者 $AS(a)$和协同邻居 $AS(u)$三者之间的关系,我们首先定义指标函数 $\theta_{v,a,u}$.由连通性假设(假设 3)可知,在路由劫持发生前,$u\in V_{(v)}$.当路由劫持发生后,若 u 优选了攻击者 a 发起的攻击路由,即 $u\in V_{(a)}$,此时指标函数值为 1;若 u 仍优选原有的到 v 的路由,则指标函数值为 0.

$$\theta_{v,a,u}=\begin{cases}1, & u\in V_{(a)}\\ 0, & u\in V_{(v)}\end{cases} \tag{4}$$

然后,定义 u 提供给自治系统 v 的安全范围 s_v^u:

$$s_v^u=\{a\mid \theta_{v,a,u}=1,a\in V\setminus\{u,v\}\} \tag{5}$$

最后,给出 v 通过协同监测获得的安全能力,即安全范围 S_v:

$$S_v=\bigcup_{u\in N_v}\{s_v^u\} \tag{6}$$

3.3.2 容错能力

协同监测网络本身的容错能力是工程实践中很重要的考量.例如,一个自治系统希望劫持本自治系统网络的路由劫持事件至少能被 k+1 个协同邻居观察到,这样,即使在 k 个监测邻居同时失效的极端情况下,也能成功地检测到该路由劫持事件,称为 k 容错.为了衡量每个参与者构建的以自身为中心的协同监测网络的容错能力,首先定义覆盖频率 f_i,$\forall i \in S_v$,如公式(7)所示,S_v 中的自治系统 i 被 f_i 个监测邻居所贡献的安全范围所覆盖:

$$f_i = \left|\left\{M_j \mid i \in s_v^{M_j}\right\}\right| (1 \leqslant j \leqslant n) \tag{7}$$

然后,定义 AS v 建立的协同监测网络的 k 容错指数 b_k,即 v 的安全范围中覆盖频率高于 k 的 AS 所占比例:

$$b_k = \frac{|\{i \mid f_i > k, i \in S_v\}|}{|S_v|} \tag{8}$$

3.3.3 邻居选择

不同于传统 P2P 网络中邻居选择多由算法决定,本方法的参与者可以自主地选择协同邻居,施加更充分的策略控制,如选择可信度高的 AS、非商业竞争对手 AS 等.我们首先考虑以下 3 种典型的邻居选取策略:

策略 1(随机选择策略(random selection policy,简称 RSP)). 每个 AS 随机地选择参与协同的邻居,直到选择了 K 个邻居时终止.

策略 2(优选连接策略(preferential attachment policy,简称 PAP)). 每个 AS 以概率 p(p=0.7)选择当前度数最高的、尚未与自己建立协同关系的 AS,迭代至选择的邻居数达到 K 时终止.

策略 3(基于安全范围的贪心策略(secure scope based greedy policy,简称 SGP)). 每个 AS 首先计算其他 AS 相对于自身的安全范围,然后依次从高到低选择对自身安全范围贡献最大的 K 个节点.该策略需要对$\forall u \in V$计算其相对于 v 的安全范围 s_v^u,对 V 中节点,依据其安全范围的大小进行排序,最后从中选择 K 个节点.

除此之外,基于之前对 AS 自我免疫能力的分析,我们提出以下启发式策略:

策略 4(启发式策略(heuristic selection policy,简称 HSP)).

(1) 依据提供商栅栏现象,HSP 优选不在自己的提供商闭包中的 AS;

(2) AS 对路由劫持的自我免疫能力反映了 AS 接收到攻击路由的可能性,HSP 优先选择路由层次中处于较高位置的 AS,如 *Tier*1;

(3) 根据定理 1,AS 能够对自身的客户闭包、对等体的客户闭包中的 AS 发起的路由劫持免疫,因此,HSP 不选择这一类 AS 作为协同邻居;

(4) AS 路径长度是路由选择的一个重要指标,HSP 优先选择距离自己较远的 AS 作为协同邻居.当路由劫持发生时,它们优选本 AS 发起的路由的可能性更小,被攻击路由污染的概率更大.

4 安全效果评估

本节以前缀劫持为例,着重考察协同监测的安全能力,并对不同邻居选取策略下的安全效果进行横向比较.

