中国科学: 信息科学 2017 年 第 47 卷 第 12 期: 1715–1729
SCIENTIA SINICA Informationis
论文

域间路由系统的级联失效攻击及检测研究

邱菡[1,2*], 李玉峰[1,3], 兰巨龙[1,3], 王清贤[1,2], 郭毅[1,2]

1. 解放军信息工程大学, 郑州 450002
2. 数字工程与先进计算国家重点实验室, 郑州 450002
3. 国家数字交换系统工程技术研究中心, 郑州 450002
* 通信作者. E-mail: qiuhan410@aliyun.com

收稿日期: 2016–11–08; 接受日期: 2017–04–05; 网络出版日期: 2017–07–24
国家自然科学基金 (批准号: 61502528, 61402525, 61402526) 资助项目

摘要 针对 BGP 协议自适应机制缺陷, 精心设计的攻击可使域间路由系统路由节点级联失效, 从而导致整个域间路由系统崩溃. 这类攻击的触发流量和响应行为均是合法的, 对该类攻击的检测是网络安全领域研究的重难点课题之一. 首先, 本文分析现有可导致域间路由系统级联失效的攻击方法, 提出 BGP 级联失效攻击的两阶段攻击模型, 分析各阶段攻击特征和攻击起效时间. 接着, 根据不同的攻击阶段, 对现有 BGP 级联失效攻击的检测方法进行分类和阐述, 从实时性、准确性和代价等多方面进行了综合评价. 最后, 对当前研究存在的问题进行总结, 并对未来研究发展进行展望.

关键词 域间路由系统, 级联失效攻击, 检测, 两阶段攻击模型, 攻击起效时间

1 引言

作为互联网骨干路由协议, BGP (border gateway protocol) 协议负责连接各 AS (autonomous system) 域, 实现域间互联, 其安全对互联网的可用性、可靠性具有决定性的影响. 近年来, 研究者们提出一系列针对 BGP 协议自适应机制缺陷精心设计的攻击, 典型的有异常 Update 攻击 [1]、BGP 压力攻击 [2]、CXPST (coordinated cross plane session termination) 攻击 [3]、DNP (distributed network paralyzing) 攻击 [4] 等, 这类攻击能够导致域间路由系统崩溃, 造成严重的危害. 特别是 Schuchard 等 [3] 在 NDSS 2011 会议上提出的 CXPST 攻击 (即 “数字大炮”), 通过对精心挑选的少量域间路由链路实施 ZMW 攻击 [5], 可导致整个互联网崩溃, 防御措施基本无效且需要数天时间互联网才能恢复. 调查报告显示, 此类攻击已逐渐出现在现实网络之中 [6].

这类攻击以关键路由节点或路由链路为打击目标, 打击成功后将导致相关联的路由节点洪泛大量 Update 报文, 并使得原本流经的数据流量转至他处, 洪泛的 Update 报文和重定向的数据流量将共同

引用格式: 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. 中国科学: 信息科学, 2017, 47: 1715–1729, doi: 10.1360/N112016-00259
Qiu H, Li Y F, Lan J L, et al. Research on cascading failure attack and detection of inner-domain routing system (in Chinese). Sci Sin Inform, 2017, 47: 1715–1729, doi: 10.1360/N112016-00259

导致相邻路由节点的过载崩溃和重启, 从而产生新的 Update 报文洪泛和数据流量重定向, 周而复始直至整个域间路由系统陷入崩溃状态. 鉴于这种级联失效的现象, 我们将此类攻击统称为 BGP 级联失效攻击. BGP 级联失效攻击可以由数据平面发起的 LDoS (low rate denial of service) 攻击触发 [3, 4], 也可以由控制平面注入的大量合法 Update 报文触发 [1, 2], 其攻击触发流量和攻击带来的反应都是合法的. 因此, 这类攻击很难被检测.

目前, 已有的域间路由系统安全技术主要是基于特征检测的方法, 针对 BGP 路由真实性验证缺乏的问题提出解决方案, 无法用于此类攻击的检测 [7~9]. 我们在文献 [10, 11] 中基于异常检测的思路, 定义 BGP 路由信息统计特征作为安全指标, 前者提出基于路由路径长度和路由事件发生频率的域间路由节点安全状态评估算法, 现网数据分析表明该方法能较好地识别前缀劫持攻击, 后者提出基于线性加权的混合云模型, 实验表明其能感知域间路由系统的控制平面和数据平面攻击. 我们认为, 通过对级联失效攻击过程的回溯, 可利用 LDoS 攻击检测方法以实现对 BGP 级联失效攻击的数据平面触发流量的早期发现 [12]. 迄今为止, 对于 BGP 级联失效攻击检测尚缺少成熟、系统的解决方案. BGP 级联失效攻击隐蔽性强、效能大, 对域间路由系统安全乃至国家网域安全具有严重威胁, 亟需展开深入研究.

本文从安全检测角度对 BGP 级联失效攻击的机理和方法展开深入研究, 定义 BGP 级联失效攻击两阶段模型并分析各阶段攻击起效时间, 从实时防御角度给出 BGP 级联失效攻击检测思路, 并对现有方法进行分类总结和定性评价, 最后对未来发展趋势进行展望, 希望能为相关领域研究提供有益启示.

2 BGP 级联失效攻击机理

异常 Update 攻击 [1] 是恶意的路由器向多个选定的对等路由器发送精心构造的恶意 Update 报文, 这些恶意 Update 报文经由可靠路由器转发至关键 BGP 节点, 从而导致关键 BGP 节点内存耗尽. 该攻击实施的前提是攻击者获得了穿越 AS 域中合法 BGP 节点的控制权.

BGP 压力攻击 [2] 选定大量关键 BGP 节点, 同时向其周期性地注入大量 Update 报文, 导致 BGP 节点路由表过载、BGP 会话重启, 产生大量新的 Update 报文致使路由系统负担加重, 超出大量 AS 的能力和容量, 从而导致互联网级联失效. 该攻击实施的前提是能够与合法 BGP 路由器建立 BGP 会话.

CXPST 攻击 [3] 是一种以 ZMW 攻击 [5] 为基础, 利用互联网的数据平面和控制平面共享物理资源这一现状发展而成的域间路由系统攻击方法. DNP 攻击 [4] 在 CXPST 基础上给出了自动化攻击实施方案. 这类攻击的基本思路是通过网络拓扑结构计算关键路径, 利用僵尸网络对关键路径上的多条 BGP 链路实施 ZMW 攻击, 造成多个关键 BGP 会话在断开与重建中不断切换; 接着, 路由协议将这种状态转换持续向外扩散, 使得网络拓扑急剧震荡, 路由器不断计算路由表并向外扩散; 最后, 几乎每台 BGP 路由器都接收到超出自身处理能力的 Update 报文而崩溃, 从而整个网络瘫痪. 该类攻击实施的前提是可获取整个域间路由系统拓扑, 具有足够带宽和性能的攻击节点, 无需拥有路由节点的控制权.

由此可知, BGP 级联失效攻击通过多个关键 BGP 节点/链路的失效造成相关联的路由节点级联失效, 从而使得整个域间路由系统陷入崩溃状态, 其攻击过程包含了关键路由节点/链路攻击和关联路由节点级联失效两个阶段. 这两个阶段, 在时间上存在顺序关系, 在攻击效果上存在着依赖关系. 为了更好地研究 BGP 级联失效攻击, 定义攻击起效时间, 分别对两个阶段进行分析.

定义1 攻击起效时间描述从攻击流量发起到预期攻击效果达成所经历的时间, 用 T 表示.

