

基于控制平面精微操作的域间流量牵引方法

罗文杭, 费金龙, 陈 迪

(信息工程大学, 河南 郑州 450001)

摘要: 针对现有域间流量牵引手段高度依赖人工经验且难以兼顾控制精度与收敛稳定性的问题, 提出一种基于控制平面精微操作的域间流量牵引方法, 据此设计以策略组合为核心架构的域间流量牵引规划框架。该方法分为路径优选和传播抑制两个阶段, 其中路径优选基于拓扑与策略感知动态生成最优牵引路径实现流量精准引导; 传播抑制通过约束路由更新传播范围限制路由信息的非必要传播, 从而消除路由表膨胀与冗余路径探索。在此基础上构建了域间流量牵引规划框架, 根据牵引目标得到满足无环和商业合规约束的 BGP(Border Gateway Protocol)策略集合。基于实体路由器环境的实验表明, 所提方法在不同的牵引距离下均能平滑收敛且无异常抖动, 相较 AS(Autonomous System)路径预置和子前缀通告在成功率、收敛时间和影响范围上更优。

关键词: 边界网关协议; BGP 团体属性; 流量工程; 网络通信

中图分类号: TP393.08

文献标识码: A

文章编号: 1671-0673(2026)02-0239-07

A Control-Plane Fine-Grained Inter-Domain Traffic Steering Method

LUO Wenhong, FEI Jinlong, CHEN Di

(Information Engineering University, Zhengzhou 450001, China)

Abstract: Aiming at the limitations that existing inter-domain traffic steering methods, heavily rely on manual experience and struggle to balance control precision with convergence stability, an inter-domain traffic steering method based on fine-grained control-plane operations is proposed, and a planning framework with policy combination as its core architecture is accordingly designed. The method is divided into two stages: path optimization and propagation suppression. In the path optimization stage, the optimal steering path is dynamically generated based on topology and policy awareness to achieve precise traffic guidance. In the propagation suppression stage, the propagation scope of routing updates is constrained to limit unnecessary dissemination of routing information, thereby eliminating routing table inflation and redundant path exploration. On this basis, an inter-domain traffic steering planning framework is constructed, which derives a set of BGP policies that satisfy loop-free and business-compliance constraints for a given steering objective. Experiments conducted in a physical router environment demonstrate that the proposed method achieves smooth convergence without abnormal jitters under different steering distances, and superior performances are observed compared to those of AS-path prepending and sub-prefix announcement in terms of success rate, convergence time, and impact scope.

Key words: border gateway protocol; BGP communities; traffic engineering; networking

边界网关协议(Border Gateway Protocol, BGP)^[1], 是互联网核心路由架构的事实性标准协议, 承担不同自治系统(Autonomous System, AS)间可达性宣告的执行与路径的抉择, 直接影响流量轨迹和全局路由收敛^[2]。BGP 运行基于信任机制, 但其内生性安全验证机制的缺失, 致使其长期面临路由劫持、前缀伪造等安全风险。在域间网络中, 域间流量牵引技术具有重要价值^[3], 既可用于前述威胁的缓解手段, 也是运营商执行备份链路负载均衡、处置突发流量黑洞、实施 DDoS 流量清洗^[3], 以及保障服务等级协议^[4]的核心技术支撑。

目前, 业界普遍采用的域间流量牵引技术主要包括 AS 路径预置、子前缀通告以及利用预定 BGP 团体属性进行调控等^[4-5]。这些技术虽然被广泛部署, 其固有局限却不能忽视: AS 路径预置对入站流量的调控粒度较粗, 且没法越过目标的结构性路径倾向^[6]; 子前缀宣告能实现精准的域间流量牵引, 但会加剧全球路由表的膨胀并扩大路由更新的传播范围^[7]; 利用预定义 BGP 团体属性进行调控的功能比较丰富、用法比较灵活, 实际利用时却常受限于策略协调与标准化程度; Birge-Lee 等^[8]提出的 SICO 框架使用 BGP 团体属性实现了精细域间流量操纵, 其牵引流程却高度依赖人工试探和对网络策略细节的先验认知, 缺乏对路径可达性、商业合规性及全局收敛稳定性的保障。总体而言, 现有手段的运作高度倚重人工经验的介入, 自动化程度低, 且难以在达成目标(如 DDoS 流量清洗或故障路径规避^[9])的同时, 有效规避服务中断与收敛延迟等衍生副作用^[10-11]。