4.1 评估方法

每个 AS 参与协同监测所获得的安全能力取决于其协同监测邻居向它贡献的安全范围.根据公式(4)、公式(5),计算安全范围的关键在于计算指标函数$\theta_{v,a,u}$.具体地,给定受害者 AS v,攻击者 AS a 和协同邻居 u,计算该指标函数需要解决以下两个问题:

(1) AS 路径预测,需要预测 v 宣告前缀 d 时,该前缀从 v 到 u 的传播路径(受害者路径),以及 a 宣告同一前缀 d 时,该前缀从 a 到 u 的传播路径(攻击者路径);

(2) 路由选择模拟,需要预测 u 在受害者路径和攻击者路径之间做出的路由选择.

问题(2)可以简化为依次优选客户路由、对等体路由、提供商路由(*GR*2)和具有更短 AS 路径长度的路由,但问题(1)中,AS 间的路径预测却是一个难题.Mao 等人在给定 AS 路径第 1 跳的情况下,仅获得了 70%~88%的准确率[19];Qiu 等人给出了预测准确率的上界是 90%[20].

为了避免路径预测引入的偏差,本评估方法使用现实存在的 AS 路径来计算受害者路径、攻击者路径和指标函数,计算过程如表 4 所示.给定 AS $v,a\in V$ 和一个 RouteViews 或 RIPE-RIS 项目的数据采集点 u,表 4 的第 2 行~第 5 行从 u 的路由表 Rib_u 中提取 v 和 a 宣告的前缀集合 D_v,D_a,以及 D_v,D_a 中的前缀到 u 的传播路径集 $P(v\to u)$ 和 $P(a\to u)$.由于一个 AS 一般拥有多个网络前缀,当 a 发起对 v 的前缀劫持时,我们假设 a 从 v 拥有的前缀中随机挑选一个(记为 d)并劫持该前缀,因此,受害者路径为 $p\in P(v\to u)$的概率(w_p)正比于 v 宣告的、以 p 为传播路径的前缀数量(第 6 行).类似地,攻击者路径为 $q\in P(a\to u)$的概率(w_q)正比于 a 宣告的、以 q 为传播路径的前缀数量(第 7 行).综上,当 a 发起针对于 v 的前缀劫持时,受害者路径和攻击者路径分别是 p 和 q 的概率可以表示为 w_pw_q,见第 8 行.第 8 行中,$Selection(p,q)$在路径 p 和 q 之间做路由选择,当优选路径 q(攻击者路径)时返回 1,否则返回 0.最后,第 9 行将临时变量 var 与预设的置信阈值 Th 进行比较,仅当 var 高于此阈值时,才认为指标函数 $\theta_{v,a,u}$=1.在本文中,我们将此阈值设定为 95%.

Table 4 Calculate indicator function $\theta_{v,a,u}$ based on RouteViews and RIPE-RIS data

表 4 基于 RouteViews 和 RIPE-RIS 路由数据计算指标函数 $\theta_{v,a,u}$

v, a, u:分别是受害者 AS、攻击者 AS、RouteViews 或 RIPE-RIS 项目的数据采集点 AS
D_v/D_a:AS v/a 宣告的前缀的集合
$P(v\to u)$/$P(a\to u)$:AS v/a 宣告的前缀从 v/a 到 u 的传播路径集合
w_p/w_q:当 v/a 宣告一个新的前缀时,u 选择、使用路径 p/q 去往该前缀的概率
var, Th:临时变量、预设置信阈值
1. Scan Rib_u to calculate D_v, D_a, $P(u\to v)$ and $P(u\to a)$ as follows:#扫描 u 的路由表并计算以下指标
2. $D_v=\{r.prefix\|r\in Rib_u\wedge r.origin=v\}$
3. $D_a=\{r.prefix\|r\in Rib_u\wedge r.origin=a\}$
4. $P(v\to u)=\{r.as\text{-}path\|r\in Rib_u\wedge r.origin=v\}$
5. $P(a\to u)=\{r.as\text{-}path\|r\in Rib_u\wedge r.origin=a\}$
6. $\forall p\in P(v\to u)$, $w_p=\|\{r\|r\in Rib_u\wedge r.as\text{-}path=p\}\|/\|D_v\|$
7. $\forall q\in P(a\to u)$, $w_q=\|\{r\|r\in Rib_u\wedge r.as\text{-}path=q\}\|/\|D_a\|$
8. $var=\sum_{p\in P(u\to v)}\sum_{q\in P(u\to a)} w_pw_qSelection(p,q)$
9. if (var>=Th) $\theta_{v,a,u}$=1, else $\theta_{v,a,u}$=0