对于 BGP 级联失效攻击, 其攻击起效时间 $T_{\text{BGP-CFA}}$ 存在下列关系:

$$T_{\text{BGP-CFA}} = T_1 + T_{1,2}, \tag{1}$$

其中, T_1 表示关键路由节点/链路攻击起效时间, $T_{1,2}$ 表示从关键路由节点/链路失效到整个网络瘫痪所经历的时间.

2.1 关键路由节点/链路攻击机理

关键路由节点/链路攻击阶段可以是大量合法 Update 报文触发的针对关键路由节点的攻击 [1,2], 也可以是 ZMW 攻击触发的针对关键路由链路的攻击 [3,4], 由此, BGP 级联失效攻击可以分为控制平面注入和数据平面阻塞两大类.

2.1.1 控制平面注入类

控制平面注入类 BGP 级联失效攻击主要是通过同时向选定的多个关键节点直接或间接注入大量的 Update 报文, 导致 BGP 会话中断. 从攻击实施上, 都包括了关键节点选取、攻击载荷构造和 Update 报文注入 3 个步骤. 其中, 关键节点选取的好坏决定了关联路由节点级联失效这个阶段能否成功. 从攻击者的角度而言, 关键节点是能够使得攻击效能最大化的那些节点, 文献 [2] 中给出了关键节点选择的 3 条原则, 具体包括拥有很多 AS 邻居、数量尽可能多和分布尽可能广. 所构造的攻击载荷都是合法的 Update 报文, 从报文的数据特征来看, 异常 Update 攻击为确保 Update 报文能够被转发至选定的关键节点, 所构造的 Update 报文中包含特殊 IP 地址块, 例如 123.101.128.0/24 等 [1]; 而 BGP 压力攻击采用直接向关键节点注入的方式, 为避免被检测, 所构造的 Update 报文中不包含特殊 IP 地址 [2].

异常 Update 攻击和 BGP 压力攻击都是当抵达同一关键 BGP 节点的 Update 报文数量达到阈值 (与该 BGP 节点的内存容量成线性关系), 即会造成该关键 BGP 节点的内存耗尽. 从消息注入到导致关键路由节点失效所耗费的时间上来看, BGP 压力攻击采用直接向关键 BGP 节点注入的方式, 其关键路由节点攻击起效时间为 Update 消息注入到关键 BGP 节点资源耗尽的时间, 记为 $T_1^{\text{BGP-S}}$, 主要为 BGP 的内存被全部占用所需要的时间, 则有

$$T_1^{\text{BGP-S}} = \frac{\frac{M_R}{M_U} \times L_U}{R_R}, \tag{2}$$

其中, M_R 为关键 BGP 节点的内存, M_U 为平均每条 Update 消息消耗的内存, L_U 为平均每条 Update 消息的长度, R_R 为 BGP 节点的链路容量. 典型条件下 [1], M_R 为 1024 MB, M_U 为 4 KB/条, L_U 为 108 字节/条, R_R 为 100 Mbps, 则 $T_1^{\text{BGP-S}}$ 的值为 2.2 s.

对于异常 Update 攻击而言, 其关键路由节点攻击起效时间为 Update 消息从注入到抵达关键 BGP 节点并导致处理队列拥塞的时间, 记为 $T_1^{\text{BGP-AUP}}$, 则有

$$T_1^{\text{BGP-AUP}} = T_1^{\text{BGP-S}} + \sum_{i=1}^{K}[t_r(i-1,i) + t_p(i)], \tag{3}$$

其中, K 为注入点到关键路由节点的路径上的路由节点个数, 取值区间为 [0, 255]; $t_r(i-1,i)$ 为 Update 报文在 $i-1$ 节点和 i 节点间的传输时延; $t_p(i)$ 为 Update 消息在第 i 个节点经历的时延. 攻击假设传

输路径上的 BGP 链路并不拥塞, $t_r(i-1,i)$ 可忽略不计. 又当路由器重载条件下, Update 报文在 BGP 节点经历的最大时延为 4 s [1], 可得

$$T_1^{\text{BGP-AUP}} = T_1^{\text{BGP-S}} + 4K. \tag{4}$$

2.1.2 数据平面阻塞类

数据平面触发 BGP 级联失效攻击的关键链路攻击阶段同样包括了关键链路选取、攻击流规划和 ZMW 攻击 3 个步骤. 在关键节点选取上, 文献 [3] 给出了基于路径地图的关键链路选取方法, 文献 [4] 在此基础上提出基于给定攻击资源的关键链路选择和流量定向方法. 攻击流规划主要是针对攻击流的路径、流量进行计划和分配, 在避免上下行链路拥塞的同时使得攻击流量在关键链路处汇聚. ZMW 攻击则是通过向关键链路持续发送周期性的 LDoS 数据包, 导致关键路由节点缓冲区拥塞无法及时处理用于保持链接的控制数据包, 从而导致 BGP 会话断开 [5].

与普通的 LDoS 攻击相比 [12], ZMW 攻击要使得目标关键节点的 Hold Timer 超时才能造成 BGP 会话断开, 其关键链路攻击起效时间为从攻击流量发出到 BGP 会话断开时间, 记作 $T_1^{\text{BGP-ZMW}}$, 即有

$$T_1^{\text{BGP-ZMW}} = t_{\text{K-A}} + t_{\text{BGP-HT}}, \tag{5}$$

其中, $t_{\text{K-A}}$ 表示从攻击流量发出到造成 BGP 会话中断的第一个 Keep Alive 包丢弃所经历的时间, $t_{\text{BGP-HT}}$ 为路由器 Hold Timer 设定值, 对于 Cisco 路由器而言, $t_{\text{BGP-HT}}$ 为 180 s, 对于 Juniper 路由器, $t_{\text{BGP-HT}}$ 则为 90 s. 由于攻击流是周期发出的脉冲流, Keep Alive 包也是周期发出的, 因此, 要想成功造成 BGP 会话中断, 攻击流需要使得定时器重启后的第一个 Keep Alive 包丢失, 即攻击流的第一个分组就能造成 TCP 拥塞丢包, 则有

$$T_1^{\text{BGP-ZMW}} = t_L + t_{\text{BGP-HT}}, \tag{6}$$

其中, t_L 表示第一组突发长度为 L 的攻击数据包从发出到导致 TCP 拥塞丢包的时间. 为了能够引起 TCP 拥塞机制超时且躲避检测, L 一般设定在 (RTT, 2RTT) 之间, RTT (round-trip time) 为 TCP 往返时间, 因此, t_L 应在 (2RTT, 3RTT) 之间 [12]. 由此, 可得

$$T_1^{\text{BGP-ZMW}} \leqslant 3\text{RTT} + t_{\text{BGP-HT}}. \tag{7}$$

基于僵尸网络的高协同性 [13,14] 和攻击流时间同步算法 [5,15,16], ZMW 攻击更倾向于分布式实现. 因此, ZMW 攻击流属于 LDDoS (low rate distributed DoS) 攻击流的一种 [17], 聚合的攻击流呈现 LDoS 流特征, 即周期性、短时高速脉冲, 就数据而言, 并无显著特征.

2.2 关联路由节点级联失效攻击机理

由于域间路由系统的开放性和关联性, 无论是控制平面还是数据平面触发的关键路由节点/链路失效, 系统都将进入震荡状态, 其状态的不断变化将通过大量 Update 报文向相邻路由节点扩散, 造成网络拓扑的急剧震荡、路由表的不断计算和 Update 报文洪泛, 最终大量路由节点过载, 网络陷入瘫痪.

