从图 10 可以看出,实验数据集中,边缘节点及其链路所占比例较大:节点度数为 1 约占总节点数的 54%,所在图的核数小于 3 的节点占总节点的 80%,介数为的 0 节点占总数的 70%.

根据分析结果,在验证监测系统部分关键节点链路情况下 ESCT 方法检测性能时,将所监测的节点分别按照度数、核数和介数的降序进行排列,按顺序将不同数目的节点及其之间的链路加入监测序列.实验采用样本容量均为 350 组,其他实验条件与样本数据集为(WLTD,WSAD)时一致.实验结果如图 11 所示.

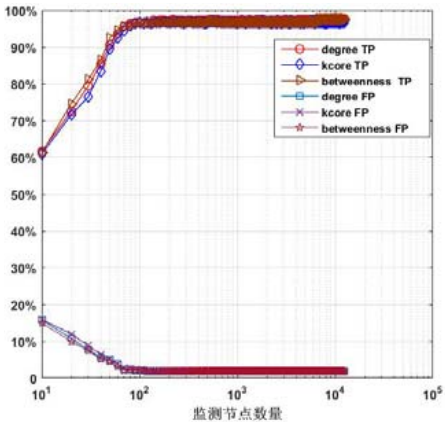


Fig.11 Results of ESCT detectionunder different monitoring conditions

图 11 不同监测条件下 ESCT 检测结果

实验中,随着所监测节点和链路数量的增加,ESCT 方法的 TP 增加,FP 降低.当对 *degree*≥40 的 70 个节点及其之间的链路进行监测时,检测率和误报率分别为 95.46%和 2.41%;对 *kcore*≥14 的 77 个节点及其之间的链路进行监测时,检测率和误报率分别为 95.55%和 2.36%;对 *betweenness centrality*≥0.0045 的 69 个节点及其之间的链路进行监测时,检测率和误报率分别为 95.43%和 2.40%.此后,当监测节点和链路数量继续增加时,ESCT 方法检测率和误报率提升较为缓慢.图 11 结果反映出 ESCT 方法仅需检测系统部分关键节点及其之间的链路便能够取得较好的检测效果,这也意味着在实际系统中部署 ESCT 检测方法时,其监控、计算开销可以控制在合理范围之内.

对比 3 种不同关键节点和链路监测方案的结果也可以看出:尽管所关注的重点不同,3 种监控方案均具备较好的检测结果.这是主要因为 3 种方案所监控的节点和链路重复率较高,在互联网域间路由系统中,度数较高的节点,其介数和核数也较高;同样,介数、核数较高的节点,其度数也往往较高.

3.2 与已有的LDoS攻击检测方法对比

已有的 LDoS 攻击检测不能用于 BGP-LDoS 攻击检测的原因主要有两个方面:① 域间路由系统系统具有一定抗扰动性,仅在单个或多个节点中检测到 LDoS 攻击时,不能判定系统遭遇 BGP-LDoS 攻击;② BGP-LDoS 攻击经过严密的攻击路径规划,通过对少量关键链路发起攻击引发系统级联失效,这也意味着 BGP-LDoS 攻击中,大量节点遭遇的并非是 LDoS 攻击.为验证此判断,进行以下对比实验:

在第 3.1 节搭建的仿真平台下设置两种情景:第一种为 Only-LDoS,在不引发系统级联失效前提下,随机对系统 $n(n>10)$条链路进行 LDoS 攻击;第二种场景为 BGP-LDoS,利用文献[4,5]所用的方法进行 BGP-LDoS 攻击,攻击时利用文献[6]提出的方法进行攻击节点和流量的重新规划.每种场景重复实验 30 次,共计 60 次.为降低实验复杂度,每次实验中,在系统中所有 degree≥40 的节点上利用小波变换分析方法(DWT)[19]和小信号检测分析方法(MSS)[23]对 LDoS 攻击进行检测,记录 60 次实验中检测到 LDoS 攻击节点的数目,记录在数组 $O_{DWT}(i)$, $O_{MSS}(i)$中,其中,i=1,2,…,60.

