软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(12):3853−3867 [doi: 10.13328/j.cnki.jos.005310]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于突变平衡态理论的 BGP-LDoS 攻击检测方法*

苗 甫[1], 张连成[1], 郭 毅[1,2], 王 禹[3], 王振兴[1]

[1](解放军信息工程大学,河南 郑州 450001)

[2](清华大学 网络科学与网络空间研究院,北京 100084)

[3](河南工程学院,河南 郑州 450007)

通讯作者: 苗甫, E-mail: ufoaim@qq.com

摘 要: 域间路由系统是互联网的关键基础设施.针对域间路由系统的低速率拒绝服务攻击(low-rate DoS against BGP sessions,简称 BGP-LDoS)能够引起大范围级联失效,造成域间路由系统全局瘫痪.已有的防护机制和检测方法难以有效应对这种源自数据平面的大规模低速率流量拥塞攻击.分析域间路由系统在 BGP-LDoS 攻击威胁下的状态突变过程,提出一种基于突变平衡态理论(the equilibrium state of the catastrophe theory,简称 ESCT)的 BGP-LDoS 攻击检测方法.以流量周期性特征、路由会话特征和报文转发量为检测特征进行突变模型的选择,并确定相应的状态变量和控制变量,进一步利用采集的历史数据为训练样本,对突变函数进行训练,以定义系统正常和失效状态时的平衡曲面.利用训练后的尖点突变模型对系统运行状态进行监控,根据分歧集函数判断系统是否出现由正常向失效的跳变,从而实现对攻击的检测.实验结果表明:ESCT 方法仅需要监控系统中少量的关键链路和节点就能够具备较强的 BGP-LDoS 检测能力,为及时发现和提早应对攻击提供可靠参考.

关键词: 突变理论;域间路由;低速率拒绝服务;攻击检测;网络安全

中图法分类号: TP393

中文引用格式: 苗甫,张连成,郭毅,王禹,王振兴.基于突变平衡态理论的 BGP-LDoS 攻击检测方法.软件学报,2018,29(12):3853−3867. http://www.jos.org.cn/1000-9825/5310.htm

英文引用格式: Miao F, Zhang LC, Guo Y, Wang Y, Wang ZX. Method for BGP-LDoS attack detection of inter domain routing system based on the theory of catastrophe equilibrium state. Ruan Jian Xue Bao/Journal of Software, 2018,29(12):3853−3867 (in Chinese). http://www.jos.org.cn/1000-9825/5310.htm

Method for BGP-LDoS Attack Detection of Inter Domain Routing System Based on the Theory of Catastrophe Equilibrium State

MIAO Fu[1], ZHANG Lian-Cheng[1], GUO Yi[1,2], WANG Yu[3], WANG Zhen-Xing[1]

[1](The PLA Information Engineering University, Zhengzhou 450001, China)

[2](Institute of Cyberspace and Network Science, Tsinghua University, Beijing 100084, China)

[3](Henan University of Engineering, Zhengzhou 450007, China)

Abstract: Inter domain routing system is a key infrastructure for the Internet. A large-scale low rate denial of service attack against BGP sessions (BGP-LDoS) can trigger a wild range of cascading failure and cause the overall paralysis of inter domain routing system. Unfortunately, the existing protection mechanisms and detection methods are not effective in detecting this type of threat originated from the system's data plane. To tackle the issue, this paper analyzes the inter domain state catastrophe process under BGP-LDoS attack, and then proposes a BGP-LDoS attack detection method based on the equilibrium state of the catastrophe theory (ESCT). Flow periodic characteristics, routing session characteristics and system forwarding packets are chosen as the detection characteristics. Based on the

* 基金项目: 国家自然科学基金(61402525, 61402526); 国家高技术研究发展计划(863)(2012AA012902)

Foundation item: National Natural Science Foundation of China (61402525, 61402526); National High Technology Research and Development Program of China (863) (2012AA012902)

收稿时间: 2017-01-17; 修改时间: 2017-03-10; 采用时间: 2017-04-25

detection characteristics, the catastrophe model is selected and the state variables and control variables are determined. Using the collected historical data as training samples, the catastrophe function is trained in order to establish the normal and abnormal state of the equilibrium surface. Using the trained cusp catastrophe model to monitor the running state of the system, the detection of the attack is realized by utilizing the bifurcation set function to judge whether the system will jump from normal to failure. The experimental results show that this method can achieve good detection capability while only monitoring a few links and nodes. It can also provide a reliable reference for the network administrator to detect and respond to attacks in advance.

Key words: catastrophe theory; inter domain routing; lowrate denial of service; attack detection; network security

域间路由系统作为互联网的关键基础设施,其安全性对互联网健康稳定运行具有重要意义.然而,域间路由系统主要采用的 BGP(border gateway protocol)协议在设计之初就存在严重的安全隐患,导致域间路由系统面临严峻安全威胁[1−3].近年来,针对域间路由系统的攻击手段不断更新,其造成的危害也愈加严重.Zhang 等人[4]在低速率拒绝服务攻击(low-rate denial of service,简称 LDoS)的基础上提出了针对 BGP 会话的 ZMW 攻击方式.该攻击通过不断阻塞路由器之间 KeepAlive 报文的传递,重置路由器之间的正常会话,影响路由节点功能.以 ZMW 攻击为基础,Schuhard 等人[5]进一步提出了基于 BGP 数据平面的跨平面攻击方式 CXPST(coordinated cross plane session termination).CXPST 利用大规模僵尸节点,在系统多条关键路径上同时发起 ZMW 攻击,通过反复中断路由会话诱发大量路由更新,耗尽系统关键路由节点的存储和计算资源,导致整个系统陷入瘫痪.与 CXPST 类似的攻击还有 Crossfire[6],DNP[7],LAAEM[8]等,由于这些攻击均是针对 BGP 的 LDoS 攻击,能够导致域间路由系统局部或整体失效,下文统称此类攻击为 BGP-LDoS 攻击.文献[5]通过实验仿真表明:利用 250 000 个僵尸节点,BGP-LDoS 可以瘫痪整个互联网域间路由系统达数个小时,且尚无有效的解决方法.文献[6]在实际网络环境中对美国的部分大学、州及东西部海岸地区的网络进行了实际攻击,结果表明,攻击能够有效阻断这些地区的正常网络通信.随着物联网的不断发展,攻击者可利用僵尸网络规模也将越来越大,波及的地区和范围也越来越广[9],以大规模僵尸网络为基础攻击条件的 BGP-LDoS 将给互联网的安全稳定运行带来严重威胁.