针对上述局限, 本文提出一种能够实现精确控制影响范围的域间流量牵引方案。该方法的核心思路在于, 首先对 BGP 的路由决策机理进行系统分析, 结合 AS 层级拓扑与路由策略意图(策略感知), 并利用 BGP 团体属性作为执行策略的手段, 从而构建一个“感知—决策—执行”的控制框架。

本文主要工作包括如下 3 点。

1) 提出一种基于控制平面精微操作的域间流量牵引方法, 能够对网络拓扑和路由策略进行双重感知, 将 AS 间商业关系、拓扑层级等结构信息与细粒度的策略意图相结合, 实现比传统方法影响范围更可控、调控目标更精确的流量引导。

2) 构建基于控制平面精微操作的域间流量牵引方法的策略组合规划与配置自动生成规划框架, 能够将流量牵引的特定目标自动转化为可执

行的 BGP 路由策略配置, 降低人工操作的不确定性、复杂性及由此引发的收敛延迟风险。

3) 搭建基于实体路由器的真实域间路由骨干网络环境, 验证了该方法在实现精准流量牵引目标的同时, 能有效减少路由更新扰动、避免路由表膨胀和冗余路径探索, 并显著提升域间流量控制与调度的有效性和自动化水平。

1 基础知识

1.1 边界网关协议

BGP 属于路径矢量路由协议, 通过传播目的前缀的可达性与路径属性, 让路由器能形成一个全网范围的域间拓扑与可达关系的认知, 从而支持跨 AS 的路由转发与策略控制。

当路由器接收到多条指向同一前缀的路径时, BGP 先按最长前缀匹配, 再依据属性选择: AS 路径用于环路检测, 本 AS 编号一旦出现, 路径将被直接丢弃。本地优先级在出口选择中权重更高, 以体现策略。若优先级相同, 则选比 AS 路径更短的路径^[6]。以上构成了 BGP 稳定运行的核心基础。

1.2 自治系统与商业关系

互联网由众多自治系统通过 BGP 进行域间路由互联, 其路由策略受 AS 间商业关系约束。AS 关系通常抽象为两类: 提供商—客户关系与对等关系。

在提供商—客户关系中, 客户付费获取转发服务, 并向所有邻居通告自身及从上游学到的路由; 提供商则仅将客户路由通告给其客户或对等体, 避免向上游传播。在对等关系中, 双方免费交换流量, 路由传播更为谨慎, 一般只向下游客户通告。此类传播行为符合 Gao-Rexford 原则与无谷(No-Valley)^[12]原则, 在实践中有效维持了域间路由的稳定性。

1.3 BGP 团体属性

BGP 团体属性是一种可传递的路径属性, 用于对路由进行标记与分组, 以简化策略配置, 可跨 AS 传播, 但传递范围取决于中间 AS 是否保留该属性。标准团体属性采用 32 位编码, 格式为 AS_number: Value, AS_number 标识管理域, Value 承载分类或动作语义。其核心作用是对路由进行分类标记, 而动作型语义通常由运营商本地约定, 用于触发如优先级调整、传播控制等行为。扩展团体属性在编码长度上有所扩展, 可携带更丰富的结构化信息, 支持如 VPN 标识等更复杂的策略语义。