对于任意 AS $v\in V$,通过限定 $N_v\subseteq M$(N_v 是 v 选择的协同邻居 AS 集合,M 是 RouteViews 和 RIPE-RIS 项目的数据采集点 AS 集合),基于上述方法就可以计算每个 AS $u\in N_v$ 向 v 贡献的安全范围 s_v^u,并根据公式(6)计算出 v 通过协同监测获得的安全能力 S_v.同时,根据公式(7)和公式(8)还可以计算 v 建立的协同监测网络的 k 容错指数.

4.2 数据集和数据采集点的选取

评估实验使用 2010 年 1 月 20 日 RouteViews 和 RIPE-RIS 项目发布的路由表作为数据集.当时,这两个项目共有 717 个数据采集点,我们只选取公开了整个路由表的采集点.具体地,只有当其路由表包含超过 300 000 个前缀时,我们才认为该数据采集点公开了整个路由表,共得到 224 个这样的采集点.在去除数据采集点之间的冗余,例如同一个 AS 可能会同时向 RouteViews 和 RIPE-RIS 项目提供数据,我们最后一共得到了 113 个有效的数据采集点 AS,包含 14 个 *Tier*1,90 个 *Transit* 和 9 个 *Stub*.

4.3 实验结果

在实验部分,我们首先验证协同监测机制取得的安全效果;然后,通过考察各种邻居选择策略下参与者 AS 获得的安全范围、1-容错指数、选择的邻居节点的度数.我们对 4 种邻居选择策略进行了比较.

4.3.1 安全效果

理论上,协同监测能够改善参与者 AS 对前缀劫持的免疫能力.为了验证改善效果,我们从 113 个数据采集点 AS 中随机选取若干个 AS 作为一组(采用 RSP 策略),然后计算这些 AS 两两之间建立协同关系后对前缀劫持的免疫能力.对于每个特定的成员数量,我们将这个过程重复 1 000 遍,并在图 7 中展示了这些 AS 参与协同监测之前和之后免疫能力的平均值/标准差.如图 7 所示,参与协同监测之前,AS 对前缀劫持的免疫能力接近于 0.相比之下,协同监测组即使只包含 5 个 AS,也能使免疫能力增强到 60%以上.此外,协同监测提供的安全能力的

平均值/标准差随着协同监测组中成员数量的增长而提高/减小,但这种提高/减小在组中成员数量超过 40 以后变得不明显.这种现象表明,部署者 AS 只需要与一小部分 AS 建立协同关系,就可以达到较好的免疫效果.

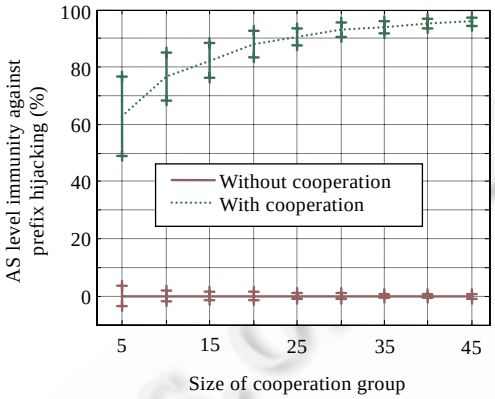

Fig.7 Size of secure scope per member

图 7 协同检测成员获得的平均安全能力

4.3.2 安全范围

协同监测方法为参与者提供的安全范围的大小是最重要的安全指标.如图 8 所示,在邻居数较少(*K* 值较小)的情况下,SGP 和 HSP 具有显著的优势.随着 *K* 值的增加,4 种策略的差距逐渐缩小.当 *K* 达到 25 时,RSP,PAP,SGP,HSP 产出的安全范围的平均大小分别是 29 037(85.4%),31 018(91.2%),32 715(96.2%)和 32 792(96.4%).这也意味着,一个监测器仅仅选择 25 个 AS 并与之建立协同关系,就可以使自身对路由劫持的免疫力达到 95%以上.当 *K* 超过 40 之后,4 种策略所提供的安全范围的差别已经很小,说明协同网络的构建在邻居数较多的情况下,其效果并不依赖于节点选择策略,在部署实践中具有较强的操作性.

