域间路由系统级联失效下的目标失效链路定位方法研究

曾子懿 邱 菡* 朱俊虎 王清贤 陈 迪
(战略支援部队信息工程大学 郑州 450001)
(国家数字交换系统工程技术研究中心 郑州 450001)

摘 要：协同跨平面会话中断攻击(CXPST)通过反复对多条目标关键链路实施低速率拒绝服务攻击(LDoS)造成域间路由系统的级联失效，从而导致互联网的崩溃。在攻击发生的初期，准确定位受攻击的关键链路并进行针对性防御可遏制级联失效的发生。现有定位方法研究主要基于单源假设，没有考虑多条目标链路同时失效对路径撤回的影响，定位准确度受限。针对上述问题，该文提出一种基于加权统计匹配得分的多失效链路定位方法(WSFS)，以级联失效攻击目标链路选择策略作为推断基础，将撤销路径长度的倒数作为权重对评分进行加权。基于实际网络拓扑和有利点位置的级联失效攻击仿真实验结果表明，WSFS比目前最优方法平均准确率可提升5.45%。实验结果证明WSFS相比于其他定位方法更适合应对域间路由系统级联失效下的目标失效链路定位问题。

关键词：多失效链路定位；域间路由系统；级联失效；路径长度加权
中图分类号：TN915.08 **文献标识码**：A **文章编号**：1009-5896(2020)09-2134-08
DOI: 10.11999/JEIT200008

Research on Target Failure Link Location Method in Inter-domain Routing System Cascading Failure

ZENG Ziyi QIU Han ZHU Junhu WANG Qingxian CHEN Di
(*Information Engineering University*, *Zhengzhou* 450001, *China*)
(*National Digital Switching System Engineering & Technological Research Center*, *Zhengzhou* 450001, *China*)

Abstract: Coordinated Cross Plane Session Termination (CXPST) repeatedly implements Low rate Denial of Service (LDoS) attacks on multiple target critical links, causing the cascading failure of the inter-domain routing system and the collapse of the internet. In the early stages of an attack, accurately locating the critical link under attack and carrying out targeted defense can prevent the occurrence of cascading failures. The research on existing locating methods is mainly based on the single-source hypothesis, and does not consider the impact of simultaneous failure of multiple target links on path withdrawal, so the locating accuracy is limited. To solve the above problems, a locating method is proposed based on Weighted Statistical Fit Score (WSFS). Using the target link selection strategy of cascading failure attack as inferring basis, scores are weighted by the reciprocal of the length of the withdrawal paths. The simulation results based on the actual network topology and vantage point location show that WSFS can improve the average accuracy rate by 5.45% compared with the current optimal method. Experimental results prove that WSFS is more suitable for locating target failure links in inter-domain routing system cascading failure than other locating methods.

Key words: Multiple failure link location; Inter-domain routing system; Cascading failure; Path length weighting

1 引言

域间路由系统是因特网的骨干路由系统，承载了因特网数据交换的核心职能。域间路由系统的现行协议是边界网关路由协议(Border Gateway Protocol, BGP)[1]，运行该协议的BGP路由器可依据路由策略将网络可达性信息动态地向其他BGP路由器传递，使得局部的网络可达性变化能够传播至整个域间路由系统。BGP由多个自治域(Autonomous System, AS)组成。由于BGP自身协议设计存在许多缺陷，攻击者利用这些缺陷可以构

收稿日期：2020-01-02；改回日期：2020-08-05；网络出版：2020-08-13
*通信作者： 邱菡 qiuhan410@aliyun.com
基金项目：国家自然科学基金(61502528)
Foundation Item: The National Natural Science Foundation of China (61502528)

造多种针对域间路由系统的攻击，较为常见的攻击包括IP前缀劫持[2]、AS路径篡改[3]等。

近年来，研究者通过对BGP协议自适应机制缺陷的深入研究发现能够借由对BGP数据平面实施阻断攻击来对BGP的控制平面产生影响：由于数据平面和控制平面共用信道，数据平面的阻塞能够妨碍控制平面信息的传递；控制平面信息传递受阻，可能导致新的路径计算，转而影响数据平面的流量转发。这些攻击包括异常Update攻击[4]、BGP压力攻击[5]、协同跨平面会话中断攻击(Coordinated Cross Plane Session Termination, CXPST)[6]以及分布式网络瘫痪攻击(Distributed Network Paralyzing, DNP)攻击[7]。特别是CXPST攻击，通过利用ZMW攻击[8]阻断精心挑选的少量域间路由链路，引发级联失效现象，致使整个域间路由系统崩溃。

域间路由系统级联失效攻击危害十分巨大，然而由于其利用了BGP协议设计上的缺陷，现有的防御手段在应对级联失效攻击时作用有限[9]。邱菡等人[10]在对仿真实验和现网安全事件数据分析后指出，引发域间路由级联失效需要经历至少1 h的时间。根据主动防御思想，如果在攻击还处于致使目标节点或链路失效的阶段时对攻击目标进行准确定位，那么就能够采取有针对性的防御性手段，防止数据平面的攻击向控制平面迁移，遏制级联失效的发生[11]。目前级联失效防御相关研究多集中在异常检测[12–14]方面，针对域间路由系统级联失效下的目标失效链路定位方法开展的研究相对较少。