2 跨域流量牵引实现原理

2.1 问题定义与基本假设

考虑两个正在进行正常通信的自治系统:源AS(记作 AS_s)与目的AS(记作 AS_d),目标前缀归属于 AS_d 。正常情况下, AS_s 至目标前缀的数据流沿原始域间路径转发。在不影响端与端之间通信语义的前提下,考虑是否可以引入第3方可控AS(记作 AS_c)作为稳定中转节点,将流量牵引至经由该 AS_c 的新路径。

该方法的目标是在不修改源自治系统 AS_s 与目的自治系统 AS_d 归属关系以及端到端通信语义的前提下,利用处于第3方的可控的牵引 AS_c 对跨域路径竞争关系进行精细调节,使源 AS_s 到目的 AS_d 的业务流量偏向经过 AS_c 的指定中转路径。

本文方法满足以下设计约束:不要求修改其本地路由策略;不依赖跨域隧道或覆盖网络;仅假

设 AS_c 具备常规多目的连接能力,并可对其边界路由器配置出站策略;假设所需BGP团体属性语义可通过运营商公开策略文档或对接协商获得。

2.2 方法介绍

本文方法的本质在于, AS_c 通过在BGP路由宣告中附加特定的BGP团体属性,对 AS_s 到 AS_c 的路径P上的AS实施远程策略控制。该机制通过以下两个维度的协同操作实现。1)路径优选:最大化路径P对 AS_s 的吸引力。2)传播抑制:严格限定路由信息的传播边界,防止非预期扩散和路由环路,保障全网路由稳定性。

如图1所示,假设已选定了一条合法的引流路径P,表示为序列 $AS_s \rightarrow AS_{x1} \dots \rightarrow AS_c \rightarrow AS_{y1} \dots \rightarrow AS_d$ 。 AS_c 将在向其直接上游邻居(即路径P上的下一跳节点)宣告到目标前缀的路时,附加一组复合BGP团体属性指令。这些指令将沿路径P传播并触发沿途AS执行相应的路由策略。

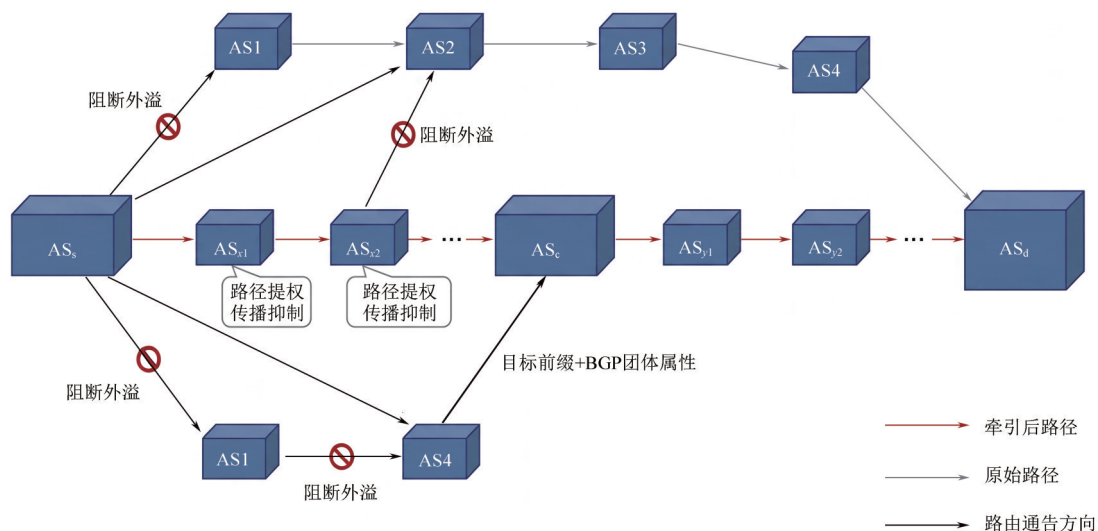


图1 基于控制平面精微操作的域间流量牵引场景示意图

1) 路径优选

为确保在路径P的每一个路由决策点,流向 AS_c 的方向始终被选为最优出口,本文方法利用BGP选路原则中优先级最高的属性——本地优先级进行干预。尽管该属性仅在自治系统内部生效,但多数ISP(Internet Service Provider)及IXP(Internet Exchange Point)允许下游客户通过预定义的BGP团体属性远程设定对应路由的本地优先级值。