为应对域间路由系统面临的安全威胁,现有的安全增强机制主要有协议扩展和安全监测两类.

- 协议扩展是对现有的 BGP 协议进行修改,主要采用认证技术解决 BGP 协议安全性不足的问题,典型的有 S-BGP(secure BGP)[10,11],soBGP(secure origin BGP)[12],psBGP(pretty security BGP)[13]和 Listen & Whisper[14]等.由于需要修改现有的 BGP 协议,协议扩展部署成本较高,且主要防范前缀劫持、路径伪造等针对域间路由系统控制层面的攻击,难以有效防范针对数据平面的 BGP-LDoS 攻击;
- 安全监测技术不改变现有 BGP 协议,而是通过检查、识别域间路由系统各自治域(autonomous system,简称 AS)间交换的路由信息,发现异常路由.典型的有 MyASN 服务[15]、PHAS[16]、IRV[17]等.现有的安全监测技术能够确保路由信息传播过程中真实性和完整性,防范前缀劫持、路由泄漏以及路径伪造等安全问题的发生,但其监测重点仍在系统的控制平面,难以有效应对 BGP-LDoS 攻击.

现有的 LDoS 攻击的检测方法主要有两类[18].一类是特征检测.由于 LDoS 攻击流量具备周期性和短时高脉冲的特点,特征检测技术通过分析 LDoS 攻击周期、脉冲强度和持续时间等特征,能够有效检测出 LDoS 攻击的存在,典型的有动态时间封装方法(dynamic time wraping,简称 DTW)[19]、HAWK 方法[20]等;另一类是异常检测.通过分析当前网络中流量偏离正常状态的时间变化序列信息,检测出攻击的存在.典型的有小波变换分析[21]、频谱分析[22]、统计分析[23]、信息度量分析[24]、小信号检测分析[25]等技术.

与传统的 LDoS 攻击相比,BGP-LDoS 攻击有 3 个方面明显不同.

- 首先,攻击目标不同:LDoS 主要针对单个节点或链路,在攻击过程中,攻击目标是明确和固定的;而 BGP-LDoS 是针对系统多条关键路径的攻击,选择攻击目标时,由于资源和流量限制,为保证攻击路径互不干扰,BGP-LDoS 攻击目标是非固定的,根据攻击资源、流量和路径的变化而不断调整;
- 其次,破坏机制不同:LDoS 主要针对 TCP 协议的拥塞控制机制进行攻击;而 BGP-LDoS 虽然利用了 TCP 协议拥塞控制机制的不足,但更主要的是利用 BGP 路由更新机制存在的缺陷放大攻击效果;
- 另外,攻击后果不同:LDoS 攻击后会导致以 TCP 作为传输层协议的有效通信流量明显下降;而 BGP-

LDoS 攻击效果主要表现是链路两端的路由器处于反复通断的震荡状态,整个域间路由系统的路由节点因计算、存储资源耗尽而瘫痪.

由于上述区别的存在,使得现有 LDoS 攻击检测技术在应对 BGP-LDoS 时的准确性和时效性会有较大幅度的降低,从而出现大量的误判和漏判.

针对当前缺乏有效的 BGP-LDoS 攻击检测方法,本文在分析 BGP-LDoS 攻击流程及影响的基础上,利用突变理论在描述系统质变上的优异性,提出一种基于突变平衡态理论(the equilibrium state of the catastrophe theory,简称 ESCT)的 BGP-LDoS 攻击检测方法.通过分析 BGP-LDoS 攻击前后域间路由系统突变特性,以 3 类强表征性的流量统计特征、路由会话特征、系统报文转发量为状态和控制变量,选取尖点突变模型建立起系统正常状态和异常状态的平衡曲面.对系统状态进行监控,根据分歧集函数判断系统状态是否由正常向失效跳变,实现对 BGP-LDoS 攻击的检测,为及时发现和提早应对攻击提供可靠参考.

1 突变理论与失效路由系统的突变特性

突变是指系统状态随控制变量变化而发生突然和不连续的质变.域间路由系统是一个开放的复杂巨系统,其运行状态受到拓扑结构、网络故障、病毒攻击等诸多因素影响,呈现出非线性、非平稳性等复杂非线性动力学特征.虽然域间路由系统具有一定的鲁棒性,当遭遇部分偶发故障或小规模攻击时系统仍能保持正常运行状态,然而当失效的链路或节点属于系统关键节点或链路,或失效节点链路数量超过一定阈值时,系统中将会出现级联失效,导致整个系统迅速陷入瘫痪状态.由于系统的级联失效过程是一个非平稳、非连续过程,可将其视为一个突然质变过程,利用突变理论进行描述和分析.

1.1 突变理论

突变理论[26,27]是非线性科学中的重要理论之一,不仅能够直接处理不连续问题,还适合于内部作用机理未知的系统.突变理论主要通过精确的数学公式和形象的数学模型来描述和预测系统连续性被中断而产生的质变,具体来说,涉及到以下几个数学概念.

- 势函数:用于描述系统行为,通常表示为 $F(X,B)$.$F(X,B)$包含两类参数,$X=(X_1,X_2,\ldots,X_n)$是系统的 n 维状态变量,表示系统的行为状态,$X\in R^n$,R^n为系统状态空间;$B=(B_1,B_2,\ldots,B_m)$是系统的控制变量,表示影响系统行为状态的控制因素,$B\in R^m$,R^m为系统控制空间;
- 临界点 u:若$\exists u\in R^n$使得 $\left.\frac{DF(x,b)}{\partial x}\right|_u=0$,即 $\left.\frac{\partial F(x,b)}{\partial x_1}\right|_u=\left.\frac{\partial F(x,b)}{\partial x_2}\right|_u=\ldots=\left.\frac{\partial F(x,b)}{\partial x_n}\right|_u=0$,则称 u 为 $F(X,B)$的临界点;
- 平衡曲面(equilibrium surface)M:对于任意 m,若 m 满足 $\left.\frac{DF(x,b)}{\partial x}\right|_m=0(m\in R^n)$,则 $m\in M$,也就是说 M 是由全部临界点 u 构成的,突变理论中,对于系统状态突变的解释需要利用平衡曲面进行解释;
- 奇点集 S:当势函数中的自变量发生连续变化时,如果在定态点附近状态函数的状态变量出现不连续、跳跃等现象,这些定态点就是奇点.对于任意点 s,若 s 满足$\Delta H(F)=\det H(F)=0$(其中,det 表示行列式,$\{H(F)\}$是 F 的 *Hessen* 矩阵),则 $s\in S$,即所有奇点构成奇点集;
- 分歧集(bifurcation set)Bs:联立方程 $\begin{cases}DF(x,b)=0\\ \det H(F(x,b))=0\end{cases}$求解,消去所有状态变量 x,仅利用控制变量 c 所建立的方程.分歧集是奇点集在特定控制空间的投影,用于对突变现象进行判定.