本文主要在域间路由系统级联失效攻击背景下，开展目标失效链路定位问题的研究。第2节分析了单失效链路定位方法的有效性和存在的不足；第3节在分析级联失效攻击目标选择策略的基础上，提出了一种基于加权统计匹配得分的多失效链路定位方法。第4节通过实验验证了方法的有效性；第5节对本文的工作进行了总结。

2　单失效链路定位方法分析

根据定位方法是否主动发送探测流量，失效链路的定位方法可分为主动式探测以及被动式监听两种。主动式探测一般使用traceroute等工具主动发送流量探测失效位置。为了达到对关键链路全覆盖的目标，主动式探测必须同时监控多个网络前缀的可达性，并在监控过程中周期性地产生大量的数据包，加剧控制平面的计算资源消耗，不适用于级联失效下的目标链路定位。相反，被动式监听不会产生额外的数据包，通过分析被动接收的UPDATE消息，设计启发式方法利用控制平面的异常变化定位失效的节点或链路，在数据平面阻塞时仍可正常工作。现有的被动式监听方法一般基于单链路失效假设，而域间路由系统级联失效则是由多条链路同时失效引发。下面对现有被动式监听方法应对多链路同时失效的适用性进行分析。

2.1　现有方法的分析

Caesar等人[15]设计了一种定位路由变化源位置的BGP健康推理系统。该方法认为当从单个观测点观测到大量的前缀可达性变化共享同一公共路径时，失效源应该位于该公共路径上。在分析单个观测点观测结果的基础上可以进一步通过综合多个观测点的观测结果准确定位单条失效链路。

Feldmann等人[16]提出了一种域间路由系统不稳定源的推断方法。与Caesar等人的研究类似，该方法以两个假设为前提条件：(1)引发域间路由系统不稳定的根源可能是单个节点失效或单条链路失效；(2)节点或链路的失效将引发路径的变化，且源节点或链路位于被撤销的路径或新宣告的路径中。以此为基础，该方法将存续路径包含的节点或链路视为稳定的节点或链路，形成稳定集合；将新宣告或撤销的路径包含的节点或链路视为不稳定的节点或链路，形成不稳定集合。不稳定源应同时满足存在于不稳定集中而不存在于稳定集中，因此由不稳定集与稳定集的差集能得到不稳定源的候选集。然而，该方法不能按照失效源可能性大小对节点或链路进行排序，所有候选的节点或链路是等可能的。在候选集较大时，定位结果缺乏实际的指导意义。

Javed等人[17]通过实例分析找到Feldmann等人假设存在的问题，即存在失效节点或链路并不位于被撤销的路径或新宣告的路径中的情况，其原因在于该假设未考虑BGP的复杂路由选择策略带来的影响。针对这个问题，Javed等人提出了一种递归型源定位方法，通过逐步缩小可能的失效源范围，能够应对BGP路由器选路策略多样性导致UPDATE消息传播过程中根源信息丢失的问题，然而该方法需要下游路由器运行于合作模式。

Glass等人[18]提出了一种基于节点介数排序的失效源定位方法。该方法首先确定了观测点集合以及目标AS集合，并基于这两个集合间的路径重新定义了节点的介数。由于当失效发生时，从观测点到目标AS的路径将会被重新计算，必然导致节点介数的改变，因此计算节点介数的变化就有可能定位失效节点。Glass等人认为介数变化幅度越大的节点越有可能是失效节点，然而在处理UPDATE消息计算节点介数变化时，该方法并没有区分ANNOUNCE

消息和WITHDRAW消息，因此容易将一些受波及的节点错误地视为失效节点，使得失效节点的定位准确率不高。

Ventorim等人[19]提出了一种基于最大评分因子的F1Score分类器对失效节点进行定位。该方法的假设是：大多数发生变化的路径经过此失效源，而大多数经过此失效源的路径发生了变化。根据该假设，F1Score方法仅以路径撤销信息作为启发式算法的输入，而忽略了新宣告的路径和存续不变的路径。然而事实上，一条链路若发生失效那么它不应该存在于实际的可用路径中。在进行失效源定位时，应当同时使用当前可用路径信息作为算法的输入。

针对上述单失效链路定位中存在的问题，Holterbach等人[20]提出了一种基于匹配得分的失效链路定位方法(Fit Score, FS)，使用路径的撤销信息以及当前可用路径信息对链路进行综合评分，具有定位精度高的特点。除此之外，该方法可给出链路失效的可能性排序，利于失效链路的进一步筛选。

根据对现有单失效链路定位方法的分析可知，此类定位方法的思想是利用路径变化信息构造启发式算法，对失效链路进行直接筛选或评分排序。单失效链路定位方法的分析结果如表1所示，其中基于FS的失效链路定位方法是目前单失效链路定位方法中综合最优的方法。下面，将对FS展开进一步分析，并以此研究单链路失效方法在多链路失效情形下的不足之处。