关联路由节点级联失效攻击阶段并没有直接的攻击流量和清晰的攻击过程, 而是在关键路由节点/链路攻击奏效的情况下, 节点/链路状态震荡在域间路由系统内部的传播. 文献 [2] 面向 BGP 压力

攻击效果提出 AS 级别的级联失效模型, 以 AS 域作为节点、AS 间的连接作为边, 以注入 Update 报文为触发条件, 重点研究网络的同步和共振现象. 其中, 节点用包含初始、学习、超载和失效等 4 个状态的有限状态机来描述, 基本传播原理是当一个节点因路由表过载失效时, 周围的节点会撤回所有从失效节点学习的路由, 路由的撤回导致路由更新信息, 从而引发新一轮的路由过载节点失效. 文献 [3, 4] 并没有对级联失效攻击进行理论分析, 主要通过仿真实验来证明级联失效的效果.

由于 BGP 级联失效效应具有极大的破坏性, 且涉及路由节点数量庞大, 无法在实际网络中开展实验, 而基于小型实验网络获取的级联失效实验结果可信性较差 [18~20], 许多研究者们基于复杂网络理论对 BGP 级联失效现象开展研究. 胡乔林等 [21, 22] 提出了攻击条件下的网络拓扑健壮性评估方法、基于介数的路由变化特性分析方法, 以介数为主要指标对路由节点失效下的域间路由系统健壮性进行分析评估; 文献 [23] 对文献 [2] 中的 AS 级别级联失效模型进行了改进, 提出了 CFM (cascading failure model) 模型, 以节点度的大小为依据定义节点的初始负载和额定负载, 引入节点摘除攻击, 通过设置扰动致使节点过载乃至失效, 节点失效后本应从这些节点经过的流量将按照一定的流量转移规则转至其邻居节点, 导致其他节点超载而崩溃, 形成连锁反应而导致网络失效; 与文献 [23] 的思想类似, Wang 等 [24] 在 BGP 级联失效模型中引入了摘除边的攻击. Liu 等 [25] 以 CXPST 攻击为出发点, 以域间链路的失效作为级联失效传播的发起点, 提出了 CAFEIN (cascading failures in inter-domain routing system) 模型, 并基于该模型评估了恶意攻击和随机故障的效果 [26]. CAFEIN 模型包括拓扑构建、域间路由和链路状态评估 3 个相互连接的组件, 级联效应通过时间迭代来模拟, 具体请参考文献 [25] 中图 3. 其中, 拓扑构建组件通过实际拓扑、初期失效和拥塞链路来构建虚拟拓扑; 域间路由组件用来模拟域间路由过程, 所有 AS 域路由选择均服从 customer-prefer 和 valley-free 特性, 域间链路的负载由经过链路的路径数、源 AS 规模和目的 AS 规模共同决定; 链路状态评估组件用来评估链路是否拥塞, 链路的拥塞属于 “虚拟断开”, 当路由更新时流量被迁移到其他链路, 该链路将被恢复并进行路由交换. 模拟实验表明, 级联效应在关联 AS 的链路容量低时将被放大, 且有目的攻击造成的攻击效果并不比随机故障带来的影响更显著. Yang 等 [27] 引入了域间路由系统介数, 提出了基于域间路由系统介数的模型, 主要分析节点在级联失效时的动态行为, 引入路由重启时延、更新报文存活时延来分析域间路由节点重启、失效的真实过程.

根据上述研究成果, 可知级联失效攻击在足够的、合适的关键节点/链路失效下, 1 个小时的攻击将使得每路由节点每秒需处理的 Update 数据包平均数量上升到 138 个以上 (文献 [1] 中, 20 min 的攻击将使每 5 s 到达的 Update 数据包达到 728 个以上; 文献 [26] 中, 1 h 的攻击将使 3 min 内到达的 Update 数据包在 2.5×10^4 以上), 此时, 网络基本陷入瘫痪, 由此, $T_{1,2}$ 典型值可取为 1 h.

综上所述, BGP 级联失效攻击过程如图 1 所示. 其中, 序号 1.x 或 1.$x.y$ 代表关键路由节点/链路攻击阶段的时序事件, 序号 2.x 或 2.$x.y$ 代表关联路由节点级联失效环节阶段的事件, x 表示时间先后, y 为事件编号, 虚线箭头表示后续事件择一发生. 无论第一阶段关键节点失效还是关键链路失效, 第二阶段都会产生 Update 报文广播和流量重定向, 从而导致关联节点和关联链路失效, 进一步导致更多的节点和链路失效, 直至整个网络瘫痪. 依据式 (2), (4) 和 (7), 控制平面注入类攻击若采用直接注入方式则其第一阶段攻击起效时间为 2.2 s, 否则其在 [6.2, 1022.2] s 之间, 数据平面阻塞类第一阶段攻击起效时间为 180.5 s 以上; 从关键路由节点/链路失效到整个网络瘫痪所经历的时间 $T_{1,2}$ 为 1 h.

3 BGP 级联失效攻击的检测

文献 [28] 从攻击触发机理入手提出 5 种措施阻止 CXPST 攻击实施，但不能用于检测且可行性较

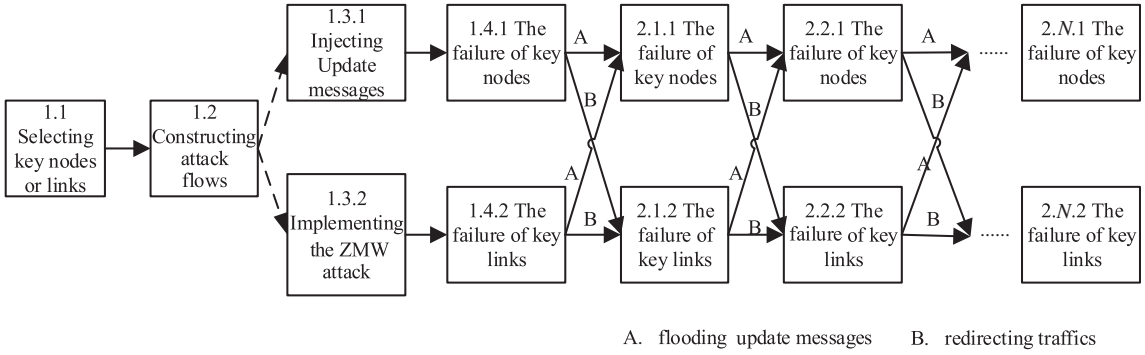


图 1 BGP 级联失效攻击过程

Figure 1 The process of the BGP cascading failure attacks

差. 根据第 2 节的分析, 无论数据平面阻塞类还是控制平面注入类 BGP 级联失效攻击, 其攻击过程都包含关键路由节点/链路攻击和关联路由节点级联失效两个不同阶段, 这两个阶段中攻击流量、BGP 节点/链路状态各异, 因此, 可从两个攻击阶段分别入手, 以实现对 BGP 级联失效攻击的检测. 正是由于攻击所处的阶段不同, BGP 节点/链路状态不同, BGP 级联失效攻击的实时防御和响应对于检测的实时性提出了较高的要求.

3.1 关键节点/链路攻击的检测

根据关键节点/链路攻阶段的触发流量和目标类型, 关键节点/链路攻击检测可以分为控制平面注入关键节点攻击检测和数据平面阻塞关键链路攻击检测.

3.1.1 控制平面注入关键节点攻击的检测

控制平面注入关键节点攻击采用大量合法的 Update 报文注入关键节点, 可采用特征检测或者异常检测的方法检测 Update 攻击流. 从攻击造成的结果而言, 控制平面注入关键节点攻击将导致关键节点的失效和 BGP 会话重启, 为此, 还可通过监测关键节点运行状态变化进行攻击的检测.