突变理论的突变模型具有多态性、不可达性、突变性、发散性和滞后性等多个特性.根据状态变量和控制变量个数的不同,有 7 种初等突变模型,见表 1.

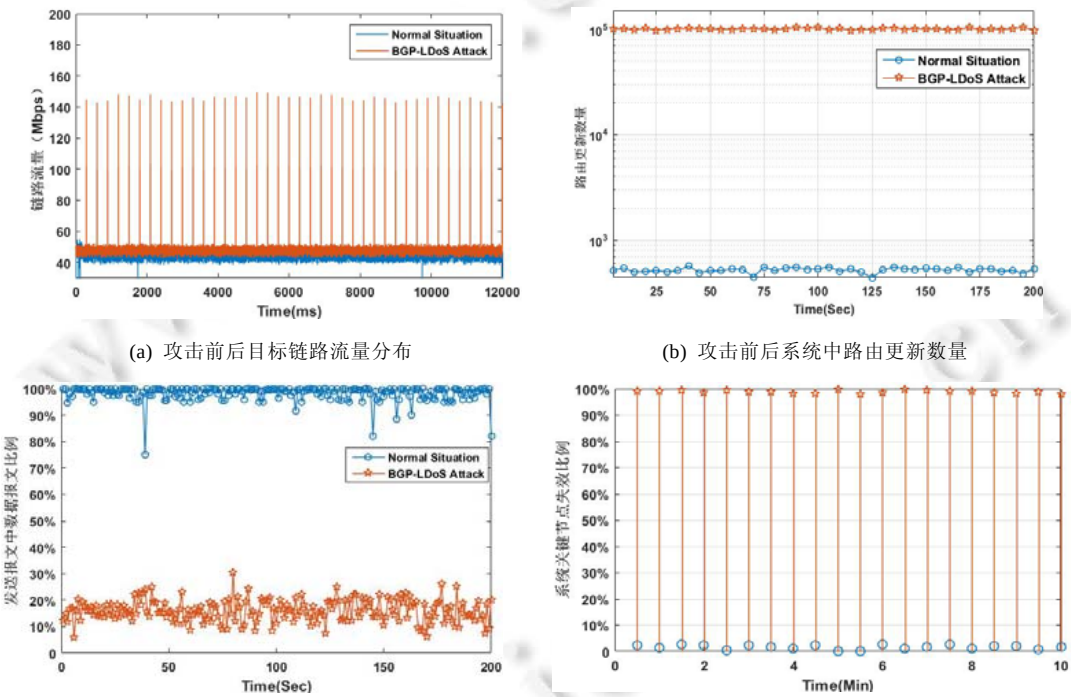
Table 1 Seven kinds of elementary catastrophe model

表 1 7 种初等突变模型

突变模型名称	状态变量个数	控制变量个数
折迭突变	1	1
尖点突变	1	2
燕尾突变	1	3
蝴蝶突变	1	4
椭圆脐点	2	3
双曲脐点	2	3
抛物脐点	2	4

1.2 失效域间路由系统的突变特性

在正常运行与遭遇 BGP-LDoS 攻击失效两种状态下,分析已有研究实验数据[5,6,29,30],系统中核心路由节点路由更新数量、攻击目标链路流量、失效节点比例等变化情况如图 1 所示.



(a) 攻击前后目标链路流量分布

(b) 攻击前后系统中路由更新数量

(c) 攻击前后节点发送报文中数据报文所占比例

(d) 攻击前后系统关键节点失效比例

Fig.1 System's state changes before and after BGP-LDoS attack

图 1 BGP-LDoS 攻击前后系统状态变化

从图 1 可以看出,尽管系统中路由节点的路由更新数量、数据报文转发量、节点之间链路流量等数据呈现出波动性,但在同一种状态下,这些数据的波动均保持在一定范围内,即使遭遇一些随机扰动,扰动对系统的影响也将很快消失[28],可以视为系统一种平衡态.不同状态下,路由更新数量、数据报文转发量、节点之间链路流量存在显著差异,这表明这系统正常和失效状态可视为两种不同平衡态,两种状态之间的变化是一种质变.

域间路由系统是一个复杂开放系统,具有幂律、小世界、异配等结构特性.这种结构特性决定了系统动力学特征是复杂、非线性和非平稳的.由正常向失效状态转变过程中,进一步分析失效关键 AS 节点比例变化,如图 2 所示.从图 2 可以看出:遭遇 BGP-LDoS 攻击后,系统在由正常向失效状态转变过程中,失效节点个数以指数增长到失效后的平衡态.这表明系统从正常到失效的质变过程是一个突发和剧烈的过程.

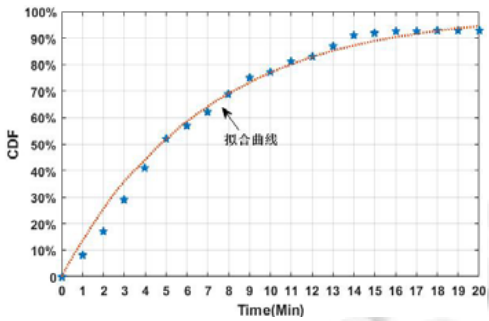


Fig.2 Cumulative distribution of failurekey nodesin the attack

图 2 遭遇攻击时关键节点失效比例随时间变化的累计分布

综合图 1 和图 2,由于域间路由系统的正常和失效状态可视为两种不同的平衡稳定状态,而两种状态的转变过程是非线性和非平稳的质变,与突变理论中的突变过程相似,因此,可以利用突变平衡态理论对 BGP-LDoS 攻击进行检测.

2 BGP-LDoS 攻击检测方法 ESCT

基于域间路由系统的突变特性,以及突变理论在描述复杂系统状态变迁方面的优越性,本文提出一种基于突变平衡态理论的 BGP-LDoS 攻击检测方法 ESCT,其流程如图 3 所示.