2.2 FS

在链路失效发生后的一段时间内，基于匹配得分的失效链路定位方法从采集的UPDATE消息中提取撤销路径，并计算当前可用路径。该方法的基本思想是找出那些被撤销路径经过的次数尽可能多且被当前可用路径经过次数尽可能少的链路作为失效链路。对于任意链路l，l的FS是撤销占比(Withdrawal Share, WS)和路径占比(Path Share, PS)的加权几何平均值

$$\mathrm{FS}(l,t)=[\mathrm{WS}(l,t)^{\omega_{\mathrm{WS}}}\cdot\mathrm{PS}(l,t)^{\omega_{\mathrm{PS}}}]^{\frac{1}{\omega_{\mathrm{WS}}+\omega_{\mathrm{PS}}}} \tag{1}$$

其中，WS是经过链路l的撤销路径数占所有撤销路径数的比值，PS是经过链路l的撤销路径数占经过该链路的撤销路径数与当前可用路径数之和的比值。WS和PS可表示为

$$\mathrm{WS}(l,t)=\frac{W(l,t)}{W(t)} \tag{2}$$

$$\mathrm{PS}(l,t)=\frac{W(l,t)}{W(l,t)+P(l,t)} \tag{3}$$

其中，$W(l,t)$是时间t内撤销的路径经过l的次数，简称为l的撤销次数。$W(t)$是时间t内撤销的路径总数，$P(l,t)$是t时刻仍然可用的路径经过链路l的次数，简称为l的存续次数。ω_{WS}与ω_{PS}分别是WS与PS的权值。假设当$t=0$时发生链路失效，采集点还未能感知到任何路径变化，因此$P(l,0)$可表示失效发生前经过链路l的路径数。

2.3 单链路失效情形下FS的有效性分析

为了便于分析问题，在进行FS有效性分析时作出两个一般性假设：

(1) 可以获取网络中的所有路径变化。

(2) 路径计算采用最短路径优先方法。

对于一条路径p，$L_p(p)$表示由p中经过的链路组成的集合。对于一个路径集合P，定义P对应的链路集合为

$$L_p(p)=\bigcap_{p\in P}L_p(p) \tag{4}$$

设时刻0链路$\hat{l}$失效，经过时间t后网络趋于相对稳定。假设网络中的节点以最短路径优先的方式进行路由计算。观察失效前后的路径变化，不妨设链路失效前的路径集合为$\widehat{P}$，链路失效后的路径集合为$\breve{P}$，消失的旧路径集合$\tilde{P}=\widehat{P}-\widehat{P}\cap\breve{P}$。那么失效链路$\hat{l}$一定存在于失效前的链路集合$L_p(\widehat{P})$中而不存在失效后的链路集合$L_p(\breve{P})$中，这是由链路$\hat{l}$失效这个事实决定的。因此在理想情况下，$W(\hat{l},t)>0$且$P(\hat{l},t)=0$，此时$\mathrm{PS}(\hat{l},t)=1$。

进一步的，当$\widehat{P}\cap\breve{P}\neq\varnothing$时，可以确定失效链路$\hat{l}\in L_p(\tilde{P})$。对于失效链路$\hat{l}$，一定有$W(\hat{l},t)=$

表 1 单失效链路定位方法的对比分析

方法	可排序	区分路径更新类型	使用路径撤销信息	使用可用路径信息	合作需求
Caesar等人[15]		√	√	√	
Feldmann等人[16]		√	√	√	
Javed等人[17]		√	√	√	√
Glass等人[18]	√		√		
Ventorim等人[19]	√	√	√		
Holterbach等人[20]	√	√	√	√	

$W(t)$。证明过程如下：首先一定存在$W(\hat{l},t)\le W(t)$。若$W(\hat{l},t)<W(t)$，那么必然存在$p\in\tilde{P}$, p不经过$\hat{l}$，与单链路失效条件矛盾，因此有$W(\hat{l},t)\ge W(t)$，故$W(\hat{l},t)=W(t)$。因此在单链路失效情形下有$W(\hat{l},t)=1$。　　证毕

2.4 多链路失效情形下FS的不足

根据2.3节对PS有效性的证明可知，因子PS的有效性来源于链路失效事实本身。对于链路$l\in\hat{L}$, $\hat{L}$为失效链路集合，仍有$W(l,t)>0$且$P(l,t)=0$，因子PS在多源条件下仍然有效。然而，因子WS的有效性证明利用了单链路失效假设。因子WS在多链路失效情形下的有效性存疑。

考虑图1展示的一个双链路失效情形，假设网络中每个节点都以最短路径优先的方式计算抵达其他节点的路径，网络中每个节点都具有监测路径变化的能力。在0时刻链路AC与链路BC因遭受攻击而失效，经过时间t后网络趋于稳定。各链路WS值如表2所示，在6条链路中非失效链路CD的WS值最高，失效链路AC与BC的WS值次高。这是由于当一条链路的$P(l,0)$越大，它与其他链路共同出现于同一链路的可能性就越大，这将导致非失效链路的WS值很有可能高于实际失效链路的WS值。