由第 2 节分析可知, 异常 Update 攻击所构造的 Update 报文中包含特殊 IP 地址块, 其数据具有明显的特征字, 采用特征匹配的方法能够实现在攻击起效时间 $T_1^{\text{BGP-S}}$ 内的快速识别 [29,30]. BGP 压力攻击所构造的 Update 报文中不包含特殊 IP 地址, 更适合异常检测的方法.

目前, 针对构造的合法 Update 攻击流检测和关键节点运行状态变化监测的研究较少, 可以借鉴域间路由系统攻击检测方面的研究成果, 具体在 3.2 小节详述.

3.1.2 数据平面阻塞关键链路攻击的检测

数据平面阻塞关键链路攻击主要是针对选定的多个关键链路发起 ZMW 攻击, 依据第 2 节的分析, ZMW 攻击具备 LDDoS 攻击的特点, 即为分布式攻击流, 其聚合攻击流量服从 LDoS 攻击流特征. 为此, 针对数据平面拥塞关键链路攻击的检测可以运用已有的 LDoS/LDDoS 攻击检测方法进行 ZMW 攻击的发现, 在 ZMW 攻击起效时间 $T_1^{\text{BGP-ZMW}}$ 内可实现检测的方法优先.

LDoS 攻击的检测研究由来已久, 主要包括时域分析和频域分析两类算法, 时域分析算法一般识别率低、误报率高、实时性好, 而频域分析算法识别率较高、误报率低, 但实时性较差 [31]. 然而, 由于 LDDoS 攻击采取攻击流同步算法 [15], 其分布式的攻击流具有更小的突发时长、峰值速率和更长的周

期 [17], LDoS 攻击检测方法在进行 LDDoS 攻击检测时并不能完全奏效. 其中, 基于攻击流特征识别的 LDoS 检测方法在用于 LDDoS 攻击检测时, 将因无法识别出分布式攻击流从而提取聚合流特征而失效 [31], 而基于攻击流与正常流量差异的检测方法仍可用于 LDDoS 攻击检测, 这类方法主要包括基于信息度量的检测方法 [32] 和基于相关性的检测方法 [33,34]. 针对 LDDoS 攻击流的检测研究则主要集中在 LDDoS 攻击流特征分析 [35,36] 和基于攻击流行为分析的检测方法 [17,37], 这两类方法针对每个流进行检测, 能够识别出分布式的攻击流.

(1) 基于聚合流与正常流差异的检测. 基于信息度量的检测方法 [32] 是在假设正常流量和攻击流量的特征分布 (例如源 IP 地址或者分组长度) 分别为分形 Gauss 噪声分布和 Poisson 分布的基础上, 提出了分离度优于 Shannon 熵和 KL 距离的广义熵和信息距离, 同时, 证明了信息距离具有累加性和非对称性, 指出聚合流的信息距离可以由独立流的信息距离累加而成. 该方法需要在所有的路由器上进行流量采样和信息距离计算, 能够实现对 LDDoS 攻击的发现, 还可对分布式攻击流量发起网络进行回溯, 但尚不能实现分布式攻击流的识别.

文献 [33] 利用秩相关系数能够较好区分攻击流和正常流这一研究结果, 引入 SRC (spearman rank correlation) 和 PRC (partial rank correlation) 两个参数对任意两个流分布的相似性进行度量, 选取源 IP、目的 IP 和协议作为攻击流的属性特征, 通过现网数据分析说明了 SRC 和 PRC 可以有效区分攻击流量和正常流量, 且 PRC 有更好的区分效果. 文献 [34] 基于循环卷积的互相关算法分析了攻击流量与混合流量的互相关序列, 发现该互相关序列具有和攻击流量相同的周期, 指出可利用基于循环卷积的互相关算法预估计出峰值速率、突发时长和周期等关键参数, 从而构造出检测序列. 通过计算当前网络流量序列与检测序列的互相关序列, 分析其峰值的分布特征, 根据无攻击流量的互相关序列峰值均值较小而含攻击流量的互相关序列峰值较大这一事实, 可以识别有无 LDoS 攻击的存在.

由上可知, 基于聚合流与正常流差异的检测无需识别每条分布式攻击流以计算度量参数, 可同时用于 LDoS 和 LDDoS 检测. 这类方法属于时域统计分析, 具有较好的实时性. 鉴于上述文献并未研究统计时长与检测准确率的关系, 我们暂且将其采用的统计时长 (分别为 300 s [32,33], 20 s [34]) 作为检测所需时长, 由此可知, 基于循环卷积互相关的检测方法能够在攻击起效前实现 ZMW 攻击检测.

(2) 基于分布式攻击流特征分析的检测. 尽管采取不同的攻击流分配算法 [17], LDDoS 流仍然具有 LDoS 攻击流的周期性、突发性等特点, 只是其突发时长和周期难以预估, 且大规模僵尸网络协同条件下单一攻击流量的突发时长更短、周期更长, 难以提取. 基于分布式攻击流特征分析的检测方法, 通过对分布式攻击分组特征、流特征的深入挖掘, 定义基于统计的度量参数, 基于特征检测的方法进行 LDDoS 检测, 这类方法在检测攻击的同时能够识别出分布式攻击流.

文献 [35] 分析了文献 [17] 给出的 4 种攻击流分配方案, 定义了 mipdv (mean Internet protocol packet delay variation), 鉴于 LDDoS 攻击流的周期性, 其 mipdv 理论值为 0, 而 TCP 流的 mipdv 则由发送数据和链路状态所决定, 其理论值远大于 0. 基于这一想法, 文献 [35] 提出了 ILF (ipdv-based LDDoS filtering) 方法, 通过在路由器之前或者路由器上基于每个流的前 7 个数据包计算 mipdv, 根据 mipdv 的值判断是否为攻击流, 在此基础上进一步对攻击流过滤. ILF 检测方法不需要在所有路由器上部署, 成本较低, 且只需要根据前 7 个数据包计算, 可硬件实现, 能够在 10 ms 内实现 LDDoS 攻击流检测.

文献 [36] 利用分布式攻击流的分组速率呈周期性变化这一特点, 提取源 IP 的熵、IP 源的变化和分组速率作为网络流量的特征, 在此基础上定义了 FFSc (feature feature scores) 进行攻击流的检测.

(3) 基于分布式攻击流行为分析的检测. 文献 [17] 指出正常 TCP 流积极避免网络拥塞, 而攻击流则导致网络拥塞, 在出现 TCP 拥塞时, 攻击流速率变化缓慢, 正常流速率则迅速降低. 基于这一现

象, 定义了 CPR (congestion participation rate) 对流在 TCP 拥塞时的速率变化进行度量, 具体的, 流的 CPR 等于拥塞出现时该流的到达分组数与该流所有到达分组数的比值, 在拥塞发生时, 正常 TCP 流和 LDDoS 流的平均最小 CPR 差值为 0.683, 足以区分出 TCP 流和 LDDoS 流. 为了应对没有拥塞出现时, 攻击流与正常 TCP 流的 CPR 值均为 0 的极端情况, CPR 度量需与 RED (random early detection) 队列管理机制配合使用, 可在识别出攻击流的同时进行防御. 基于 CPR 的检测方法也属于时域统计分析, 其检测时间与抽样的时长有关, 由于拥塞发生在攻击流量突发时, 持续两次突发即可实现检测, 由此检测时间应大于攻击流的两个周期 (依据文献 [17] 中的攻击流分布算法, 当采用攻击频率聚合时攻击流的周期最长, 具体可用 $\min \mathrm{RTO} \times N$ 估计, 其中 min RTO (retransmission timeout) 为 TCP 的最小超时重传时间, N 为分布式攻击流的个数), 记为 $2 \min \mathrm{RTO} \times N$.