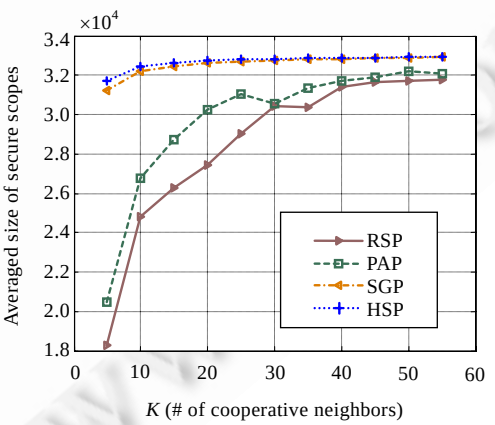

Fig.8 Average size of secure scope as *K* increases

图 8 不同 *K* 值和策略下安全范围的平均值

4.3.3 1-容错指数

对 4 种策略下的 1-容错指数的评估如图 9 所示.与图 8 一样,SGP 和 HSP 策略表现最好,随后是 PAP 策略,RSP 策略表现最差.虽然 HSP 策略在安全范围方面的表现略好于 SGP 策略,但两者在 1-容错指数方面的表现基本相同.在 *K*=25 时,4 种策略下的 1-容错指数分别是 82.1%,89.4%,96.2%和 96.2%.当 *K* 超过 25 之后,1-容错指数的增长开始放缓.如果采用 SGP 或 HSP 策略,在 *K*=25 时即可达到比较满意的容错水平.

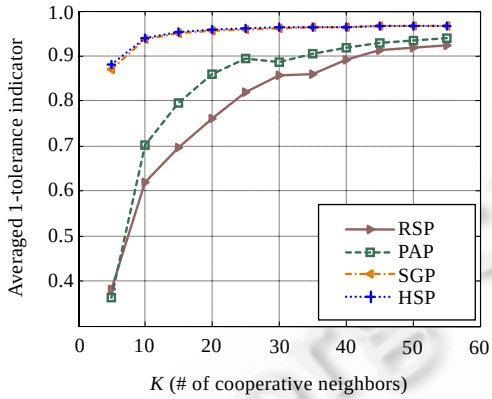

Fig.9 Average b_1 level as K increases

图 9 不同 K 值和策略下的平均 1-容错指数

4.3.4 邻居节点的度数

直观上,协同主要在规模相近的运营商之间发生.本文使用各种策略下所选取的邻居节点的平均度数来衡量 AS 间进行协同的难易程度,如图 10 所示.PAP 策略偏好于度数最大的节点,因此选取的邻居节点也具有最大的平均度数,紧接着的是 SGH 和 HSP 策略,RSP 策略产出的拓扑中邻居节点的平均度数最低.同时也注意到,随着 K 的增大,除 RSP 之外的其他 3 种策略所选择的邻居节点的平均度数迅速减少.这是因为除 RSP 之外的 3 种策略虽然着眼点不同,但为了通过选取有限数量的邻居达到最大效益,都倾向于选择连通性较好的自治系统作为监测邻居,产生了类似于 PAP 策略的效果.

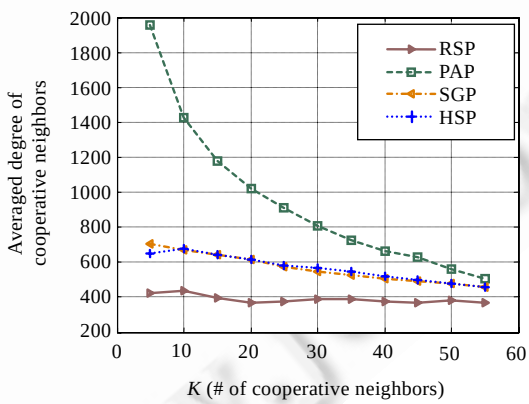

Fig.10 Average degree of partners as K increases

图 10 不同 K 值和策略下所选择协同邻居节点的平均度数

虽然 SGP 和 HSP 策略的效果相似,但 HSP 策略的复杂度远低于 SGP 策略,因而具有更好的实用性.