3 级联失效攻击下的目标失效链路定位方法

WS评分在多链路失效情形下并不一定能得到理想的结果。WS“平等”地看待每条撤销路径，然而这样的“平等”是不合适的。如果一条撤销路径不包含非失效链路，那么对这条路径中的链路进行统计将不存在对非失效链路的评分增加，反之则会提升非失效链路的评分；路径中包含的非失效链路数越多，则有越多的非失效链路的评分被提升。因此，需要考虑失效链路数在撤销路径中的占比。

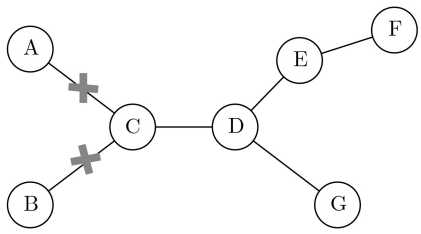


图 1 双链路失效图

表 2 各链路的WS值

链路	WS值
CD	1.00
AC	0.75
BC	0.75
DE	0.50
DF	0.25
EG	0.25

3.1 级联失效攻击的目标链路选择策略

近年来，研究者们提出了一系列针对BGP协议自适应机制缺陷精心设计的攻击，特别是针对BGP协议数据平面的一类低速率拒绝服务攻击，能够造成域间路由系统性能的降级直至崩溃，其危害十分严重。最典型的一类攻击是Schuchard等人[6]提出的CXPST攻击，通过对多条精心挑选的域间路由系统关键链路实施ZMW攻击[8]，反复重置多条BGP会话，使得相关节点产生大量UPDATE消息，这些大量的UPDATE消息足以致使路由器过载，导致更多的UPDATE消息的产生，最终致使整个互联网崩溃。Li等人[7]在Schuchard等人工作的基础之上研究了攻击流量规划问题，证明了控制大规模僵尸网络的攻击者可以利用DNP攻击来严重威胁域间路由系统安全。

在实施攻击前，攻击者首先要选定目标关键链路并对攻击流量进行规划。为了使用有限的攻击资源达成最大化的攻击效果，攻击者在选择目标关键链路时将倾向于能够影响更多路径的关键链路。例如，在实施CXPST攻击前，攻击者首先统计当前各条链路的$P(l,0)$。由于高$P(l,0)$的链路失效意味着大量路径的重新计算，因此攻击者应该从具有高$P(l,0)$的链路集合中选取目标关键链路。在此之上，攻击者在选择目标攻击链路时还将考虑以下两点：

(1) 组合毁伤效果最优：由于一条路径可能经过多条目标关键链路，这些目标关键链路同时失效造成对控制平面的影响不能简单叠加，因此独立考虑每条链路的$P(l,0)$难以达成实际最优的攻击效果。所以，在进行目标关键链路选择时，攻击者应该尽力避免多条目标关键链路位于相同路径上的情况。

(2) 攻击流的非目标拥塞避免：在实施攻击时，大量攻击流量将会从各个僵尸节点发往目标链路。为了避免攻击流量在非目标关键链路处发生拥塞而丧失了阻断目标关键链路能力的情况，应当对攻击流量加以规划。然而，当大量的路径中包含多条目标关键链路时将出现两难的局面：(a)为了减小发往这些目标链路的攻击流量间的相互影响，将使攻击流量受限。攻击流的非目标拥塞避免的结果很可能是关键目标链路上无法汇聚足够的攻击流量，致使攻击失败。(b)若不进行攻击流的非目标拥塞避免，那么攻击实际上难以造成预先选定的目标关键链路失效，因此将会造成攻击资源的浪费。

因此，为了确保攻击的可实施性以及最大化攻击效果，攻击者在选择目标关键链路时需要参考两

个指标：一是链路的$P(l,0)$值，二是每一条路径包含的目标链路数。前者是越高越好，后者相反。

3.2 撤销路径特性

为了进一步分析多链路失效情形下的源定位问题，首先定义链路集合L在p上的最大共现子集。

定义1 对于路径p以及链路集合L，若$\chi \subset L$且$\chi \subset L_p(p)$，那么χ是L在p上的一个共现子集。

定义2 对于路径p以及链路集合L，定义L在p上的最大共现子集$\chi_{\max}(L,p) = L \cap L_p(p)$。

考察大小为n的失效链路集$\hat{L}$在撤销路径集合$\tilde{P}$中的每一条路径上的最大共现子集，可按照集合模的大小将这些最大共现子集分为$\left|\hat{L}\right|+1$类，其中$\rho(k)$表示子集模大小为k的最大子集数量，很明显$\rho(0)=0$。根据3.1节对级联失效攻击的目标链路选择的分析可知，攻击者希望可用路径包含的目标链路数越少越好，因此可以有$\rho(k)>\rho(k+1), k=1,2,\cdots,\left|\hat{L}\right|+1$。在理想情况下有

$$\rho(1) \gg \sum_{k} \rho(k), k=2,3,\cdots,n \tag{5}$$

表示大多数撤销路径仅包含一条失效链路，而较少撤销路径包含多条失效链路。当$L_p(p)$增大时，由于p中包含的失效链路数并不随$L_p(p)$增大而增大。当$|L_p(p)|=1$时，p可以提供最利于定位的信息。不仅如此，根据上述分析可知，对于大多数$p \in \tilde{P}$，有$|\chi_{\max}(L,p)|=1$。在更新WS值时短路径将引入更少的非失效链路噪声。