文献 [37] 认为在进行攻击防御时, 存在攻击成本和可检测性之间的博弈, 防御机制要么提高攻击成本, 要么提高攻击可检测性. 基于这种想法, 该文发现在增加拥塞链路带宽时, 正常 TCP 流的发送速率随之增加, 而攻击流的速率由于成本原因不能及时提高, 因此, 通过对拥塞链路带宽增加时流吞吐量变化的监控可以识别出攻击流和正常 TCP 流. 这种方法需要对拥塞链路进行扩容和监控, 在通常的网络中难以实现, 为此, 设计了基于 SDN (software-defined network) 的 SPIFFY (scalable persistent indistinguishable link-flooding attacks with reduced cost asymmetry) 方案. SPIFFY 也属于时域统计分析方法, 文中对 20 s 数据进行分析, 实验表明 15 s 时正常 TCP 流的吞吐量出现显著变化, 由此, SPIFFY 的检测时间可设为 20 s.

综上可知, 基于分布式攻击流行为分析的检测方法主要基于攻击流与正常 TCP 流在链路拥塞时、拥塞链路扩容时的行为不同提出相应的度量指标, 能够有效区分攻击流和正常 TCP 流, 但对于攻击流和 UDP 流的识别尚待进一步研究. 这类方法属于主动式检测, 在识别同时可进行防御, 但需要 RED 或者 SDN 配合实施.

3.2 关联节点级联失效的检测

针对关联节点级联失效检测的研究相对较少, 可借鉴域间路由系统攻击检测的相关研究成果. 在域间路由系统的攻击检测方面, 已有研究主要集中在针对异常域间路由的识别上, 用以应对 BGP 协议存在的路由真实性验证机制缺陷所导致的安全问题, 具体可划分为基于集中分析的攻击检测和基于协同验证的攻击检测.

基于集中分析的攻击检测基本原理是: 利用部署在网络各处的数据采集节点收集域间路由信息并上传至中心服务器, 由中心服务器对所有路由信息进行分析检测. 此类检测方法的典型研究有: Yin 等 [38] 提出的基于签名的域间路由安全监测方案, 可以识别出那些虚假的或是违反用户策略的路由并将其剔除. Kim 等 [39] 提出的 GRADUS 服务构建路由数据库, 基于网络运营商提供的策略信息进行违背策略的路由检测; Osterweil 等 [7] 提出的 TASRS 系统, 以 DNS 和 DNSSEC 为基础构建 Internet 号码资源的证书管理架构, 对每个域间路由器的允许状态集合进行积极监管; Feamster [40] 的 Bogon 系统可监控私有地址或未分配地址是否出现在路由前缀中; Guo 等 [8] 的 ITMM 模型利用生物免疫机制可检测异常域间路由和异常节点.

不同于基于集中分析的攻击检测方法, 基于协同验证的攻击检测利用 AS 之间询问 - 应答的方式共享路由信息, 形成全面的监测信息集合从而识别虚假路由. 典型研究有: Thaler 等 [41] 提出的分布式域间路由故障诊断结构, 可用于检测并剔除掉那些违背用户路由策略的域间路由; Wu [42] 提出的基于路由交互的域间路由监测系统, 可通过各 AS 协同验证识别虚假路由; Goodell 等 [43] 提出的 IRV 服务方案, 通过在各 AS 设立查询服务器构成一个分布式查询系统, 供 AS 查询并验证其收到的 BGP 路

由的真实性; Wang 等 [44] 提出的 SDS 方法与 IRV 类似, 但进一步增加了 UMAC 加密认证功能, 从而提高了对源 IP 地址认证的有效性; Guo 等 [45] 提出的 DAIR 机制则规定参与节点通过查询全局邻接信息, 验证路由信息中的 AS 路径是否被伪造或篡改.

由于关联节点级联失效阶段所产生的大量 Update 报文, 属于合法的、真实路由消息, 上述基于身份认证、特征检测的异常路由攻击检测方法将无法奏效. 文献 [10] 基于异常检测的思路, 引入路由事件发生频率对每天的 Update 报文数量进行刻画, 基于平均路径长度、路径编辑距离和路由事件发生频率定义路由节点的综合安全特征, 在此基础上, 借助二维正态云模型定义域间路由节点安全状态评估模型 CSSAM, 从而实现由定量数值对安全状态的定性描述. 利用 RouteViews 提供的正常 BGP 路由信息数据构建路由节点的安全正常态, 通过对路由节点安全特征偏离正常态的度量获得路由节点被威胁的概率, 50% 以上的威胁概率意味着可能遭受攻击. 文献 [11] 在文献 [10] 的基础上, 针对域间路由系统可能遭遇的控制平面和数据平面威胁进行分析, 定义 FAM (frequency of announce message)、FWM (frequency of withdraw message)、APL (average aspath length) 和 APED (average aspath edit distance) 为安全特征, 并基于正态云模型为每个安全特征建立正常状态子模型, 基于这些子模型建立加权混合模型 MAF-SAM, 由此可通过计算路由节点安全特征偏离正常态的值获得路由节点的威胁概率. 实验表明, 该方法可实现对前缀劫持、AS 路径篡改、路径泄露和数据平面阻塞类级联失效攻击的感知. 文献 [10] 以天为单位进行路由事件发生频率的统计, 在以小时为单位进行安全评估时, 需要等比例放大 Update 报文数量, 文献 [11] 将安全特征的统计时长调整为 15 min, 能够较好地实现以小时为单位的安全评估, 由于安全评估的间隔与该阶段攻击起效时间 $T_{1,2}$ 均为 1 h, 能否在攻击起效时间内实现对级联失效攻击的发现尚待进一步的研究. 另外, 基于异常检测的 BGP 路由节点安全状态评估算法可以感知威胁的存在, 尚不能识别出威胁的类型和起源.

3.3 域间路由系统的级联失效攻击检测方法比较

就目前研究情况来看, 可用于域间路由系统级联失效攻击检测的方法众多, 切入点各异, 表 1 分别从检测环节、检测技术、检测时间、代价等方面展示各检测方法之间的差异. 从表 1 可知, 在级联失效攻击的第一阶段, 对数据平面阻塞类攻击的检测方法较多, 主要基于特征检测的思想, 具有较好的实时性、准确率以及较低的代价, 能够实现在攻击起效前发现攻击; 对控制平面注入类攻击的检测方法较少, 在实时性和准确性有待提高, 在攻击起效前发现攻击尚且困难. 目前, 针对关联节点级联失效攻击的检测主要基于异常检测方法, 有先天难以识别攻击类型的缺陷, 在具有较好实时性的同时需要付出较高的代价, 由于异常检测间隔与攻击起效时间相当, 在攻击起效前能否发现攻击尚待进一步研究.

4 研究展望

域间路由系统的级联失效攻击可导致域间路由系统的崩溃, 是近年来国内外研究者关注的热点. 就目前研究而言, 研究者在级联失效攻击原理上基本达成共识, 在级联失效攻击检测研究方面还处于起步阶段. 下面从 3 个方面指出当前研究存在的不足, 并对未来研究进行展望.