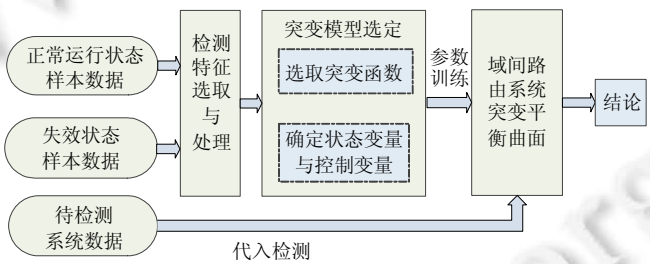


Fig.3 BGP-LDoS attack detection process based on ESCT

图 3 基于 ESCT 的 BGP-LDoS 攻击检测流程

首先,选取能够有效表征 BGP-LDoS 攻击的检测特征;然后,根据检测特征选择相应的突变函数,并确定相应的状态变量和控制变量;之后,利用前期采集的训练样本对突变函数进行参数训练,定义系统正常和失效状态时的平衡曲面;此后,利用平衡曲面对系统运行情况进行监控,检测 BGP-LDoS 攻击的存在.

2.1 检测特征选取及标准化处理

2.1.1 检测特征选取

检测特征的选取直接决定了检测方法的有效性和准确性.在检测特征选取时,本文主要分析 BGP-LDoS 攻击原理及其对系统状态变换的影响,提取其中有效表征系统遭遇 BGP-LDoS 攻击的检测特征.

BGP-LDoS 攻击原理及其对系统状态影响.

I 攻击前的探测.实施 BGP-LDoS 攻击前,攻击者需对系统拓扑进行分析,选择路由系统中关键链路作为目标,分析这些目标链路的带宽、RTT、MinRTO 等参数,根据这些参数对僵尸节点资源进行分配,对攻击流量的路径进行规划.此时,系统状态尚未发生变化;

II 链路 BGP 会话中断.依据探测结果,攻击者选取一定攻击周期和攻击流量强度对目标链路进行 LDoS 攻击,使得所有目标链路处于拥塞状态,中断目标链路上的 BGP 会话.会话被中断的路由节点分别向各

自邻居发送更新报文,导致这些节点重新计算路由表.此时,系统状态最明显的变化就是多条关键链路上出现周期性峰值流量;

III 目标链路 BGP 会话重建.由于目标链路仅被攻击虚拟切断,而非物理链路实际断开,因此当攻击流量引向其他路径后,链路两端节点再次建立 BGP 会话,并再次向各自邻居发送路由更新报文,其他路由节点根据路由更新报文再次重新计算路由表;

IV BGP 会话的反复中断和重建.不断重复第 II 步、第 III 步攻击过程,使得目标链路上 BGP 会话在通断之间反复震荡,此时,系统状态较明显的变化是系统中出现巨量的路由更新报文;

V 级联失效.由于对多个目标链路同时进行攻击,攻击将在系统中引发巨量更新报文,部分路由节点在存储和计算这些更新报文时,因计算和存储资源耗尽进入失效状态.这进一步放大 BGP-LDoS 攻击效果,引发系统级联失效,陷入最终瘫痪状态.此时,系统中较明显的特点是有效报文转发量急剧下降.

通过分析攻击过程及其造成的系统状态变化可以看出:遭遇 BGP-LDoS 攻击后,域间路由系统中链路流量呈现出明显的周期性;路由更新报文数量和路由会话重置次数显著增多;节点有效报文转发量显著降低.这些变化为检测 BGP-LDoS 攻击提供了依据.

将攻击前后系统的这些变化归纳为 3 类检测特征:链路流量周期性特征、路由节点状态特征和数据报文转发特征.3 类特征的具体定义如下.

定义 1(链路流量周期性特征λ). 由于 BGP-LDoS 攻击针对目标链路采用了 LDoS 攻击手段,因此系统目标链路上的流量呈现出明显的周期性.利用λ表示系统链路中存在的周期性脉冲流量特征,$\lambda=\{T,L,R\}$,包含周期性流量的周期 T、脉冲长度 L 以及脉冲强度 R.当链路上不存在周期性流量时,$\lambda=\{0,0,0\}$.

定义 2(路由节点状态特征γ). 由于 BGP-LDoS 攻击造成目标链路频繁通断,路由节点的路由会话也频繁重置,产生大量的路由更新报文.利用γ表示系统路由节点状态,$\gamma=\{U,S\}$,其中,U 表示单位时间 t 内路由节点中排队待处理的路由更新报文数量,S 表示单位时间 t 内路由节点与邻接点的会话重置次数.

定义 3(数据报文转发特征ρ). 由于 BGP-LDoS 攻击引发的级联失效致使系统内部产生大量的控制报文,而正常的数据报文转发功能受到严重削弱.利用ρ表示单位时间 t 内所监测路由节点数据报文转发量,将其作为检测系统是否遭遇 BGP-LDoS 攻击的一项指标.

2.1.2 特征标准化处理

选取特征后,由于不同特征的取值范围和单位量纲不同,影响检测模型检测的准确性,需标准化处理.在标准化处理过程中,依据突变理论中突变级数评价方法:特征隶属度越大越好,也就是在特征标准化过程中,特征值越大,所反映系统遭遇 BGP-LDoS 攻击的威胁度也越高.

对于链路流量周期性特征λ,处理过程如下.

① 单位时间 t 内,链路 i 中检测到的周期性流量的脉冲长度为 L_i,则标准化处理后所得的长度 L_i' 为 $L_i'=L_i/L_{ref}(L_i<L_{ref})$或 $L_i'=1(L_i\geqslant L_{ref})$,其中,$L_{ref}$ 为设定的参考脉冲长度,$L_{ref}=\max(L_i)$;若未检测到周期性流量,则 $L_i=0$.

② 单位时间 t 内,链路 i 中检测到周期性流量的周期为 T_i,标准化后所得的周期 T_i' 为 $T_i'=T_i/T_{ref}(T_i<T_{ref})$ 或 $T_i'=T_{ref}/T_i(T_i'\geqslant T_{ref})$,其中,$T_{ref}$ 为设定的参考脉冲长度,$T_{ref}=\max(T_i)$;若未检测到周期性流量,则 $T_i=0$;

③ 单位时间 t 内,链路 i 中检测到周期性流量的脉冲强度为 R_i,标准化后所得的脉冲强度 R_i' 为 $R_i'=R_i/R_{ref}$ $(R_i<R_{ref})$或 $R_i'=1(R_i\geqslant R_{ref})$,其中,$R_{ref}$ 为设定的参考脉冲强度,$R_{ref}=\max(R_i)$;若未检测到周期性流量,则 $R_i=0$.