3.3 基于加权统计匹配得分的失效链路定位方法

根据对多链路失效情形下FS的不足以及对撤销路径特性的分析，本文提出一种基于加权统计匹配得分的多失效链路定位方法(Weighted Statistical Fit Score, WSFS)，对面向级联失效的蓄意攻击造成的多失效链路进行准确定位。由于单失效链路定位方法未考虑链路共现带来的WS值虚高现象，因此在遍历路径时，以撤销路径中失效链路的共现次数与撤销路径长度对WS值的影响。具体来说，有别于FS平等的对待不同撤销路径，WSFS认为撤销路径p对评分的贡献取决于$\left|\chi_{\max}(\hat{L},p)\right|$。撤销路径$p$的$\left|\chi_{\max}(\hat{L},p)\right|$越高，$p$引入的噪声就越小。当$\left|\chi_{\max}(\hat{L},p)\right| = L_p(p)$时，由于$p$中任意链路都是失效链路，此时通过$p$更新链路的WS值时不会对非失效链路的WS值产生影响。其次，由于$\left|\chi_{\max}(\hat{L},p)\right|$无法提供链路中具体哪些链路失效的信息，因此在评分时平等看待$L_p(p)$中的各条链路。WSFS可以表示为

$$\mathrm{WSFS}(l,t) = [\mathrm{WSWS}(l,t)^{\omega_{\mathrm{WS}}} \cdot \mathrm{PS}(l,t)^{\omega_{\mathrm{PS}}}]^{\frac{1}{\omega_{\mathrm{WS}}+\omega_{\mathrm{PS}}}} \tag{6}$$

WSWS是加权统计的撤销占比，可表示为

$$\mathrm{WSWS}(l,t) = \frac{\mathrm{WSW}(l,t)}{\mathrm{WSW}(t)} \tag{7}$$

其中，$\mathrm{WSW}(l,t)$是截止时刻t加权统计后的链路l的撤销次数，$\mathrm{WSW}(t)$是截止时刻t加权统计后的撤销路径数。$\mathrm{WSW}(l,t)$与$\mathrm{WSW}(t)$可分别表示为

$$\mathrm{WSW}(l,t) = \sum_{p\in\tilde{P}} Q(l,p) \cdot \frac{\left|\chi_{\max}(\hat{L},p)\right|}{|L_p(p)|} \tag{8}$$

$$\mathrm{WSW}(t) = \sum_{p\in\tilde{P}} \frac{\left|\chi_{\max}(\hat{L},p)\right|}{|L_p(p)|} \tag{9}$$

其中$Q(l,p)$是一个判别函数，判断路径p是否经过链路l。当路径p经过链路l时，$Q(l,p)=1$；反之，$Q(l,p)=0$。显然在一般情况下，准确估计路径p的$\left|\chi_{\max}(\hat{L},p)\right|$是十分困难的。然而根据前文对级联失效攻击导致的撤销路径特性分析表明，由于组合毁伤效果最优以及攻击流的非拥塞避免，对于大多数$p\in\tilde{P}$，有$\left|\chi_{\max}(\hat{L},p)\right|=1$。因此，面向级联失效攻击时，$\mathrm{WSW}(l,t)$与$\mathrm{WSW}(t)$可分别表示为

$$\mathrm{WSW}(l,t) = \sum_{p\in\tilde{P}} Q(l,p) \cdot \frac{1}{|L_p(p)|} \tag{10}$$

$$\mathrm{WSW}(t) = \sum_{p\in\tilde{P}} \frac{1}{|L_p(p)|} \tag{11}$$

为了给出最终的定位结果，WSFS需要估计失效链路的个数。假设某时刻有n条链路失效，而WSFS的评分结果是完全正确的，即评分最高的前n条都是失效链路。那么根据撤销路径中失效链路相对独立出现的特性可知当$\omega_{\mathrm{WS}}=\omega_{\mathrm{PS}}=1$时，评分降序排列的前$n$条链路$l_1,l_2,\cdots,l_n$的WSFS值之和等于1，即

$$\sum_{i=1}^{n} \mathrm{WSFS}(l_i,t) = 1 \tag{12}$$

证明过程如下：由于$l_1,l_2,\cdots,l_n$是失效链路，因此$P(l_i,t)=0$, $\mathrm{PS}(l_i,t)=1$, $i\in\{1,2,\cdots,n\}$。理想情况下$\sum_{k=2}^{|\hat{L}|+1}\rho(k)=0$，因此$\tilde{P}$可被划分为$n$个子集，其中每个子集中的撤销路径都仅包含失效链路$l_1,l_2,\cdots,l_n$中的一条，那么有

$$\sum_{i=1}^{n} \mathrm{WSW}(l_i,t) = \mathrm{WSW}(t) \tag{13}$$

因此$\sum_{i=1}^{n}\mathrm{WSWS}(l_i,t)=1$, $\sum_{i=1}^{n}\mathrm{WSFS}(l_i,t)=1$。证毕