由于 DWT 和 MSS 方法主要是用于单个节点遭遇 LDoS 攻击的检测,难以直接用于整个域间路由系统的 BGP-LDoS 攻击检测,因此,实验设置利用 DWT 和 MSS 方法检测 BGP-LDoS 攻击时,以遭遇攻击的节点数目作

为阈值来判断 BGP-LDoS 攻击是否存在.例如在第 i 次实验中,若 $O_{DWT}(i)\geqslant\eta$,则认为存在 BGP-LDoS 攻击;否则认为不存在攻击.3 种方法检测结果如图 12 所示.

从图 12 可以看出:当设置较小的η值时,DWT 和 MSS 方法能够有效检测 BGP-LDoS 攻击,但存在非常高的误报率;当η值设置过大时,误报率虽然下降,但其检测率严重降低.对比结果也充分证明了 ESCT 方法在 BGP-LDoS 攻击检测时的有效性.

由于 DWT 和 MSS 两种方法仅检测链路流量,实验对比分析在不同数量的流量检测样本时,3 种检测方法所花费的运算时间.实验进行 60 次,取结果平均值.对比结果如图 13 所示:

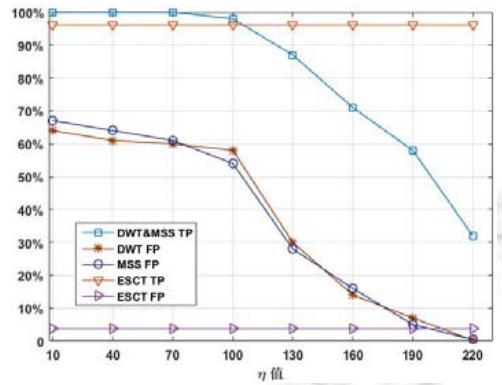


Fig.12 Results of the three detection methods

图 12 3 种检测方法检测结果对比

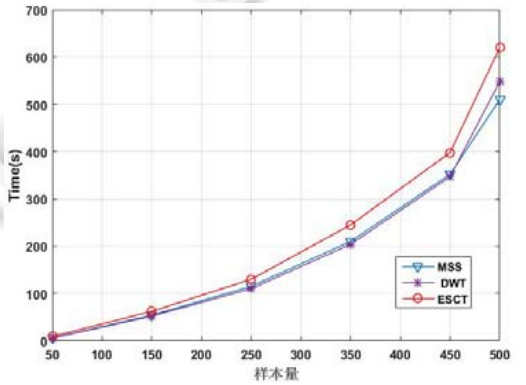


Fig.13 Comparison of execution time between the three detection methods with different number of samples

图 13 不同数量待测样本下三种检测方法时运行时间对比

从图 13 可以看出:ESCT 检测时运算时间优于 MSS 方法,与 DWT 方法处理时间接近.3 种方法运行时间均随待测样本中流量数量的增加而增长.ESCT 检测时运算时间与 DWT 方法接近的主要原因是,ESCT 方法在分析样本流量周期性特征时采用了与 DWT 方法相似的特征提取方法.但与 MSS 方法和 DWT 方法需对全系统链路流量分析处理不同,在实际检测部署中,ESCT 方法仅需处理和分析系统少量关键节点和链路的信息时便可获得较高的检测准确率,因此实际应用过程中,ESCT 方法可有效减少检测时间.但图 12 也表明,ESCT 方法仍存在计算开销较大的问题,下一步对计算开销进行深入的优化.

4 结 论

随着互联网及信息安全技术的不断发展,域间路由系统面临日益严峻的安全威胁,尤其是近年出现的 BGP-LDoS 攻击,其技术的复杂度和可能造成的危害都要远大于传统网络攻击.已有的域间路由系统安全技术主要是为了应对针对系统控制平面的安全威胁,难以有效检测针对系统数据平面的 BGP-LDoS 攻击.为此,本文在分析 BGP-LDoS 攻击过程的基础上,利用 BGP-LDoS 攻击造成的域间路由系统的突变,提出一种基于突变平衡态的 BGP-LDoS 攻击检测方法 ESCT.分析 BGP-LDoS 攻击的具体步骤和每步时系统状态变化,选取具有强表征性的流量统计特征、路由状态特征和系统报文转发量作为控制和状态变量,运用突变理论中的尖点突变模型建立域间路由系统正常和失效状态下的平衡曲面.通过监控系统状态,计算系统所处平衡曲面位置,判断系统状态是否发生突变,检测系统中存在的 BGP-LDoS 攻击.实验证明:仅利用系统少量关键的 AS 节点和链路数据信息进行参数训练和攻击检测,ESCT 方法便能达到 95%的正确率和低于 2.5%的误报率.说明在实际系统中部署 ESCT 检测方法时,其监控、计算开销可以控制在合理范围之内.同时,与已有的 LDoS 攻击检测方法对比,ESCT 方法表现出较高的准确性和较低的误报率.由于真实互联网域间路由系统中关键节点和链路所占比例较小,因此 ECST 方法可以在互联网域间路由系统中进行实际部署.但该方法还存在计算开销过大及如何进行节点、链路信息收集等问题,下一步将继续对 ESCT 方法进行优化,降低计算复杂性,提高检测的实时性.