5 相关工作和展望

路由监测是防范路由劫持的一类重要方法.不同于对 BGP 安全模型的研究[27],监测方法不依赖于全网范围内的 PKI 体系,无需修改 BGP 协议,且容易增量部署,近年来得到了学术界的广泛关注.路由监测具体分为对控制平面的监测[28]、对数据平面的监测[29]以及对数据平面和控制平面的联合监测[30]:

- 对控制平面进行监测开销较小,但面临着 3 个方面的问题:

  - 一是监测效果受限于数据采集点的数量和覆盖范围[31].运营商出于保护商业隐私的考虑,很少有AS 愿意无条件地公开自己的 BGP 数据.如本文实验部分中,绝大多数 RouteViews 和 RIPE- RIS 的采集点都仅公开了部分路由数据;
  - 二是对控制平面的监测多采用集中式部署,需要用户主动注册网络前缀-源 AS 的对应关系[28],对路由劫持的检测效果取决于注册数据的时效性和准确性;
  - 三是在路由劫持发生时,由于受害者网络已不可达,该类方法还面临着如何通知受害者的困局.

  本文方法也属于控制平面的监测机制,参与协同的 AS 互为监测数据的来源,并直接受益于协同行为,解决了路由监测中数据难于获取的问题.每个参与者 AS 独立地检测针对所属网络的路由劫持,避免了第三方难以区分正常路由变化和路由劫持的问题;而且对路由劫持的检测在本地进行,也避免了路由劫持时的通信困局;
- 对数据平面的监测多从运营商本身的角度出发,如 iSPY[29],不依赖于实时的 BGP 数据,易于部署,但所依赖的 Ping,Traceroute,TCP Ping 等手段也是网络攻击的基本手段,常被运营商视为威胁而被阻塞;其次,该类机制需要周期性、持续性地探测 Internet,会消耗较多的网络带宽;最后,该类机制具有较高的误检率和漏检率,可用性有待改善;
- 对数据、控制平面联合监测的方法兼具两者的优点和缺点,开销较大,只适合于对少数重点网络进行监测.

参与协同监测的 AS 在互利互惠的基础上对 BGP 路由的可信性进行分析,能够克服 BGP 路由中单个 AS 的视图局部性问题.网络运营商是极端重视隐私的群体,如何在开展协同获得较高安全能力的同时保护运营商的隐私,是协同监测迫切需要解决的问题,也是协同监测能否走向应用的关键.在这个方面,Harlan 等人设计了一种根据其他 AS 的投票结果评价路由信息可信性的机制[32],该机制只要求参与者 AS 回答“是”或“否”,就能够较好地保护参与者的隐私.但该方法只能给出统计意义上的结论,准确率值得商榷;且该方法不能直接用于检测路由劫持,需要引入另外的检测机制.Goodell 等人提出的 IRV 方法具有和本文方法类似的结构,每个参与者 AS 需要在域内设立 IRV 服务器,回答其他 AS 发送来的路由验证请求,并根据本地路由策略、网络拓扑等对给定路由的真实性进行判断和回答[33].在这种协同方式下,参与者 AS 需要向外界暴露较多的策略信息.以上两种方法均未对查询请求的范围进行限制,因此很容易被用来实现一些恶意的目的.例如,通过大量、反复的查询,推断目标 AS 的直接邻居.本文方法中,每个 AS 只向协同邻居请求相关于所属网络的路由变化,并不要求其他参与者 AS 直接暴露自己的路由策略、网络拓扑等隐私信息,是一种更合理的协同策略.此外,每个参与者所暴露的路由信息以多个片段的形式分布在不同的协同邻居之间,外界难以推断参与者的路由策略.国内学术界也对通过在 AS 之间引入协同机制防范路由劫持进行了一些研究.例如,刘欣等人设计了专用于检测前缀劫持的协作监测机制[34],但该方法需要在参与者之间使用新的协议机制,且不能检测下一跳劫持.胡宁等人设计了协同监测下的信息共享机制,但并未涉及对路由异常的监测[35].