根据式(12)，在以方法的正确性为前提假设下，可以按照链路评分降序排序从前至后累加链路的WSFS直至WSFS的累加结果超过1。

4　实验

4.1　实验设置

对多链路失效安全事件的事后分析缺乏对失效链路的标记，因此采用仿真实验的方式对WSFS的有效性进行实验验证。为了提供可信的实验结果，选用Shurhard在进行级联失效实验时使用的自治域关系数据库[21]构建网络。该AS关系数据库中的每一条信息记录了两个AS之间存在的商业关系，由三元组<AS1, AS2, Relationship>表示，其中AS1与AS2是AS号，Relationship表示AS之间的关系，包括客户——服务提供商关系(–1)、对等关系(0)、服务提供商——客户关系(1)以及兄弟关系(2)。通过读取解析AS关系数据库，构建符合实际AS连接关系的网络拓扑，包括33567个AS节点以及75001条链路。

在监测路径变化时，一般采用静默的路由节点被动地收集网络信息，这样的路由节点称之为有利点(Vantage Point, VP)。显然，VP在网络中的分布对实验结果的评估存在影响。本文通过世界互联网组织RIPE提供的UPDATE监测数据[22]解析得到VP与AS的映射关系。

在目标链路选择中，首先计算VP到各AS的最短路径，并对每条链路在这些路径中出现的次数进行统计，并按照次数从高到底对其进行排序。根据对级联失效攻击的目标链路选择策略的分析，攻击者一般在攻击时倾向于攻击初始存续次数更大的目标链路，因此将排序前0%～2%和2%～5%的链路集作为集合1与集合2，实验所用的目标链路分别从两个集中挑选，分别挑选20, 40, 60, 80, 100, 140, 200条链路作为失效链路。为了使失效链路具有一定的随机性，按如下方式挑选失效链路：(1)计算所有链路的$P(l,0)$；(2)随机选择集合中的一条链路作为第1条失效链路；(3)遍历路径集合，当路径中存在该失效链路时，其他与其共现的链路$P(l,0)$减1；(4)选择$P(l,0)$最高的链路加入失效链路集，重复执行方式(2), (3), (4)直到失效链路数量达到要求。

实验设置的对比方法为WS方法与WSWS方法、FS方法、WSFS方法以及F1Score方法。在应用FS方法与WSFS方法时。为了估计失效链路范围，设置$\omega_{\mathrm{WS}}=1$, $\omega_{\mathrm{PS}}=1$评估指标为方法的准确性，即定位结果中包含的实际失效链路数占实际总失效链路数的比值。

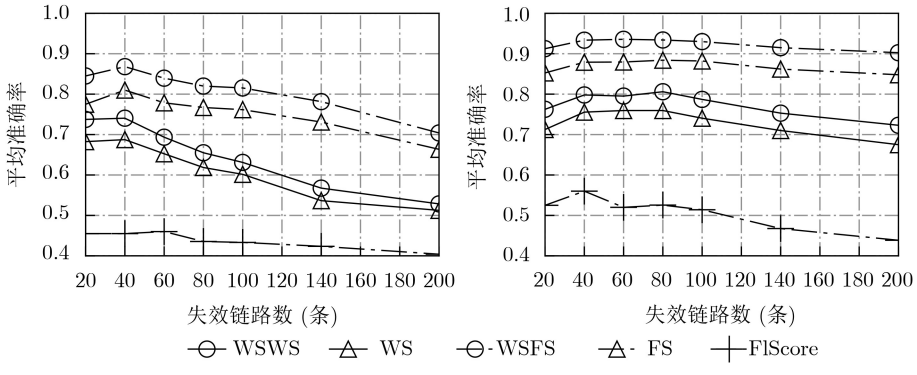
在实验开始时，首先计算网络中节点间的最短路径。然后根据不同的失效链路组合摘除网络中对应的链路。接着更新网络中节点间的最短路径。将两个路径集合输入算法，得到按照评分降序排列的候选失效链路，并比较方法的准确率。

4.2　实验结果与分析

不同方法的平均定位准确率如图2所示，其中图2(a)与图2(b)分别展示了在集合1与集合2上随失效链路数量增加，不同定位方法的平均准确率的变化。从图中可以看出WSFS在不同链路失效数下都取得了最优的结果，WSWS方法同时也优于WS方法。5种对比方法中使用F1Score方法准确率最低。

对比图3(a)与图3(b)，可以发现在集合1的实验中，失效链路数量增多将明显导致定位准确率的下降；而在集合2的实验中，各定位方法结果的准确率下降并不明显。分析失效链路的属性可以发现，集合1的链路之间初始存续次数偏高，因此当失效链路增多时，更容易影响定位结果。

在链路集合1上的实验结果表明，FS-WPSL相比于F1Score方法、WS方法、WSWS方法以及FS方法的平均准确率提升分别为37.2%, 19.7%, 16.0%以及5.5%。在链路集合2上的实验结果表