操作时,向通往特定上游AS的路由宣告中添加映射到高优先级的团体属性(如Community- AS_{xi} : higher local Preference)。当接收到带此标签的路由时,对端路由器将根据入站策略将其本地优先级提升至预定高值。由于默认路由优先级通常较

低,经提权的路径将在本AS胜出,且此优势会沿路径逐跳向上传递,形成级联效应,从而保证整条路径在竞争中持续保持最优状态。

2) 传播抑制

为防止路由泄露导致的路由环路或对非目标网络的非预期影响,须将路径P的传播严格限制在预期拓扑范围内。所以,本文控制 AS_c 在宣告中附加限制传播范围的团体属性,如标准的传播抑制(NO_EXPORT)属性。

传播抑制要求接收AS仅在本AS内传播该路由,禁止向任何eBGP邻居转发。这样发布的路由通告可阻断经对等链路的非必要扩散,并防止路由回流至下行提供商而导致黑洞或环路,从而将

引流影响限定在 AS_s 到 AS_d 的路径范围内,对互联网其余部分保持透明。

综上所述,通过组合使用“路径提权”与“传播抑制”策略, AS_s 将接收到一条经过特殊工程处理的、具备高优先级的路由通告,从而将发往 AS_d 的流量主动牵引至 AS_c ,且该过程不会破坏 AS_c 自身的出站路径及网络其余部分的连通性。

3 跨域流量牵引策略规划框架

在基于控制平面精微操作的跨域流量牵引方

法基础上,为提升其可部署性与自动化水平,本文进一步提出一个以策略组合为核心的规划框架。该框架系统整合了前述方法,并提供了完整的实现架构。

该框架如图2所示,核心流程包含3个阶段:1)转发路径确定,确定牵引操作的安全底线,防止网络阻断;2)引流路径构造与筛选,在网络拓扑中搜索符合商业关系的候选路径;3)策略组合与配置文件生成下发,生成包含路径提权与传播抑制功能的BGP团体属性策略集合,并下发至物理网络。

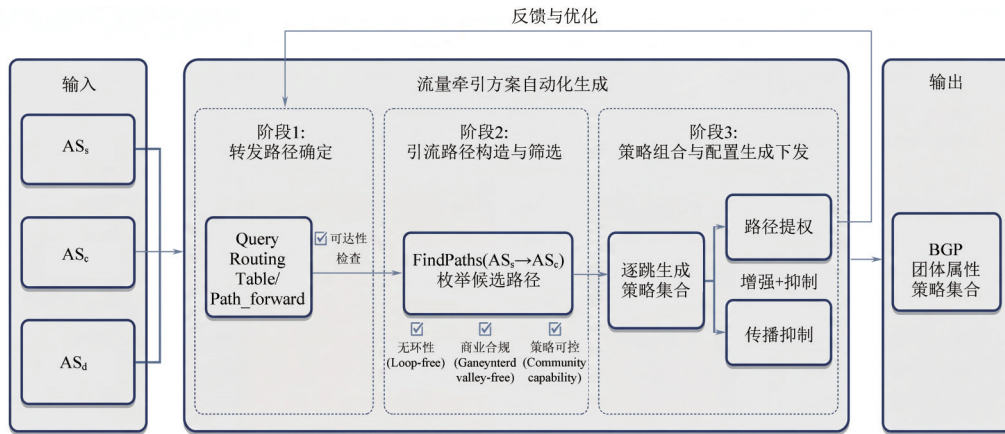


图2 基于策略组合的域间流量牵引规划框架

本框架的核心逻辑通过“精准流量牵引策略生成算法”实现。该算法输入 AS_s 、 AS_c 、 AS_d 及网络状态知识,输出可部署的BGP团体属性策略集合 π 。具体逻辑如算法1所示。