本文方法也存在一定的局限性.协同监测网络是建立在 Internet 之上的层叠网,因此也继承了这一类层叠网所面临的一系列问题[36],如层叠网本身的安全性问题,在以后的工作中需要进一步改进和完善.

致谢 在此,我们向对本文提出宝贵修改意见的评审老师和同行表示衷心的感谢!

References:

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

[2] Ramachandran A, Feamster N. Understanding the network-level behavior of spammers. In: Proc. of the ACM SIGCOMM 2006. Pisa: ACM Press, 2006. 291–302. [doi: 10.1145/1159913.1159947]

[3] Nordstrom O, Dovrolis C. Beware of BGP attacks. SIGCOMM Computer Communication Review, 2004,34(2):1–8. [doi: 10.1145/997150.997152]

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

[5] RIPE-NCC, YouTube hijacking: A RIPE NCC RIS case study. http://www.ripe.net/news/study-youtube-hijacking.html

[6] Murphy S. BGP security vulnerabilities analysis. RFC 4272, 2006.

[7] Cooperative Association for Internet Data Analysis. AS relationships. http://as-rank.caida.org/data/

[8] Muhlbauer W, Feldmann A, Maennel O, Roughan M, Uhlig S. Building an AS-topology model that captures route diversity. In: Proc. of the ACM SIGCOMM 2006. Pisa: ACM Press, 2006. 195−206. [doi: 10.1145/1159913.1159937]

[9] Griffin TG, Shepherd FB, Wilfong G. The stable paths problem and interdomain routing. IEEE/ACM Trans. on Networking, 2002, 10(2):232−243. [doi: 10.1109/90.993304]

[10] Griffin TG, Wilfong G. An analysis of BGP convergence properties. SIGCOMM Computer Communication Review, 1999,29(4): 277−288. [doi: 10.1145/316194.316231]

[11] Gao LX. On inferring autonomous system relationships in the Internet. IEEE/ACM Trans. on Networking, 2001,9(6):733−745. [doi: 10.1109/90.974527]

[12] Gao LX, Rexford J. Stable Internet routing without global coordination. IEEE/ACM Trans. on Networking, 2001,9(6):681−692. [doi: 10.1109/90.974523]

[13] Goldberg S, Schapira M, Hummon P, Rexford J. How secure are secure interdomain routing protocols. In: Proc. of the ACM SIGCOMM 2010. New Delhi: ACM Press, 2010. 87−98. [doi: 10.1145/1851182.1851195]

[14] University of Oregon route views project. http://www.routeviews.org/

[15] Routing information service (RIPE-RIS). http://www.ripe.net/data-tools/stats/ris/routing-information-service

[16] Zhao XL, Pei D, Wang L, Massey D, Mankin A, Wu SF, Zhang LX. An analysis of BGP multiple origin AS (MOAS) conflicts. In: Proc. of the 1st ACM SIGCOMM Workshop on Internet Measurement. San Francisco, 2001. 31−35. [doi: 10.1145/505202.505207]

[17] Oliveira R, Zhang BC, Zhang LX. Observing the evolution of internet AS topology. In: Proc. of the SIGCOMM 2007. Kyoto: ACM Press, 2007. 313−324. [doi: 10.1145/1282380.1282416]

[18] Oliveira R, Pei D, Willinger W, Zhang BC, Zhang LX. The (in)completeness of the observed Internet AS-level structure. IEEE/ACM Trans. on Networking, 2010,18(1):109−122. [doi: 10.1109/tnet.2009.2020798]

[19] Mao ZM, Qiu L, Wang J, Zhang Y. On AS-Level path inference. In: Proc. of the 2005 ACM SIGMETRICS Int'l Conf. on Measurement and Modeling of Computer Systems. Banff: ACM Press, 2005. 339−349. [doi: 10.1145/1064212.1064257]

[20] Qiu J, Gao LX. AS path inference by exploiting known AS paths. In: Proc. of the IEEE Global Telecommunications Conf. San Francisco, 2006. 1−5. [doi: 10.1109/glocom.2006.27]

[21] Rexford J, Wang J, Xiao Z, Zhang Y. BGP routing stability of popular destinations. In: Proc. of the 2nd ACM SIGCOMM Workshop on Internet Measurment. Marseille: ACM Press, 2002. 197−202. [doi: 10.1145/637201.637232]

[22] Alexa top 500 global sites. http://www.alexa.com/topsites

[23] Google public DNS. http://code.google.com/intl/zh-CN/speed/public-dns/

[24] OpenDNS. http://www.opendns.com

[25] Whois lookup. http://www.whois.net

[26] Heffernan A. Protection of BGP sessions via the TCP MD5 signature option. RFC 2385, 1998.