为降低计算复杂度,将流量周期性特征 T_i',L_i',R_i' 视为互不相关的 3 个变量,根据突变级数评价法,链路 i 在单位时间 t 内的流量周期性特征为 $\lambda_i=\min(\sqrt{T_i'},\sqrt[3]{L_i'},\sqrt[4]{R_i'})$.系统总体的流量周期性特征为 $\lambda=\sum_{i=1}^{m}\lambda_i$,其中,$m$ 为所监测的链路的个数 $U_j/U_{ref}(U_j<U_{ref})$.

对于路由节点状态特征γ,处理过程如下.

① 单位时间 t 内,节点 j 中收到的 U_j 个其他节点路由更新报文,则标准化后所得的 U_j' 为 $U_j'=U_j/U_{ref}(U_j<U_{ref})$ 或 $U_j'=1(U_j\geqslant U_{ref})$,其中,$U_{ref}$ 为设定的参考路由报文更新数量,$U_{ref}=\max(U_j)$.

② 单位时间 t 内,节点 j 中路由重置的次数为 S_j,则标准化后所得的 S'_j 为 $S'_j = S_j / S_{ref}$ ($S_j < S_{ref}$) 或 S'_j =1 ($S_j \geqslant S_{ref}$),其中,S_{ref} 为设定的参考路由器重置次数,S_{ref}=max(S_j).

由于大量节点重置和路由更新均是 BGP-LDoS 攻击存在的显著标志,将节点重置和路由更新视为互不相关变量,根据突变级数评价法,节点 j 中路由状态特征为 $\gamma_j = \min(\sqrt{S'_j}, \sqrt[3]{U'_j})$.单位时间 t 内,系统总体的路由特征为 $\gamma = \sum_{j=1}^{n} \gamma_j$,其中,$n$ 为所监测节点的个数.

对于路由报文转发特征ρ的处理过程如下:设单位时间 t 内,节点 j 中的报文转发量为ρ_j,标准化后所得 ρ'_j 为 $\rho'_j = 1 - \rho_j / \rho_{ref}$ ($\rho_j < \rho_{ref}$) 或 $\rho'_j = 0$ ($\rho_j \geqslant \rho_{ref}$),其中,$\rho_{ref}$ 为设定的参考报文转发量,ρ_{ref}=max(ρ_j).单位时间 t 内,系统总体报文转发量为 $\rho = \sum_{j=1}^{n} \rho'_j$,其中,$n$ 为所监测节点的个数.

2.2 突变模型的选取与参数估计

2.2.1 突变模型的选取

在 BGP-LDoS 攻击下,域间路由系统状态有正常、失效两种平衡状态,且第 2.1 节所选的检测特征总数为 3 个,这表示突变模型中变量总数为 3.在突变理论模型中,尖点突变模型具有双模态[27],能够描述系统在两个稳定状态之间的突变,且根据表 1,尖点模型状态和控制变量总和也为 3,因此选取尖点突变模型对 BGP-LDoS 攻击进行检测.

尖点突变的几何结构如图 4 所示,图中上部分是尖点突变模型的平衡曲面,由上中下三叶 A,B,C 组成,叶 A 表示正常稳定状态,叶 C 表示失效平衡态,叶 B 为不稳定的平衡位置,也为系统的不可达区域.当系统从 A 页面上 p 点转变到 C 页面 q 点时,p-q 之间有一个突然的跳变(sudden jump),即为突变.图中下半部分是尖点突变模型的几何形状,它是由 u,v 两个控制变量支配的分歧集,p-q 的轨迹经过分歧集曲线.

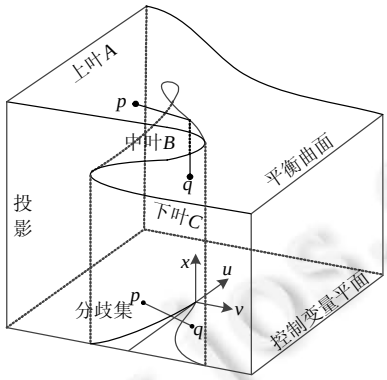


Fig.4 Geometry of cusp catastrophe

图 4 尖点突变的几何结构

尖点突变模型的势函数 $F(x)=x^4+aux^2+bvx$,其中,x 表示状态变量,u,v 分别表示控制变量,a,b 是系数.根据第 1.1 节对突变理论的介绍,尖点突变模型的平衡曲面 M 为

$$M{:}F'(x)=4x^3+2aux+bv=0 \tag{1}$$

奇点集 S 的曲面方程为

$$S{:}F''(x)=6x^2+au=0 \tag{2}$$

联立公式(1)、公式(2)消去 x,得到分歧集 Bs 的表达式:

$$Bs{:}8a^3u^3+27b^2v^2=0 \tag{3}$$

它由平衡曲面临界点组成并且属于系统的控制空间,系统的突然跳变都是发生在这个空间中.从图 5 可以看出,分歧集实质也是尖点突变流形在 u–v 平面投影.

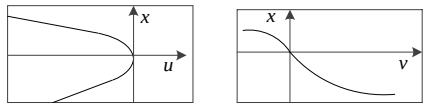


Fig.5 Projection of a cusp catastrophe manifold on plane $u–x$, $v–x$

图 5 尖点突变流形在平面 $u–x$,$v–x$ 上的投影

对于一种稳定的平衡态,其临界点位于突变模型平衡曲面的边界点上,控制变量的波动也位于该集合中.当部分因素受到外力发生改变时,稳定的平衡态会被破坏,当偏离到达一定的阈值时,系统将变得非常不稳定,脱离平衡态的控制,这样就产生了跳变,系统从一个旧的平衡态进入一个新的平衡态.

为确定λ,γ,ρ和 x,u,v 之间对应关系,采用数据拟合方式进行分析.在尖点突变模型中,尖点突变流形在平面 $u–x$,$v–x$ 上的投影如图 5 所示.

在实际的 BGP-LDoS 攻击数据中,λ,γ,ρ的相互关系如图 6 所示.