(1) BGP 级联失效攻击方法和攻击原理的研究文献 [1~4] 对攻击方法进行了深入的探讨, 认为足够的、合适的 BGP 节点失效或会话失效将导致域间路由系统的级联失效, 重点探讨了对等节点 Update 报文注入和大量 Update 报文直接注入等两种导致 BGP 节点失效的方法和 ZMW 攻击导致 BGP 会话中断的一种方法. 事实上, 足够多的控制平面 (包括路由、运维、管理等) 报文可导致节点失

表 1 BGP 级联失效攻击检测方法比较

Table 1 Comparison of the current detection methods for the BGP cascading failure attacks

The stages and types of attacks			The onset time of attack	The attack detection methods	The identification time	Cost	The identification rate	The false positive rate
The stage of attacking key nodes or links	Injecting attack from the control plane	Abnormal Update messages attack	[6.2,1022.2] s	Feature detection	A few seconds	Low	Low	High
		BGP routing stress attack	2.2 s	CSSAM	1 d	High[a)]	High	High[b)]
				MAF-SAM	1 h	High[a)]	High	High[b)]
	Blocking attack from the data plane		182 s	Detection by information metrics	300 s	It should be arranged on all routing nodes	High	Low
				Detection by relation characteristic	20 s	Low	High	Low
				Detection by ILF	10 ms	Low	High	Low
				Detection by CPR	$2N$ s[c)]	It should be acted with RED	High	High[d)]
				SPIFFY	20 s	It should be implemented on SDN	High	High[d)]
The stage of cascading failure of related nodes			1 h	CSSAM	1 d	High[a)]	High	High[b)]
				MAF-SAM	1 h	High[a)]	High	High[b)]

a) The normal state of model need incremental updated.

b) It cannot identify the threat type.

c) N is the number of distributed attacking flows.

d) It cannot differentiate attack flows with UDP flows.

效, 而 BGP 会话的 Hold Timer 超时可使得关键链路失效, 研究者可以拓展研究范围, 研究新的、隐蔽性更强的攻击方法. 此外, 根据不同的攻击效果, 攻击者可能会提出针对不同攻击目标的攻击方法, 研究出类似文献 [46] 提出的指定网域断网攻击.

文献 [2, 21∼27] 在关联节点级联失效攻击机理方面进行了深入的研究, 基于复杂网络理论建立了 BGP 级联失效模型, 模型以 AS 域为节点, AS 间的连接为边, 以节点或者边之一作为研究对象, 要么考虑节点或者边失效带来的流量重定向这一要素, 流量过载时会导致节点或边的失效, 要么考虑边失效带来的 Update 报文洪泛这一要素. 实际上, BGP 级联失效现象是高度复杂的, 如图 1 所示, 节点或边失效都会带来流量重定向和 Update 报文洪泛, 这两种毁伤要素共同推动着级联失效的发展, 两者相互促进, 并且逐渐扩散; 节点的失效并非由流量过载导致, 而是由 Update 报文过载导致, 节点的崩溃 – 重启 – 再崩溃循环是异步的, 却又因流量重定向和 Update 报文洪泛而存在相互关联; 边的失效则由流量过载导致, 会话的断开 – 建立 – 再断开具有和节点类似的特点 [47]. 在未来的研究中, 需要建立路由器级域间路由系统模型, 以节点和边同时作为研究对象, 定义节点失效和边失效的不同条件, 针对流量重定向和 Update 报文洪泛两种毁伤要素建立级联失效攻击模型, 从而真实描述级联失效的过程.

(2) BGP 级联失效攻击检测方法研究. 由表 1 可知, 虽然 BGP 级联失效攻击的相关检测方法较多, 但是在检测实时性、准确率方面尚不能满足主动防御的要求. 对于 BGP 级联失效攻击检测, 本文认为下一步应重点开展以下 4 方面的研究.

(i) 基于 Update 报文特征分析的攻击检测方法研究. 文献 [11] 通过对数据阻塞类级联失效攻击的分析, 指出该类攻击将导致某些路径处于失效和可用的交替状态, 相关 BGP 节点将向邻居发出大量的 Announce 和 Withdraw 报文, 为此, 定义 FAM 和 FWM 作为 Update 报文的安全特征. 然而, 前缀劫持、路径泄露等攻击也将造成大量的 Announce 报文传播, 在计算出较大威胁概率的情况下, 仅使用 FAM 和 FWM 并不能识别威胁的类型. 另外, 安全特征的计算以 15 min 为统计时长, 威胁概率的计算以 1 h 为间隔, BGP 级联失效攻击的起效时间在 1 h 左右, 能否在攻击起效前发现级联失效攻击尚难确定.

为此, 需要针对级联失效攻击的注入 Update 报文、关键节点/链路失效引起的 Update 报文洪泛进行更进一步的分析, 选取合适的、足够的安全特征 (如 Announce 报文和 Withdraw 报文的比值), 综合异常检测和特征检测方法, 同时考察统计时长对于检测准确性的影响, 以提高对控制平面注入关键节点攻击和关联节点/链路级联失效攻击检测的实时性和准确率.

(ii) 基于 BGP 节点行为监控的攻击检测方法研究. 已有的域间路由节点安全状态检测多是通过分析域间路由路径和域间路由控制消息等对路由节点安全状态进行评估 [8∼11]. 实际上, 无论在关键路由节点/链路攻击阶段还是关联路由节点级联失效阶段, 攻击的成功实施都会带来 BGP 会话的频繁重启, BGP 路由节点资源消耗和行为的频繁变化. 借鉴域间路由节点行为预测相关研究成果 [48, 49], 建立 BGP 节点行为模型, 与基于 Update 报文特征分析的检测方法相结合, 可进一步识别攻击类型.

基于 BGP 节点行为监控的攻击检测方法需要对 BGP 节点行为和资源消耗进行监控, 必须具备 BGP 节点的管理权限, 需要各个运营商的协同配合, 对资源消耗和行为的监控更加直接, 安全特征计算复杂度低; 基于 Update 报文特征分析的攻击检测方法只需要对 Update 报文等路由消息进行特征分析和提取, 无需拥有 BGP 节点权限, 可由第三方实施, 安全特征计算复杂度高.

(iii) 双维度攻击检测方案研究. 由于数据平面阻塞类级联失效攻击和控制平面注入类级联失效攻击在关联路由节点级联失效阶段呈现相同的攻击特征, 即使识别出存在级联失效攻击, 也难以区分出级联失效攻击的具体类型. 鉴于数据平面阻塞类级联失效攻击和控制平面注入类级联失效攻击在关键

路由节点/链路攻击阶段具有不同的攻击流量特点, 可以对数据平面和控制平面的流量、状态进行综合分析, 建立双维度攻击检测方案, 实现对攻击的精确识别, 以进行有针对性地防御和响应.

具体地, 双维度攻击检测方案即从数据平面和控制平面的双重维度同时进行级联失效攻击的检测, 具体包括数据平面攻击检测和控制平面攻击检测. 数据平面攻击检测主要分析 BGP 链路的业务流量, 可采用平均包时延方差检测法等, 进行 ZMW 攻击检测; 控制平面攻击检测主要分析 BGP 路由节点间的 Update 报文和 BGP 路由节点行为, 可综合采用 Update 报文特征分析检测法和 BGP 节点监控检测法, 进行关键节点注入阶段的异常 BGP 攻击和 BGP 压力攻击检测以及关联节点级联失效攻击的检测. 由于 BGP 级联失效攻击包括两个顺序阶段, 双维度检测结果随时间会发生变化. 当控制平面识别出存在关联节点级联失效攻击时, 回溯之前一定时段的控制平面和数据平面检测结果, 可判定具体的 BGP 级联失效攻击种类.