算法1 精准流量牵引策略生成

输入:源 $AS(AS_s)$ 、牵引 $AS(AS_c)$ 、目的 $AS(AS_d)$

输出:可部署的BGP策略 π

1. //阶段1:转发路径确定
2. $Path_forward = QueryRoutingTable(AS_c, AS_d)$; //确定 AS_c 到 AS_d 的实际优选路径
3. (Path_forward is NULL) return FAILURE;
//若无可达路径,则操作中
4. //阶段2:引流路径的构造与筛选
5. $Candidate_Paths = FindPaths(AS_s, AS_c)$;
//枚举源到牵引节点的所有物理路径
6. $st_Path = Select(Candidate_Paths)$ where:
7. Constraint A: Is Loop Free(Path + Path_forward); //无环性检查
8. Constraint B: Is Valid(Path, Gao-Rexford);
//商业关系传播合法性
9. Constraint C: Has community Capability(Path);
//具备策略操控能力
10. //阶段3:策略组合与配置文件生成合成与下发

11. Strategy $\pi = Empty$;
12. Current_Node = AS_c ;
13. While (Current_Node != AS_s) {
14. Next_Hop = GetNextHop(Best_Path, Current_Node);
15. //合成增强指令:路径提权
16. Comm_Enhance = Generate community (Next_Hop, ACTION_RAISE_LOCAL_PREF);
17. //合成抑制指令:传播抑制功能,限制传播范围,保护转发路径并避免副作用
18. Comm_Suppress = Generate community (Next_Hop, ACTION_NO_PEER/NO_EXPORT);
19. $\pi.append(\{Target: Next_Hop, Communities: [Comm_Enhance, Comm_Suppress]\})$;
20. Current_Node = Next_Hop;
21. }
22. Return π ;

上述算法的设计逻辑可概括为“先保可达、再保可选、后保可控”。

首先,通过查询 AS_c 到 AS_d 当前的转发路径 $Path_forward$,确认 AS_d 对 AS_c 可达;若本身不可达,算法直接返回失败,以避免黑洞风险。

其次,算法在 AS_s 到 AS_c 之间枚举候选路径并选择引流路径 $Path_divert$ 。不同于一般最短路径搜

整体稳定性。

AS6到AS4间的转发路径用于承接牵引后的转发。在此基础上,需要在AS1到AS6之间构造1条可传播且可控的引流路径。结合拓扑与商业关系约束,选定的引流路径为:AS1 → AS5 → AS6。该路径呈逐跳c2p“上升”结构,满足无谷约束,因此在现实BGP导出策略下具备传播基础;同时,路径节点具备BGP团体属性,为后续策略合成与影响范围控制提供了实施条件。

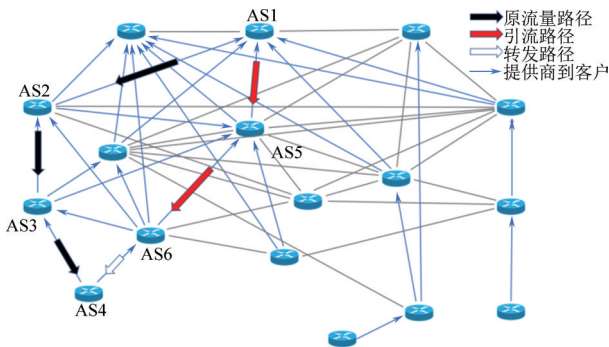


图4 域间流量牵引示例

为了使目标流量在AS1侧能够稳定选择经由AS5 → AS6的路径,本文采用“选路增强+传播抑制”的策略组合。

一方面,通过在宣告通往AS4的路由上附加可映射为“提高本地优先级”的BGP团体属性,实现引流路由在决策过程中的优先级提升。在面向AS1与AS5的策略中分别触发相应的提权标签(例如,AS5:higher localpref与AS1:higher localpref)。在该配置生效后,引流路由在AS1及AS5选择中获得稳定优势,从而实现对特定源到特定目的流量的定向牵引。