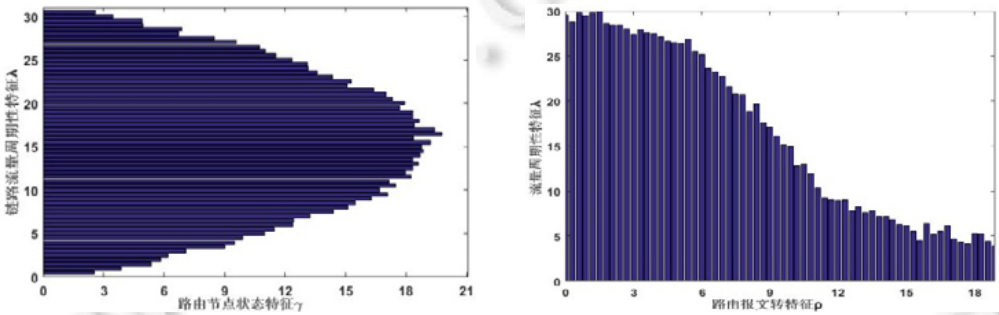


Fig.6 Relationship among λ,γ,ρ in actual data set

图 6 实际数据中λ,γ,ρ之间的关系

对比图 5 和图 6,实际数据中,$\gamma–\lambda$的关系图形与尖点突变流形在 $u–x$ 平面上投影相似,而$\rho–\lambda$的关系图形与尖点突变流形在 $v–x$ 上的投影相似,因此选取λ作为状态变量 x,γ作为控制变量 u,ρ作为控制变量 v.

2.2.2 尖点突变模型的参数估计

在选定尖点突变模型以及状态变量和控制变量后,需要通过训练样本得到公式(1)中参数 a,b 的值.

定义 4(状态变量和控制变量序列). 已知样本中,按照时间段 t 的顺序,标准化后得到的样本状态变量序列和控制变量序列分别为 $\tilde{X}=\{\lambda^k\},\tilde{U}=\{\gamma^k\},\tilde{V}=\{\rho^k\},k=1,2,...,N$.这里,N 表示系统样本数据的长度.

由于对样本的状态变量、控制变量进行标准化处理之后全部为正,对比图 5 和图 6,为更好地区分系统正常状态和受攻击后的失效状态,对样本坐标进行平移变换处理.状态和控制变量序列坐标平移平移处理过程如下.

① 在样本中,状态变量序列 $\tilde{X}$ 的均值为 $x_{avg}=\frac{1}{N}\sum_{i=1}^{N}\lambda^i$,$\tilde{X}$ 坐标平移后,状态变量序列为

$$X=\{(\lambda^k–x_{avg})|k=1,2,\ldots,N\};$$

② 控制变量 $\tilde{U}$ 中最大值为 $u_{\max}=\max(\gamma^1,\gamma^2,\ldots,\gamma^N)$,$\tilde{V}$ 中平均值为 $v_{avg}=\frac{1}{N}\sum_{i=1}^{N}\rho^i$,平移后控制变量序列分别为 $U=\{(\gamma^k–u_{\max})|k=1,2,\ldots,N\}$和 $V=\{(\rho^k–v_{avg})|k=1,2,\ldots,N\}$.

定义 5(样本集 Q). 将坐标平移后的状态变量和控制变量序列集合作为模型训练或检测的样本集:

$$Q=\{(X_1^i,U_1^i,V_1^i)\,|\,i=1,2,...,N\}.$$

系统处于稳定状态时,系统的势能最小.尖点突变模型中,突变平衡曲面 M 是势函数 $F(x)$极值点的集合,系统变化状态位于平衡曲面临界点组成的分歧集 Bs 中.理想状态下,可以用系统方程形式表示系统稳定的状态.但实际中,这种理想状态很难满足,因此采用最小化平衡曲面和分歧集方程(3)的函数 $J(a,b)$,使得系统处于最稳定

的状态.对于样本集 Q,参数 a,b 能满足系统稳定性需求时,需要使得 $J(a,b)$的值最小:

$$J(a,b)=\sum_{i=1}^{N}\{[(X_1^i)^3+aU_1^iX_1^i+bV_1^i]^2+[4a^3(U_1^i)^3+27b^2(V_1^i)^2]^2\} \tag{4}$$

根据最小平方拟和,有:

$$\begin{cases}\partial J(a,b)/\partial a=0\\ \partial J(a,b)/\partial b=0\end{cases} \tag{5}$$

$$\begin{cases}\sum_{i=1}^{N}\{U_1^iX_1^i[(X_1^i)^3+aU_1^iX_1^i+bV_1^i]+12a^2(U_1^i)^3[4a^3(U_1^i)^3+27b^2(V_1^i)^2]\}=0\\ \sum_{i=1}^{N}\{(X_1^i)^3+aU_1^iX_1^i+bV_1^i)V_1^i+54b(V_1^i)^2[4a^3(U_1^i)^3+27b^2(V_1^i)^2]\}=0\end{cases} \tag{6}$$

公式(6)为二元非线性方程组,将训练样本 Q 中的数据 (X_1^i,U_1^i,V_1^i) 代入公式(6),求得尖点突变模型参数 a,b 的值有 9 组,其中 6 组解为复数解.根据公式(2), X_1^i,U_1^i 均为实数,因此,a,b 均不为复数,排除 6 个复数解.将剩余 3 个解代入 $J(a,b)$,使 $J(a,b)$值最小的即为最优解.

2.3 BGP-LDoS攻击判定流程

ESCT 检测方法在建立系统正常状态和失效状态的平衡曲面后,判定系统是否遭遇 BGP-LDoS 攻击的具体流程如图 7 所示.

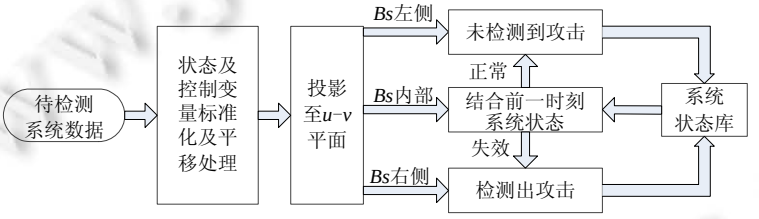


Fig.7 Decision process of whether the system suffered BGP-LDoS attacks

图 7 系统是否遭遇 BGP-LDoS 攻击的判定流程

其中的关键步骤有 4 步.