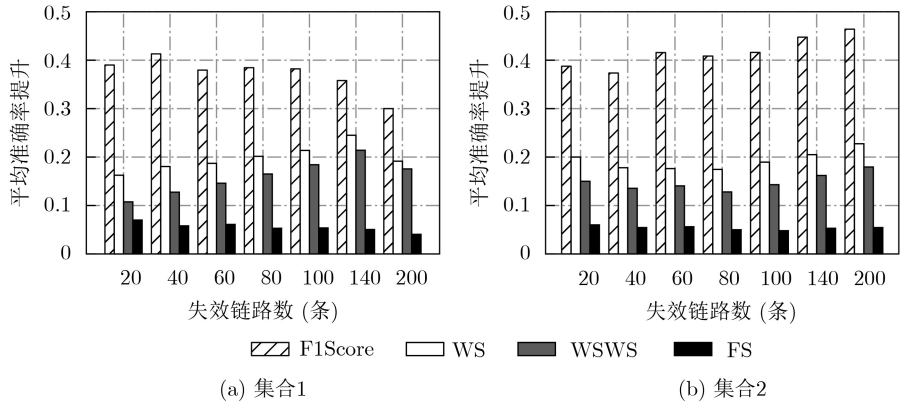


(a) 集合1　　(b) 集合2

图 2 各方法的平均定位准确率

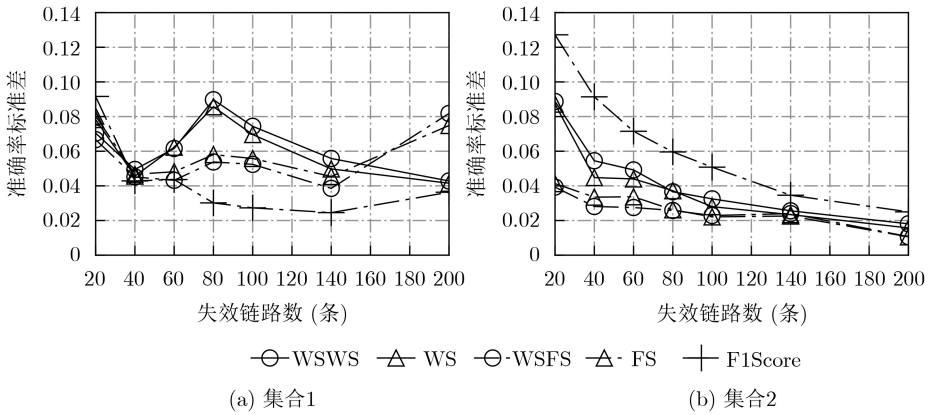
明，平均准确率提升分别为41.6%, 19.3%, 14.8%以及5.4%。图3展示了WSFS相比于4种定位方法在不同失效链路数上的准确率提升。综合两个失效链路集合上的实验结果，WSFS相比于FS评分方法提升了5.45%，具有最高的定位准确率。实验结果证明攻击者企图阻断多条域间路由链路造成域间路由系统级联失效时，所提出的WSFS方法具有更高的失效链路定位准确率。

图4展示了各定位方法精确度的标准差，其中图4(b)中各方法的定位精确度在失效链路数较小时标准差较大，而随着失效链路数量的不断增大，标准差逐渐减小。这种现象的出现是由于定位准确度的计算是以实际失效链路数量作为基数，当失效链路数量较少时，定位结果的较小差异将带来准确率的较大变化。因此，可以认为所有方法在失效链路集合2上是相对稳定的。观察图4(a)可以发现所选的5种方法在失效链路集合1上的标准差变化并不具备失效链路集合2上的规律，可能的原因是集合1中的链路的初始存续次数相差较大，失效链路组合的随机性将导致定位算法的不稳定性表现。



(a) 集合1 (b) 集合2

图 3 WSFS相较4种定位方法的准确率提升



(a) 集合1 (b) 集合2

图 4 各方法定位准确率的标准差

5 结论

多链路失效可能引发域间路由系统的级联失效，严重影响互联网的数据安全。为了深入理解安全态势，除了识别多链路失效威胁外，还应准确定位失效链路。本文首先分析得出了单失效链路定位方法在多链路失效情形下存在不足的原因是没有考虑链路共现对评分的影响。然后分析了级联失效攻击的目标链路选择策略，指出组合毁伤效果最优以及攻击流的非目标拥塞避免将会使得撤销路径中出现失效链路相对独立出现的现象。根据上述分析，提出了一种基于加权统计匹配得分的多失效链路定位方法WSFS，通过在更新撤销占比时引入对失效链路数占路径中链路总数的考虑，结合级联失效攻击导致的撤销路径特性，以路径长度的倒数进行加权。基于真实网络拓扑与VP分布的仿真实验证明，WSFS在级联失效攻击造成的多链路失效情形下相比于目前最优的单失效链路定位方法具有更高的准确率。

参 考 文 献

[1] REKHTER Y, LI T, and HARES S. IETF RFC 4271 A border gateway protocol 4 (BGP-4)[S]. 2006.

[2] SERMPEZIS P, KOTRONIS V, DAINOTTI A, *et al.* A

survey among network operators on BGP prefix hijacking[J]. *ACM SIGCOMM Computer Communication Review*, 2018, 48(1): 64–69. doi: 10.1145/3211852.3211862.

[3] BUTLER K, MCDANIEL P, and AIELLO W. Optimizing BGP security by exploiting path stability[C]. The 13th ACM Conference on Computer and Communications Security, Alexandria, USA, 2006: 298–310.