另一方面,为避免引流路由经由对等链路无序扩散并引发路由泄露或回流风险,需要在路径的关键节点施加传播抑制策略。在AS1等存在侧向互联的节点处附加NO_EXPORT类BGP团体属性(例如AS1:NO_EXPORT,具体值依运营商社区约定而定),将传播限制在接收AS内部。

通过上述限制,可将策略影响范围压缩在预期拓扑内,从而降低对互联网其他区域的扰动并提升部署的安全性。

4.4 AS_s到AS_c的AS跳数与收敛时间的变化趋势

为验证牵引路径增长时收敛过程的稳定性,在满足无谷原则且支持属性传播的拓扑中,固定其他条件,仅调整AS_s至AS_c的AS跳数 h (取1、2、3)。每组实验均在 t_0 时刻触发牵引,并持续发送业务流量以同步观测控制面与数据面变化。每组

重复50次,取平均值。该方法在不同路径长度下的收敛稳定性与可控性趋势如图5所示。

从图5可得,随着AS_s到AS_c的AS跳数 h 从1增加到3,控制面收敛时间 T_{cp} 与数据面切换时间 T_{dp} 都呈单调上升趋势,整体增长较为平滑,没有出现抖动或异常突增,说明牵引路径变长后系统仍保持良好的稳定性。

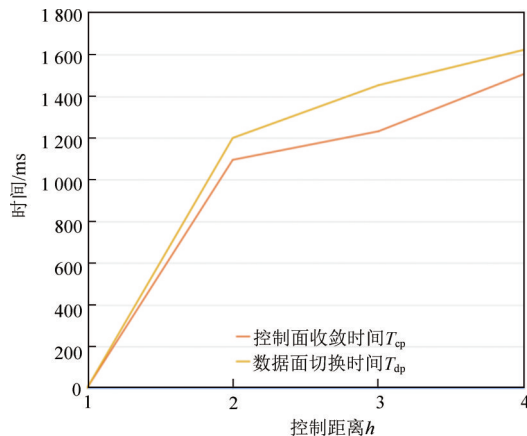


图5 AS_s到AS_c的AS跳数 h 与收敛时间的变化趋势

在各个 h 场景下, T_{cp} 与 T_{dp} 的数值始终接近,且曲线趋势一致,表明控制面路由收敛与数据面切换之间不存在明显的不同步现象,牵引生效过程具有较好的可控性。

当 h 从1增加到2、3时, T_{cp} 与 T_{dp} 仅表现出近似线性的小幅增加,未随路径长度增加而指数放大,说明本文方法对路径长度变化不敏感,对多跳牵引场景具有较好的扩展性。

综合分析,在满足无谷原则且允许路由属性传播的前提下,本文牵引机制均能在可接受时间内实现控制面与数据面协同收敛,充分验证了其在收敛稳定性和时延可控性方面的有效性。

4.5 对比实验

在相同拓扑与相同业务目标前缀下,本文进一步将所提方法与两类典型域间流量工程手段进行对比:AS路径预置与子前缀通告。其中,AS路径预置通过在更高优先级的备选路径上进行AS路径长度扩展以降低其可选性,从而使引流路径成为优选;子前缀通告则通过在AS_c上宣告更精确前缀,利用最长前缀匹配吸引到达该前缀的流量。对比评估从牵引是否成功(源端流量是否稳定切换至目标路径)、收敛时间(T_{cp} 、 T_{dp})以及影响扩散范围 s 等3个方面展开,实验结果如表1所示。