I 按照时间顺序对待测数据进行标准化和平移处理,处理后所得数据集为 $\{(x_{test}^i,u_{test}^i,v_{test}^i)\,|\,i=1,2,...,m\}$;

II 根据训练所得的参数 a,b,计算 $u_{test}^i>-\sqrt[3]{27a^2(v_{test}^i)^2/8b^3}$ & $v_{test}^i<0$ 是否成立,也就是判断该待测数据在 u–v 平面的投影是否落在 Bs 曲线的左侧:若成立,则说明当前系统处于正常状态,不存在 BGP-LdoS 攻击;若 $u_{test}^i>-\sqrt[3]{27a^2(v_{test}^i)^2/8b^3}$ & $v_{test}^i>0$,说明待测数据在 u–v 平面的投影落在 Bs 曲线的右侧,判断系统遭遇 BGP-LDoS 攻击,处于失效状态;

III 若步骤 II 中的条件均不满足,说明待测数据在 u–v 平面的投影落在 Bs 曲线上或者在曲线内部,这时需要结合系统前一单位时间内的数据 $(x_{test}^{i-1},u_{test}^{i-1},v_{test}^{i-1})$ 进行判断:若 $u_{test}^{i-1}>-\sqrt[3]{27a^2(v_{test}^{i-1})^2/8b^3}$ & $v_{test}^{i-1}<0$,则该时刻系统状态正常;否则,判断判断系统遭遇 BGP-LDoS 攻击;

IV 将系统的状态按照时间序列存入系统状态库,便于后续检测判断.

以图 4 为例,域间路由系统状态正常时,系统(X,U,V)的值位于突变流形的上叶平衡曲面.该(X,U,V)投影到 u–v 平面时,位于尖点突变模型分歧集 Bs 的左侧;当系统遭遇 BGP-LDoS 攻击失效时,此时系统(X,U,V)位于突变流形的下叶平衡曲面,该(X,U,V)投影到 u–v 平面时,位于分歧集 Bs 的右侧.对系统连续两个时刻的状态进行考察,即可实现 BGP-LDoS 攻击的检测.

以图 8 为例对 ESCT 方法检测判定标准进行说明.图 8 中,从 $c\to m$ 表示系统的 10 个样本点在 u–v 平面上的投影,其中,$c\to d,e\to f,h\to i,j\to k,l\to m$ 分别表示系统连续两个单位时间内的样本点.$l\to m$ 轨迹不经过分歧集 Bs

曲线,且在曲线左侧,表明这两个样本点的系统状态均为正常状态.$c\rightarrow d$ 的轨迹经过 *Bs* 曲线,这表明系统由正常状态向失效状态突变,判定系统中存在 BGP-LDoS 攻击.$j\rightarrow k$ 的轨迹位于 *Bs* 曲线右侧,表明系统连续两个时刻一直处于失效状态.$e\rightarrow f,h\rightarrow i$ 的轨迹经过 *Bs* 曲线,且样本点 *f*,*i* 位于 *Bs* 曲线内部,根据图 5 尖点突变流形,需要结合 *i*,*f* 前一时刻 *e*,*h* 进行判断.由于 *h* 处于正常状态,判断 *i* 处于正常状态;*e* 处于失效状态,判断样本点 *f* 处于失效状态.

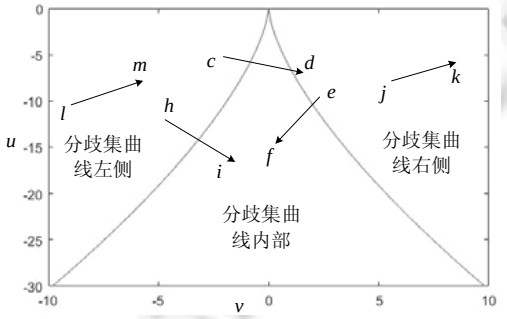


Fig.8 Criteria for judging the existence of attack in ESCT detection

图 8 ESCT 检测过程中攻击存在性判定标准

ESCT 检测方法在参数训练完毕后,检测 BGP-LDoS 攻击的时间复杂度与所监控的节点数量 *N* 和链路数量 *E* 有关,为 $O(E\log(E)+N)$.

3 实验与分析

在验证 ESCT 方法检测 BGP-LDoS 攻击有效性时,考虑到针对域间路由系统的 BGP-LDoS 攻击不适于在现实环境中实施,本文利用网络模拟器搭建实验仿真环境,验证 ESCT 检测能力.

3.1 对BGP-LDoS攻击检测效果分析

实验选取 CAIDA 提供的 2016 年 12 月 31 日 BGP AS links 数据集[31]构建仿真环境.该数据集中,AS 节点数量为 24 742 个,节点之间链路数量为 47 299 条.根据文献[32]对路由器压力测试结果,实验中设置节点最大路由更新处理和报文转发能力分别为正常状态下路由表大小和转发流量的 2 倍.链路带宽根据链路在拓扑图中的介数,分别设置为 100M~40Gb.设置正常通信终端节点 1 000 000 个,botnet 攻击节点 300 000 个.对系统进行 BGP-LDoS 攻击时,攻击节点采用复用技术,每个节点攻击时流量脉冲设置为 1Mbps.

实验过程中,区分未实施攻击前的正常状态(normal situation)和实施 BGP-LDoS 后的攻击状态(BGP-LDoS attack),对系统 4 类数据进行统计:① 全系统路由节点状态(whole system AS data,简称 WSAD),即系统中所有路由节点的会话重置、有效报文转发、路由更新报文等数据;② 关键路由节点状态(critical AS data,简称 CAD),即系统中关键节点的会话重置、有效报文转发、路由更新报文等数据,按照节点的度数进行排序;③ 全系统链路流量(whole links traffic data,简称 WLTD),即系统中每条链路上的流量数据;④ 关键链路流量(critical links traffic data,简称 CLTD),即在 CAD 中,所选关键节点之间链路的流量数据.对于流量数据,设置 20ms 搜索间隔、10ms 采样间隔,对其中可能存在的攻击流量周期、脉冲持续时间和脉冲强度进行分析和提取.流量特征、路由特征数据的采样单位时间 *t* 设置为 3s.实验分别获取 Normal Situation 和 BGP-LDoS Attack 两种状态下 30 分钟内所有节点和链路的数据,剔除其中的系统初始化数据以及无效数据,获取两种状态下的有效样本各 500 组.

测试时,使用如下两个评价指标:① 正确检测率(truth positive rate,简称 TP),指被正确标记的攻击测试样本占全部攻击测试样本的比例;② 误报率(false positive rate,简称 FP),指被错误标记的攻击测试样本占全部攻击测试样本的比例.进行实验验证时,Normal Situation 和 BGP-LDoS Attack 两种状态数据以 1:1 的比例混合后作为训练和测试样本,样本中两种状态数据各 500 组时,标记样本容量为 500.实验采用 10 次 10 折交叉验证,取平均值为最终结果.