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

[28] Lad M, Massey D, Pei D, Wu Y, Zhang BC, Zhang LX. PHAS: A prefix hijack alert system. In: Proc. of the 15th Conf. on USENIX Security Symp. Vancouver: USENIX Association, 2006. 153−166.

[29] Zhang Z, Zhang Y, Hu YC, Mao ZM, Bush R. Ispy: Detecting ip prefix hijacking on my own. In: Proc. of the ACM SIGCOMM 2008. Seattle: ACM Press, 2008. 327−338. [doi: 10.1145/1402958.1402996]

[30] Hu X, Mao ZM. Accurate real-time identification of IP prefix hijacking. In: Proc. of the 2007 IEEE Symp. on Security and Privacy. Oakland: IEEE Computer Society, 2007. 3−17. [doi: 10.1109/sp.2007.7]

[31] Zhang Y, Zhang Z, Mao ZM, Hu C, Maggs BM. On the impact of route monitor selection. In: Proc. of the 7th ACM SIGCOMM Conf. on Internet Measurement. San Diego: ACM Press, 2007. 215−220. [doi: 10.1145/1298306.1298336]

[32] Harlan Y, Rexford J, Felten EW. A distributed reputation approach to cooperative Internet routing protection. In: Proc. of the 1st IEEE ICNP Workshop on Secure Network Protocols. Boston: IEEE, 2005. 73−78. [doi: 10.1109/NPSEC.2005.1532057]

[33] 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 Network & Distributed System Security Symp. 2003.

[34] Liu X, Zhu PD, Peng YX. Co-Monitor: Collaborative monitoring mechanism for detecting prefix hijacks. Ruan Jian Xue Bao/Journal of Software, 2010,21(10):2584−2598 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3657.htm [doi: 10.3724/sp.j.1001.2010.03657]

[35] Hu N, Zhu PD, Zou P. Information sharing mechanism for inter-domain routing cooperative monitoring. Ruan Jian Xue Bao/Journal of Software, 2011,22(3):481−494 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3734.htm [doi: 10.3724/sp.j.1001.2011.03734]

[36] Wang YY, Bi J, Wu JP. Research on Internet overlay routing.Ruan Jian Xue Bao/Journal of Software, 2009,20(11):2988−3000 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3603.htm [doi: 10.3724/sp.j.1001.2009.03603]

附中文参考文献:

[34] 刘欣,朱培栋,彭宇行.Co-Monitor:检测前缀劫持的协作监测机制.软件学报,2010,21(10):2584−2598. http://www.jos.org.cn/1000-9825/3657.htm [doi: 10.3724/sp.j.1001.2010.03657]

[35] 胡宁,朱培栋,邹鹏.域间路由协同监测中的信息共享机制.软件学报,2011,22(3):481−494. http://www.jos.org.cn/1000-9825/3734.htm [doi: 10.3724/sp.j.1001.2011.03734]

[36] 王旸旸,毕军,吴建平.互联网覆盖路由技术研究.软件学报,2009,20(11):2988−3000. http://www.jos.org.cn/1000-9825/3603.htm [doi: 10.3724/sp.j.1001.2009.03603]

王小强(1985－),男,湖北荆门人,博士生,主要研究领域为新一代互联网体系结构,路由安全.
E-mail: wangxiaoqiang@nudt.edu.cn

朱培栋(1971－),男,博士,教授,博士生导师,主要研究领域为互联网路由,网络安全.
E-mail: pdzhu@nudt.edu.cn

卢锡城(1946－),男,教授,博士生导师,中国工程院院士,主要研究领域为计算机网络,分布式计算.
E-mail: xclu@nudt.edu.cn