References:

[1] Siddiqui MS, Montero D, Serral-Gracià R, *et al*. A survey on the recent efforts of the Internet standardization body for securing inter- domain routing. Computer Networks, 2015,80:1−26.

[2] Hollick M, Nita-Rotaru C, Papadimitratos P, *et al*. Toward a taxonomy and attacker model for secure routing protocols. ACM SIGCOMM Computer Communication Review, 2017,47(1):43−48.

[3] Li S, Zhuge JW, Li X. Study on BGP security. Ruan Jian Xue Bao/Journal of Software, 2013,24(1):121−138 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[4] Zhang Y, Mao ZM, Wang J. Low-Rate TCP-targeted DoS attack disrupts Internet routing. In: Proc. of the Network and Distributed System Security Symp. 2007.

[5] Schuchard M, Mohaisen A, Kune DF, *et al*. Losing control of the Internet: Using the data plane to attack the control plane. In: Proc. of the 17th ACM Conf. on Computer and Communication Security. Chicago, 2010. 726−740.

[6] Kang MS, Lee SB, Gligor VD. The crossfire attack. In: Proc. of the 2013 IEEE Symp. on Security and Privacy. 2013. 127−141.

[7] Li HS, Zhu JH, Qiu H, *et al*. The new threat to Internet: DNP attack with the attacking flows strategizing technology. Int'l Journal of Communication Systems, 2015,28:1126−1139.

[8] Li HS, Zhu JH, Wang QX, *et al*. LAAEM: A method to enhance LDoSattack. IEEE Communications Letters, 2016,20(4):708−711.

[9] Bertino E, Islam N. Botnets and Internet of things security. Computer, 2017,50(2):76−79.

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

[11] Seo K, Lynn C, Kent S. Public-Key infrastructure for the secure border gateway protocol (S-BGP). In: Proc. of the DARPA Information Survivability Conf. & Exposition II. California, 2001. 239−253.

[12] White R. Securing BGP through secure origin BGP. Internet Protocol Journal, 2003,6(3):15−22.

[13] Oorschot PC, Wan T, Kranakis E. On interdomain routing security and pretty secure BGP (ps BGP). ACM Trans. on Information and System Security, 2007,10(3):11−25.

[14] Subramanian L, Roth V, Stoica I, *et al*. Listen and whisper: Security mechanisms for BGP. In: Proc. of the 1st Symp. on Networked Systems Design and Implementation. San Francisco, 2004. 127−140.

[15] Khare V, Ju Q, Zhang B. Concurrent prefix hijacks: Occurrence and impacts. In: Proc. of the 2012 ACM Conf. on Internet Measurement Conf. ACM Press, 2012. 29−36.

[16] Lad M, Massey D, Pei D, *et al*. PHAS: A prefix hijack alert system. In: Proc. of the 15th USENIX Security Symp. Vancouver, 2006. 108−119.

[17] Goodell G, Aiello W, Griffin T, *et al*. Working around BGP: An incremental approach to improving security and accuracy of inter-domain routing. In: Proc. of the ISOC NDSS. San Diego, 2003. 75−85.

[18] Wen K, Yang JH, Zhang B. Survey on research and progress of low-rate denial of service attacks. Ruan Jian Xue Bao/Journal of Software, 2014,25(3):591−605 (in Chinesewith English abstract). http://www.jos.org.cn/1000-9825/4520.htm [doi: 10.13328/j.cnki.jos.004520]

[19] Chen H, Chen Y. A novel embedded accelerator for online detection of shrew DDoS attacks. In: Proc. of the Int'l Conf. on Networking, Architecture and Storage. Chongqing, 2008. 365−372.