实验 1. 监测系统全部链路和节点时,ESCT 方法对 BGP-LDoS 攻击的检测效果.

以(WSAD,WLTD)作为训练和测试集时,ESCT 方法检测结果如图 9 所示.

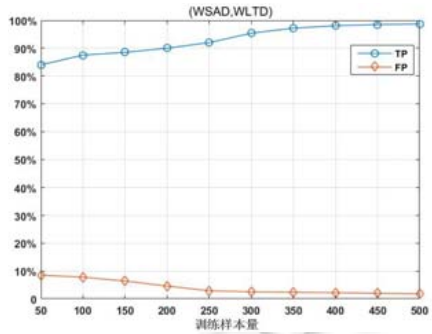


Fig.9 ESCT detection results under different number of samples in data set (WSAD,WLTD)

图 9 (WSAD,WLTD)中不同训练样本量下 ESCT 检测结果

从图 9 可以看出:当监测系统全部节点和链路条件下,训练样本容量为 350 时,ESCT 取得了 97.6%检测率和 2.1%的误报率;随着训练样本集的增大,ESCT 方法最高能够取得 98.5%检测率和 1.8%误报率.该实验结果证明了 ESCT 在检测 BGP-LDoS 时的有效性.

尽管对系统全部节点和链路进行监测能够获取较为准确的检测结果,但互联网域间路由系统中节点和链路数量规模较大,且呈现出不断增长的态势.对系统所有节点和链路进行监测不仅增大了 ESCT 方法的部署难度,还导致检测算法计算开销过大,降低了方法的可用性.分析 BGP-LDoS 攻击过程,BGP-LDoS 主要攻击对象是系统中的关键节点和链路,而对边缘节点和链路影响较小.文献[33]研究表明:在互联网域间路由系统中,大量节点链路为边缘节点链路,而关键节点和链路所占比例较小.为此,实验进一步验证了仅监测系统部分关键节点链路情况下 ESCT 方法检测性能.

实验 2. 监测系统部分关键节点和链路时,ESCT 方法对 BGP-LDoS 攻击的检测效果.

首先,按照节点的度数(degree)、介数(betweenness centrality)和所在图的核数(kcore)这 3 类指标对所用实验数据集进行分析,结果如图 10 所示.

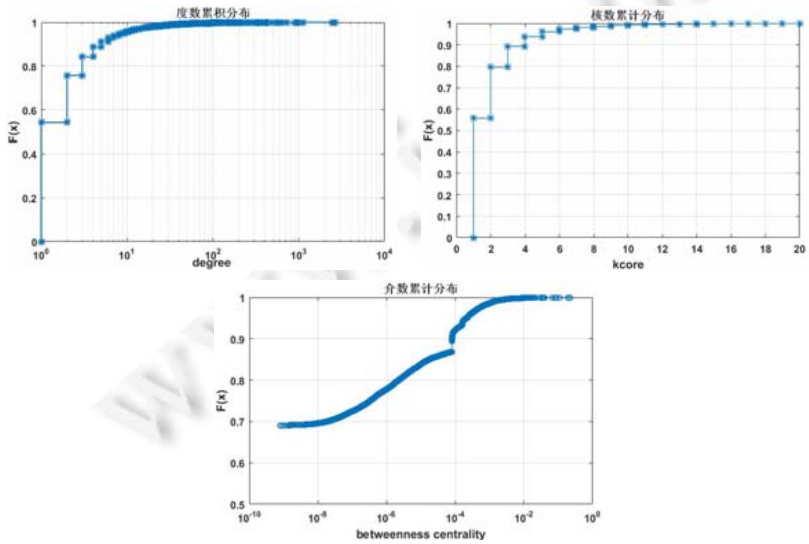


Fig.10 Distribution of different types of nodes in CAIDA data set

图 10 实验数据集中不同类型节点的分布情况

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.

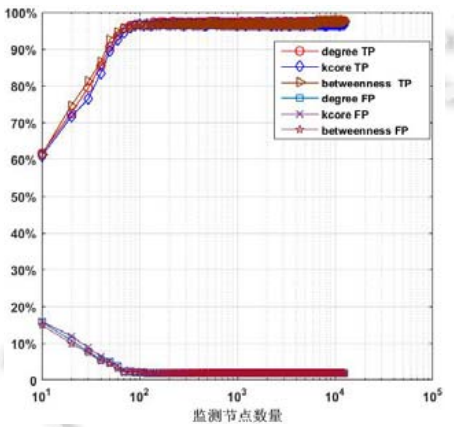


Fig.11 Results of ESCT detectionunder different monitoring conditions

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:

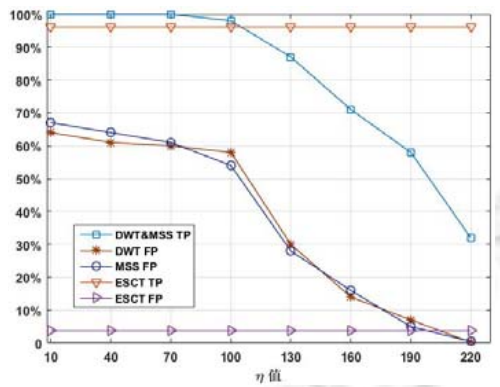


Fig.12 Results of the three detection methods

图 12 3 种检测方法检测结果对比

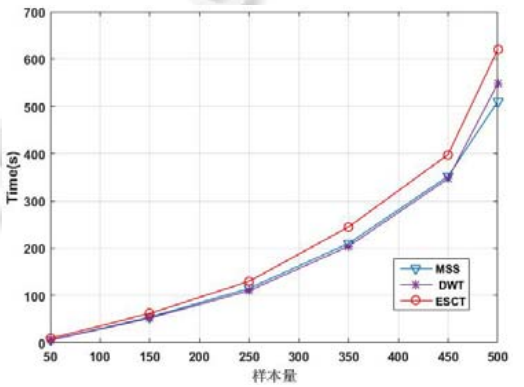


Fig.13 Comparison of execution time between the three detection methods with different number of samples

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.

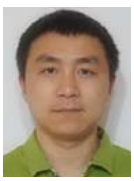
附中文参考文献:

[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.