(iv) 基于攻击者视角的攻击效果预测研究. BGP 级联失效攻击能否产生级联失效的攻击效果, 其所导致的失效范围, 取决于关键路由节点/链路的选取. 在检测出关键路由节点/链路被攻击的情况下, 从攻击者视角出发, 研究被攻击的关键路由节点/链路之间的关系, 预测攻击效果, 明确失效范围, 将有利于防御响应方案的制定.

(3) 基于大规模测试床的实验验证. 当前的研究实验验证大多在研究者自行构建的大规模模拟环境或者小规模实物仿真环境下进行, 这些实验环境与现网环境相比, 进行了大量的抽象和简化, 其实验结果并不能说明所研究方案在现网条件下的有效性 [50]. 为此, 需要在进行模拟仿真实验的基础上, 基于大规模测试床开展复杂网络环境下的实验验证, 明确影响研究方案的关键要素, 进一步调整、优化研究方案.

5 总结

域间路由系统由于其节点间的关联性, 存在着级联失效效应, 为此, 域间路由系统面临着级联失效攻击的严重威胁. 长期以来, 研究者们针对级联失效现象进行了深入研究, 提出了一些级联失效攻击的检测方案, 这些方案能够在一定程度上检测出攻击, 但离实时检测攻击、准确识别攻击源和评估攻击效果相距甚远.

本文对造成域间路由系统级联失效的攻击方法进行了分析和总结, 提出了 BGP 级联失效攻击的两阶段模型, 从安全检测的角度, 讨论了 BGP 级联失效攻击机理, 分析了各阶段攻击起效时间, 进而对各阶段攻击的检测方法进行了审视, 并从实时性、准确性和代价等多方面进行了分析, 最后对当前研究存在的问题提出了一些理解并对未来研究提出了一些建议. 下一步我们将深入研究并提出双维度级联失效攻击检测方案. 域间路由系统的级联失效攻击检测和防御不仅需要研究者在未来继续努力, 还需要运营商和相关互联网管理机构的积极配合, 期望未来我们能够有效应对这类攻击, 减少此类攻击所带来的危害.

参考文献

1 Schuchard M, Thompson C, Hopper N, et al. Taking Routers off Their Meds: Unstable Routers and the Buggy BGP Implementations That Cause Them. UMN CS Technical Report 11-030. 2012

2 Deng W P, Zhu P D, Lu X C, et al. On evaluating BGP routing stress attack. J Commun, 2010, 5: 13–22

3 Schuchard M, Mohaisen A, Foo K D, et al. Losing control of the internet: using the data plane to attack the control plane. In: Proceedings of the Network and Distributed System Security Symposium (NDSS 2011), San Diego, 2010. 726–728

4 Li H S, Zhu J H, Qiu H, et al. The new threat to internet: DNP attack with the attacking flows strategizing technology. Int J Commun Syst, 2014, 28: 1126–1139

5 Zhang Y, Mao Z M, Wang J. Low-rate tcp-targeted DoS attack disrupts internet routing. In: Proceedings of the 14th Annual Network & Distributed System Security Symposium (NDSS 2007), San Diego, 2007

6 Bright P. Can a DDoS break the Internet? Sure... just not all of it. Ars Technica (April 2, 2013). http://arstechnica.com/security/2013/04/can-a-ddos-break-the-internet-sure-just-not-all-of-it/

7 Osterweil E, Amante S, McPherson D. TASRS: Towards a Secure Routing System Through Internet Number Resource Certification. Verisign Labs Technical Report 1130009. 2013

8 Guo Y, Wang Z X. An immune-theory-based model for monitoring inter-domain routing system. Sci China Inf Sci, 2012, 55: 2358–2368

9 Liu X, Wang X Q, Zhu P D, et al. Security evaluation for interdomain routing system in the Internet. J Comput Res Dev, 2009, 46: 1669–1677 [刘欣, 王小强, 朱培栋, 等. 互联网域间路由系统安全态势评估. 计算机研究与发展, 2009, 46: 1669–1677]

10 Guo Y, Zhu J H, Wang Z X, et al. A multi-characteristics-based method for evaluating the security situation of inter-domain routing nodes. Sci Sin Inform, 2014, 44: 527–536 [郭毅, 朱俊虎, 王振兴, 等. 基于多特征的路由节点安全状态评估方法. 中国科学: 信息科学, 2014, 44: 527–536]

11 Guo Y, Duan H X, Chen J, et al. MAF-SAM: an effective method to perceive data plane threats of inter domain routing system. Comput Netw, 2016, 110: 69–78

12 Kuzmanovic A, Knightly E W. Low-rate TCP-targeted denial of service attacks: the shrew vs. the mice and elephants. In: Proceedings of ACM SIGCOMM 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Karlsruhe, 2003. 75–86

13 Qiu H, Li Y, Li H, et al. One-to-any command and control model: precisely coordinated operation on uncooperative controlled nodes. Wuhan Univ Natural Sci, 2015, 20: 490–498

14 Hoque N, Bhattacharyya D, Kalita J. Botnet in DDoS attacks: trends and challenges. IEEE Commun Surv Tut, 2015, 17: 2242–2270

15 Wu Z J, Lan M, Wang M H, et al. Research on time synchronization and flow aggregation in LDDoS attack based on cross-correlation. In: Proceedings of IEEE International Conference on Trust, Security and Privacy in Computing and Communications. Washington: IEEE Computer Society, 2012. 25–32

16 Li H S, Zhu J H, Wang Q X, et al. LAAEM: a method to enhance LDoS attack. IEEE Commun Lett, 2016, 20: 708–711

17 Zhang C, Cai Z, Chen W, et al. Flow level detection and filtering of low-rate DDoS. Comput Netw Int J Comput Telecommun Netw, 2012, 56: 3417–3431

18 Jasmina O, Javier M, Piet V M. Network protection against worms and cascading failures using modularity partitioning. In: Proceedings of the 22nd International Teletraffic Congress, Amsterdam, 2010. 1–8

19 Wang L, Saranu M, Gottlieb J M, et al. Understanding BGP session failures in a large ISP. In: Proceedings of the 26th IEEE International Conference on Computer Communications, Barcelona, 2007. 348–356

20 Kotzanikolaou P, Theoharidou M, Gritzalis D. Cascading effects of common-cause failures in critical infrastructures. In: Proceedings of International Conference on Critical Infrastructure Protection VII. Berlin: Springer, 2013. 171–182

21 Hu Q L, Peng W, Chen X, et al. MFT2-BGP: achieving disruption-free inter-domain routing protocol using multiple forwarding trees. Chin J Comput, 2012, 35: 2023–2036 [胡乔林, 彭伟, 陈新, 等. MFT2-BGP: 基于多转发树的无中断域间路由协议. 计算机学报, 2012, 35: 2023–2036]

22 Hu Q L. Research on key survivability technologies of inter-domain routing protocol. Dissertation for Ph.D. Degree. Changsha: National University of Defense Technology, 2010 [胡乔林. 可生存性域间路由协议关键技术研究. 博士学位论文. 长沙: 国防科学技术大学, 2010]

23 Guo Y, Wang Z X. A cascading failure model for inter-domain routing system, Int J Commun Syst, 2012, 25: 1068–1076

24 Wang Y, Wang Z X, Zhang L C, et al. Situation assessment model for inter-domain routing system. IET Softw, 2013, 8: 53–61

25 Liu Y, Peng W, Su J, et al. Assessing survivability of inter-domain routing system under cascading failures. In: Frontiers in Internet Technologies. Berlin: Springer, 2013. 97–108