从表1可见,AS路径预置在本地优先级处于劣势时难以实现牵引。子前缀通告虽能牵引,但

因宣告更精确前缀易吸引全网流量,影响范围较大。相比之下,本文方法在较短 T_{cp} 与 T_{dp} 下即可完成牵引,且对非目标区域的路由更新影响近乎为零。本文基于实体路由器构建物理测试环境,从跳数变化和对比两个维度评估所提跨域精准流量

牵引方法。实验结果表明,该方法在牵引路径变长时仍能稳定收敛,并在牵引成功性、收敛速度及影响扩散范围方面优于典型传统方案,能够在不引入路由震荡的前提下实现可重复、可观测的精准流量牵引。

表 1 对比实验结果汇总表

方法	牵引是否成功	影响扩散范围 $s/\%$	T_{cp}/ms	T_{dp}/ms	备注
AS 路径预置	否	33.3	6 233	7 488	AS 路径预置只能造成 AS 路径的变化,当本地优先级处于劣势时无法起效
子前缀通告	是	85.71	17 662	22 553	宣告的前缀对全网可见,会吸引所有到达该前缀的流量
本文方法	是	0	1 278	1 425	能够精准快速地牵引流量且不会影响别的链路状态

5 结束语

针对域间流量牵引中精准控制与稳定收敛难以兼顾的问题,本文提出一种基于控制平面精微操作的域间流量牵引方法。该方法深度融合 BGP 选路机制与 AS 商业关系约束,通过组合“路径提权”与“传播抑制”策略,并利用 BGP 团体属性实现流量的精确引导与影响范围控制。所构建的规划框架具备对路径异常与策略兼容性的基本容忍能力。实验结果表明,该方法能在不引起路由振荡的前提下实现跨域精准牵引,并有效控制策略影响范围。

参考文献:

[1] LI Q, LIU J J, HU Y C, et al. BGP with BGPsec: attacks and countermeasures[J]. IEEE Network, 2019, 33(4): 194-200.

[2] LAEKHANUKIT B, VETTA A, WILFONG G. Routing regardless of network stability[J]. Algorithmica, 2014, 70(3):561-593.

[3] STOEGER F, BIRGE-LEE H, GIULIARI G, et al. BGP vortex: update message floods can create Internet instabilities[C]// Proceedings of the 34th USENIX Conference on Security Symposium. Seattle, USA: USENIX Association, 2025:No.186.

[4] 苗甫,王振兴,郭毅,等.一种基于突变理论的域间路由

系统 BGP-LDoS 攻击检测方法[J]. 信息工程大学学报, 2019, 20(4):452-460.

[5] 郭毅,王振兴,孙剑平.域间路由系统安全技术研究[J]. 信息工程大学学报, 2012, 13(3):345-351.

[6] TRAINA P, MCPHERSON D, SCUDDER J. Autonomous system confederations for BGP: RFC 5065[S]. California, USA: the IETF Trust, 2007:1-13.

[7] SCOTT B A, JOHNSTONE M N, SZEWCZYK P. A survey of advanced border gateway protocol attack detection techniques[J]. Sensors, 2024, 24(19):No.6414.

[8] BIRGE-LEE H, WANG L, REXFORD J, et al. SICO: surgical interception attacks by manipulating BGP communities[C]// Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. New York, USA: ACM, 2019:431-448.

[9] MILOLIDAKIS A, BÜHLER T, CHIESA M, et al. Poster: smart BGP hijacks that evade public route collectors[C]// Proceedings of the 2021 ACM Internet Measurement Conference. New York, USA: ACM, 2021:1-2.

[10] ZENG M, HUANG X H, ZHANG P, et al. Understanding the impact of outsourcing mitigation against BGP prefix hijacking[J]. Computer Networks, 2022, 202: No. 108650.

[11] DA SILVA B A, CUNHA Í, FERREIRA R A. Automatic inference of BGP community semantics[C]// Proceedings of the 2025 IEEE Network Operations and Management Symposium. Piscataway, USA: IEEE, 2025:1-8.

(编辑:邵 华)