高等计算机网路
2020 年秋季学期

论文阅读 3

徐荣琛 2019214518 软件学院 2020 年 10 月 26 日

专题	路由协议安全
题目	Routing Around Congestion Defeating DDoS Attacks and Adverse Network Conditions via Reactive BGP Routing
作者	Jared M. Smith, Max Schuchard
会议	2018 IEEE Symposium on Security and Privacy

本篇论文的主要工作是提出了一种在 DDoS 攻击（包括 Transit-link DDoS 攻击）下可以保障关键自治系统流量的技术——路由阻塞绕行（Routing Around Congestion）。路由阻塞绕行通过伪造环路信息，毒化部分受到攻击或者保障链路附近的自治系统，进而产生一条来自关键自治系统的流量路径，这一过程称为欺诈性路线反向中毒（Fraudulent Route Reverse Poisoning，简称 FRRP）。对于 FRRP 路径，文章提出了两种策略削弱对其他自治系统带来的副作用影响，并随后讨论了基于丢包率的 FRRP 路径择优策略。

文章使用了大量的篇幅进行了实验评估，实验是基于一个模拟环境进行的，模拟过程考虑到实际网络架构、带宽、僵尸网络模型、攻击方法等因素，从多个角度论证了路由阻塞绕行技术可以有效地进行对关键自治系统在 DDoS 下关键流量的保障能力。

总体来看，文章具有以下的突出点：

- 首次显著地改善了 Transit-link DDoS 攻击造成的链路影响；
- 提出的路由阻塞绕行具备良好的推广性，因为其只需要部署在服务器端；
- 较为充分的实验论证，从理论的角度论证了路由阻塞绕行的可行性以及理想情况下的突出效果。

另一方面，个人以为本文还存在着一定的改良空间：

- 实验仅是基于了一个模拟的环境进行，虽然模拟环境考虑到了实际网络架构、带宽、僵尸网络模型、攻击方法等多方面的因素，但是相较于实际互联网而言，仍然是非常理想和简单化的。包括实际互联网之中的协议以及对应协议的实现规则、运营商规则等因素对路由阻塞绕行的可行性提出了非常大的挑战，后续 2019 年 IEEE Symposium on

Security and Privacy 中的论文 On the Feasibility of Rerouting-based DDoS Defenses 对此也进行了广泛的讨论和分析；

- 另外个人对论文中的 FRRP 路径择优也存在着一定的别的观点，因为在 FRRP 路径择优的过程之中，需要多次尝试不同的毒化目标，大量的尝试可能需要非常长的网络收敛时间，这实际可能导致择优结果的实时性不强，进而导致实际之中的不可用性。

总的而言，文章提出了一种 DDoS 攻击下关键流量保障的新思路，并且这个新思路在理论上具备一定的可行性。虽然根据最新的文献阅读，其实际的可行性并不太高，但这样的新思路对于后续的攻击防范设计还是有种非常好的启发式作用，值得更多的研究和讨论。