26 Liu Y, Peng W, Su J, et al. Assessing the impact of cascading failures on the interdomain routing system of the

Internet. New Generation Comput, 2014, 32: 237–255
27 Yang B, Zhang Y, Lu Y. A new methods for cascading failures analysis in inter-domain routing system. In: Proceedings of the 5th International Conference on Instrumentation & Measurement, Qinhuangdao, 2015. 382–385
28 Zheng H, Chen S, Liang Y. How the cyber weapon "Digital Ordnance" works and its precautionary measures. J Comput Res, 2012, s2: 69–73 [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. 计算机研究与发展, 2012, s2: 69–73]
29 Jing Q L. Design and implementation of interdomain routing security monitoring system. Dissertation for Master's Degree. Beijing: Capital Normal University, 2014 [景全亮. 域间路由安全监测系统的设计与实现. 硕士学位论文, 北京: 首都师范大学, 2014]
30 Li C X. Research on key technologies for inter-domain routing survivability. Dissertation for Ph.D. Degree. Beijing: Beijing University of Posts and Telecommunications, 2015 [李春秀. 域间路由生存性关键技术研究. 博士学位论文. 北京邮电大学, 2015]
31 Wen K, Yang J H, Zhang B. Survey on research and progress of low-rate denial of service attacks. J Softw, 2014, 25: 591–605 [文坤, 杨家海, 张宾. 低速率拒绝服务攻击研究与进展综述. 软件学报, 2014, 25: 591–605]
32 Xiang Y, Li K, Zhou W. Low-rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans Inf Forens Secur, 2011, 6: 426–437
33 Ain A, Bhuyan M H, Bhattacharyya D K, et al. Rank correlation for low-rate DDoS attack detection: an empirical evaluation. Int J Netw Secur, 2016, 18
34 Wu Z J, Li G, Yue M. Detecting low-rate DoS attacks based on signal cross-correlation. ACTA Electron Sin, 2014, 42: 1760–1766 [吴志军, 李光, 岳猛. 基于信号互相关的低速率拒绝服务攻击检测方法. 电子学报, 2014, 42: 1760–1766]
35 Mehmet S. A new metric for flow-level filtering of low-rate DDoS attacks. Secur Commun Netw, 2015, 8: 3815–3825
36 Hoque N, Bhattacharyya D K, Kalita J K. FFSc: a novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis. Secur Commun Netw, 2016, 9: 2032–2041
37 Kang M S, Gligor V D, Sekar V. SPIFFY: inducing cost-detectability tradeoffs for persistent link-flooding attacks. In: Proceedings of Network and Distributed System Security Symposium (NDSS'16), San Diego, 2016
38 Yin H, Sheng B, Wang H. Securing BGP through keychain-based signatures. In: Proceedings of the 15th IEEE International Workshop on Quality of Service, Evanston, 2007. 154–163
39 Kim E, Nahrstedt K, Xiao L, et al. Identity-based registry for secure inter-domain routing. In: Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security, Taipei, 2006. 321–331
40 Feamster N, Jung J, Balakrishnan H. An empirical study of bogon route advertisements. ACM SIGCOMM Comput Commun Rev, 2005, 35: 63–70
41 Thaler D G, Ravishankar C V. An architecture for inter-domain troubleshooting. J Netw Syst Manag, 1997, 12: 516–523
42 Wu J. Passive inter-domain routing monitor based on routing interaction. In: Proceedings of the 6th IEEE International Conference on Computer and Information Technology. Washington: IEEE Computer Society, 2006. 104
43 Goodell G, Aiello W, Griffin T, et al. Working around BGP: an incremental approach to improving security and accuracy of inter-domain routing. In: Proceedings of the Network and Distributed System Security Symposium, San Diego, 2002. 75–85
44 Wang L, Xia T B, Seberry J. Inter-domain routing validator based spoofing defense system. In: Proceedings of 2010 IEEE International Conference on Intelligence and Security Informatics, Vancouver, 2010. 153–155
45 Guo Y, Wang Z X, Liu H S, et al. A cooperation-based mechanism for detecting AS_PATH validity. J Comput Res Dev, 2012, 49: 96–103 [郭毅, 王振兴, 刘慧生, 等. 基于协同的域间路由路径真实性验证机制. 计算机研究与发展, 2012, 49: 96–103]
46 Kang M S, Lee S B, Gligor V D. The crossfire attack. In: Proceedings of IEEE Symposium on Security and Privacy, Berkeley, 2013. 127–141
47 Papadimitriou D, Careglio D, Tarissan F, et al. Internet routing paths stability model and relation to forwarding paths. In: Proceedings of the 9th International Conference on the Design of Reliable Communication Networks, Budapest, 2013. 8875: 20–27
48 Xia N, Li W, Luo J Z, et al. A routing node behavior algorithm based on fluctuation type. Chin J Comput, 2014, 37: 326–334 [夏怒, 李伟, 罗军舟, 等. 一种基于波动类型识别的路由节点行为预测算法. 计算机学报, 2014, 37: 326–334]

49 Zhang W, Bi J, Wu J P, et al. Catching popular prefixes as AS border router with a prediction based method. Comput Netw, 2012, 56: 1486–1502
50 Siaterlis C, Garcia A P, Genge B. On the use of emulab testbeds for scientifically rigorous experiments. IEEE Commun Surv Tutor, 2013, 15: 929–942

Research on cascading failure attack and detection of inner-domain routing system

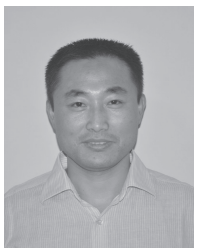
Han QIU[1,2*], Yufeng LI[1,3], Julong LAN[1,3], Qingxian WANG[1,2] & Yi GUO[1,2]

1. *PLA Information engineering University, Zhengzhou* 450002*, China*;
2. *State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450002*, China*;
3. *National Digital Switching System Engineering & Technological Research Center, Zhengzhou* 450002*, China*
* Corresponding author. E-mail: qiuhan410@aliyun.com

Abstract Attacks aiming at the vulnerabilities of a BGP self-adaptation mechanism may lead to a cascading failure of the routers, and the inter-domain routing system may even crash. The safety monitoring technologies of existing inter-domain routing systems cannot efficiently detect an attack because the attack flows and updates are practically valid. This is becoming an important and difficult research topic in the field of network security. In this paper, we first analyze the attack methods that may give rise to a cascading failure of an inter-domain routing system, propose a two-stage attack model of BGP cascading failure attacks, and extract the features and onset time of each attack stage. We then classify and elaborate on the current detection approaches, and evaluate them comprehensively from the perspectives of real-time implementation, accuracy, and cost. Finally, the current research issues are described and possible directions for future research are suggested.

Keywords inter-domain routing system, cascading failure attack, detection, two-stage attack model, onset time of attack

Han QIU was born in 1981. She received her Ph.D. degree in communication and information systems from the PLA Information Engineering University, Zhengzhou in 2008. She is currently an associate professor at PLA Information Engineering University. Her research interests include Internet routing security, modeling, and the evaluation of network security.



Yufeng LI was born in 1975. He received his Ph.D. degree in communication and information systems from PLA Information Engineering University, Zhengzhou in 2008. He is currently an associate professor at the National Digital Switching System Engineering & Technological Research Center. His research interests include routing and switching, network traffic identification, and control.

Julong LAN was born in 1962. He received his Ph.D. degree in communication and information systems from PLA Information Engineering University, Zhengzhou in 2001. He is currently a professor at the PLA Information Engineering University. His research interests include novel network architectures, smart networking, and convergence services and networks.

Qingxian WANG was born in 1960. He received his M.S. degree in computer science and technology from Peking University, Beijing in 1988. He is currently a professor at PLA Information Engineering University. His research interests include network science and security.