[4] SCHUCHARD M, THOMPSON C, HOPPER N, *et al*. Taking routers off their meds: Why assumptions of router stability are dangerous[C]. The 19th Network and Distributed System Security Symposium, San Diego, USA, 2012.

[5] DENG Wenping, ZHU Peidong, LU Xicheng, *et al*. On Evaluating BGP routing stress attack[J]. *Journal of Communications*, 2010, 5(1): 13–22.

[6] SCHUCHARD M, MOHAISEN A, FOO KUNE D, *et al*. Losing control of the internet: Using the data plane to attack the control plane[C]. The 17th ACM Conference on Computer and Communications Security, Chicago, USA, 2010: 726–728.

[7] LI Heshuai, ZHU Junhu, QIU Han, *et al*. The new threat to internet: DNP attack with the attacking flows strategizing technology[J]. *International Journal of Communication Systems*, 2015, 28(6): 1126–1139. doi: 10.1002/dac.2748.

[8] ZHANG Ying, MAO Z M, WANG J. Low-Rate TCP-targeted DoS attack disrupts internet routing[C]. 2007 Network and Distributed System Security Symposium, San Diego, USA, 2007.

[9] 郑皓, 陈石, 梁友. 关于“数字大炮”网络攻击方式及其防御措施的探讨[J]. 计算机研究与发展, 2012, 49(S1): 69–72.
ZHENG Hao, CHEN Shi, and LIANG You. How the cyber weapon “Digital Ordnance” works and its precautionary measures[J]. *Journal of Computer Research and Development*, 2012, 49(S1): 69–72.

[10] 邱菡, 李玉峰, 兰巨龙, 等. 域间路由系统的级联失效攻击及检测研究[J]. 中国科学: 信息科学, 2017, 47(12): 1715–1729. doi: 10.1360/N112016-00259.
QIU Han, LI Yufeng, LAN Julong, *et al*. Research on cascading failure attack and detection of inner-domain routing system[J]. *Scientia Sinica Informationis*, 2017, 47(12): 1715–1729. doi: 10.1360/N112016-00259.

[11] QIU Han, ZHU Huihu, LI Yufeng, *et al*. FD-SP: A method for predicting cascading failures of inter-domain routing system[C]. The 4th IEEE International Conference on Computer and Communications (ICCC), Chengdu, China, 2018: 290–295.

[12] GUO Yi, DUAN Haixin, CHEN Jikun, *et al*. MAF-SAM: An effective method to perceive data plane threats of inter domain routing system[J]. *Computer Networks*, 2016, 110: 69–78. doi: 10.1016/j.comnet.2016.09.017.

[13] ZHANG Mingwei, LI Jun, and BROOKS S. I-Seismograph: Observing, measuring, and analyzing internet earthquakes[J]. *IEEE/ACM Transactions on Networking*, 2017, 25(6): 3411–3426. doi: 10.1109/TNET.2017.2748902.

[14] ZENG Ziyi, ZHU Junhu, QIU Han, *et al*. SM-RC: A new security measurement method for inter-domain routing system[J]. *IEEE Access*, 2019, 7: 108189–108199. doi: 10.1109/ACCESS.2019.2927712.

[15] CAESAR M, SUBRAMANIAN L, and KATZ R H. Towards localizing root causes of BGP dynamics[R]. UCB/CSD-04-1302, 2003.

[16] FELDMANN A, MAENNEL O, MAO Z M, *et al*. Locating Internet routing instabilities[J]. *ACM SIGCOMM Computer Communication Review*, 2004, 34(4): 205–218. doi: 10.1145/1030194.1015491.

[17] JAVED U, CUNHA I, CHOFFNES D, *et al*. PoiRoot: Investigating the root cause of interdomain path changes[J]. *ACM SIGCOMM Computer Communication Review*, 2013, 43(4): 183–194. doi: 10.1145/2534169.2486036.

[18] GLASS K, COLBAUGH R, and PLANCK M. Automatically identifying the sources of large Internet events[C]. 2010 IEEE International Conference on Intelligence and Security Informatics, Vancouver, Canada, 2010: 108–113.

[19] VENTORIM COMARELA G. On the dynamics of interdomain routing in the Internet[D]. [Ph. D. dissertation], Boston University, 2017.

[20] HOLTERBACH T, VISSICCHIO S, DAINOTTI A, *et al*. Swift: Predictive fast reroute[C]. 2017 Conference of the ACM Special Interest Group on Data Communication, Los Angeles, USA, 2017: 460–473.

[21] CAIDA. BGP AS links[EB/OL]. http://as-rank.caida.org.

[22] RIPE. RIS raw data[EB/OL]. https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data, 2019.

曾子懿：男，1989年生，讲师，研究方向为网络安全、路由系统、复杂网络.

邱　菡：女，1981年生，副教授，研究方向为网络安全、复杂网络.

朱俊虎：男，1974年生，教授，研究方向为网络安全.

王清贤：男，1960年生，教授，研究方向为计算理论、网络安全.

陈　迪：女，1992年生，博士生，研究方向为网络安全、路由系统、复杂网络.

责任编辑：陈　倩