[20] Kwok YK, Tripathi R, Chen Y, *et al*. HAWK: Halting anomalies with weighted choking to rescue well-behaved TCP sessions from shrew DDoS attacks. In: Proc. of the Networking and Mobile Computing. Berlin, Heidelberg: Springer-Verlag, 2005. 423−432.

[21] Luo XP, Chang RKC. On a new class of pulsing denial-of-service attacks and the defense. In: Proc. of the Network and Distributed System Security Symp. San Diego, 2005.

[22] Wu ZJ, Zeng HL, Yue M. Approach of detecting LDoS attack based on time window statistic. Journal of China Institute of Communications, 2010,31(12):55−62 (in Chinese with English abstract).

[23] Wu ZJ, Hu R, Yue M. Flow oriented detection of low rate denial of service attacks. Int'l Journal of Communication Systems, 2016, 29(1):130−141.

[24] Xiang Y, Li K, Zhou W. Low-Rate DDoS attacks detection and traceback by using new information metrics. IEEE Trans. on Information Forensics and Security, 2011,6(2):426−437.

[25] Wu ZJ, Li G, Yue M. Detecting low-rate DoS attacks based on signal cross-correlation. Acta Electronica Sinica, 2014,42(9): 1760−1766 (in Chinese with English abstract).

[26] Thom R. Structure stability, catastrophe theory, and applied mathematics. SIAM Review, 1977,19(2):189−201.

[27] Stamovlasis D. Catastrophe theory: Methodology, epistemology, and applications in learning science. In: Proc. of the Complex Dynamical Systems in Education. Springer Int'l Publishing, 2016. 141−175.

[28] Deng WP, Karliopoulos M, Muhlbauer W, *et al*. *k*-Fault tolerance of the Internet AS graph. Computer Networks, 2011,55(10): 2492−2503.

[29] Liu Y, Peng W, Su J, *et al*. Assessing the impact of cascading failures on the interdomain routing system of the Internet. New Generation Computing, 2014,32(3-4):237−255.

[30] Wang Y, Wang ZX, Zhang LC. An epidemic-dynamics-based model for CXPST spreading in inter-domain routing system. In: Proc. of the 8th Int'l Conf. on Bio-Inspired Computing: Theories and Applications (BIC-TA). Springer, 2013. 485−493.

[31] Orsini C, King A, Giordano D, *et al*. BGPStream: A software framework for live and historical BGP data analysis. In: Proc. of the 2016 ACM on Internet Measurement Conf. ACM Press, 2016. 429−444.

[32] Agarwal S, Chuah CN, Bhattacharyya S, *et al*. Impact of BGP dynamics on router CPU utilization. In: Proc. of the Int'l Workshop on Passive and Active Network Measurement. Berlin, Heidelberg: Springer-Verlag, 2004. 278−288.

[33] Faggiani A, Gregori E, Improta A, *et al*. A study on traceroute potentiality in revealing the Internet as-level topology. In: Proc. of the 2014 IFIP Networking Conf. IEEE, 2014. 1−9.

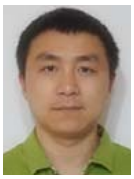
附中文参考文献:

[3] 黎松,诸葛建伟,李星.BGP 安全研究.软件学报,2013,24(1):121−138. http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[18] 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(3):591−605. http://www.jos.org.cn/1000-9825/4520.htm [doi: 10.13328/j.cnki.jos.004520]

[22] 吴志军,曾化龙,岳猛.基于时间窗统计的 LDoS 攻击检测方法的研究.通信学报,2010,31(12):55−62.

[25] 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(9):1760−1766.



苗甫(1981－),男,湖北襄阳人,硕士,主要研究领域为网络安全.

张连成(1982－),男,博士,讲师,CCF 专业会员,主要研究领域为软件定义网络安全,软件定义安全,流量追踪.

郭毅(1984－),男,博士,讲师,主要研究领域为路由协议安全.

王禹(1984－),男,博士,讲师,CCF 专业会员,主要研究领域为网络安全.

王振兴(1959－),男,博士,教授,博士生导师,主要研究领域为网络安全.