·计算机工程与应用·

基于尖点突变模型的IP网络异常行为检测方法

阳小龙[1]，张 敏[1,2]，胡武生[2]，徐 杰[2]，隆克平[1]

(1. 北京科技大学计算机与通信工程学院 北京 海淀区 100083; 2. 电子科技大学通信与信息工程学院 成都 611731)

【摘要】由于数据挖掘、贝叶斯等传统异常检测方法仅依据网络正常行为特征而没考虑异常行为特征，致使其异常检测率偏低和误报率偏高，该文基于尖点突变模型而针对性地提出了一种新的IP网络异常行为描述模型及其检测机制。它们充分利用了尖点突变模型的多稳态性和突变性，准确地描述了网络正常行为特征和异常行为特征。最后以Kdd-Cup 99数据集为例，对比了不同机制的异常检测性能，结果显示，与贝叶斯BN和决策树C4.5等机制相比，所提出的检测机制在检测率和误报率方面都有所优势。

关 键 词 异常检测; 尖点突变; IP网络; Kdd-Cup 99数据集

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2011.06.017

IP Network Anomalous Behaviors Detection Mechanism Based on Cusp-Catastrophe Model

YANG Xiao-long[1], ZHANG Min[1,2], HU Wu-sheng[2], XU Jie[2], and LONG Ke-ping[1]

(1. School of Computer and Communication Engineering, University of Science and Technology Beijing Haidian Beijing 100083;
2. School of Communications and Information Engineering, University of Electronic Science and Technology of China Chengdu 611731)

Abstract Some traditional anomaly detection mechanisms (such as data mining and Bayes methods) have much poorer performance in terms of detection rate and false alarm rate because they consider only the normal behavior feature of IP networks, and neglect that of the abnormal behaviors. Motivate by the situations, this paper proposed a new characterization model of abnormal behaviors, and also developed an anomaly detection mechanism based on cusp-catastrophe for IP networks. They not only make the best of the prominent features of cusp-catastrophe in terms of multiple steady states and discontinuous catastrophe, and also can describe the normal behavior features and abnormal ones. Finally under Kdd-Cup 99 datasets, the proposed mechanism is evaluated, and the evaluation result shows that its detection rate and the false detection have greatly been improved compared with *BN* and *C4.5*.

Key words anomaly detection; cusp-catastrophe; IP networks; KDD-cup 99 dataset

当前DoS(denial of service)、Probe、U2R(user to root)和R2L(remote to local)等网络恶意攻击事件不断出现，严重影响IP网络的正常运行。因此，如何有效地分析和检测网络故障或恶意攻击显得非常重要。如果能建立一种描述网络异常行为的模型，并提出相应的异常检测机制，准确地判断网络是否发生异常，就可采取一些有效措施减少异常对网络性能的影响。当前，一些主流的网络异常检测模型或方法(如数据挖掘、贝叶斯等)仅考虑网络的正常行为特征，没有考虑网络的异常行为特征，导致较低的异常检测率和较高的误报率[1-2]。为此，文献[1-2]在检测阶段采用了Mahalanobis距离和相似性测度等方法计算输入数据的相似性，以降低误报影响，提高异常检测精度。但是在遭遇异常事件时，IP网络行为常常会出现突变现象(如服务器遭受DoS攻击时，其服务质量和网络吞吐量可能突然恶化；当网络拥塞控制崩溃时，即使网络负载微小增加，也可能引起IP网络吞吐量急剧下降)，致使文献[1-2]的方法对网络异常行为的检测效果仍不理想。目前已有学者成功地利用突变理论解决了智能交通领域的交通流

收稿日期：2010－03－15； 修回日期：2011－05－20

基金项目：国家973计划(2007CB310706，2012CB315905)；国家自然科学基金(60725104，60873263，60932005，61172048，61100184)；教育部新世纪优秀人才支持计划(NCET-09-0268)；四川省青年基金(09ZQ026-032)；广东省产学研项目(2010A090200053)

作者简介：阳小龙(1970－)，男，博士，教授，博士生导师，主要从事新一代互联网、光互联与光交换、网络安全等方面的研究.

量控制和交通流量异常检测[3-4]，受此启发，现有不少学者也试图用突变理论解决IP网络的异常行为检测[5]。文献[5]作了一些探索性研究，利用突变理论对网络异常行为进行描述，并结合网络异常行为特征进行异常检测。但是该文献未能准确地用突变理论描述网络的异常突变行为，导致异常行为检测机制不完善，而且该文献也没有通过理论和实际仿真验证比较该类机制和传统机制的性能优劣。

为了降低传统异常检测机制的误报率，提高检测效率[1-10]，本文将网络异常行为特征和突变理论相结合，提出了一种新的IP网络异常行为检测方法。由于IP网络异常行为具有突变性，因此可首先根据网络行为特征对IP网络行为进行聚类分析、数据拟合等处理，建立描述网络正常和异常行为的突变模型。然后再对突变模型进行置信估计，构建能描述IP网络从正常到异常的突变过程的尖点突变模型。最后再根据行为模型参量间的关系，基于尖点突变模型构建一种高效的异常行为检测机制。以Kdd-Cup 99数据集(国际上的一种网络入侵检测性能分析的通用实验数据集)[11]为例，将上述模型和检测机制的性能与传统的基于正常行为的异常检测机制(如贝叶斯法和决策树法)进行仿真比较，结果表明本文机制在检测率和误报率上都有较大的改善。

1　IP网络性能的异常突变现象

一般地，在没有采取任何保护措施的情况下，IP网络性能会因网络故障或恶意攻击而恶化。例如，当IP网络受DoS或DDoS攻击时，服务器或路由器瞬间内收到大量攻击包，致使计算、存储、带宽等资源被恶意占用，严重影响正常用户的QoS。本文以Kdd-Cup 99实验数据为例，对IP网络因受到异常攻击而出现的性能异常突变现象进行分析，如图1所示。

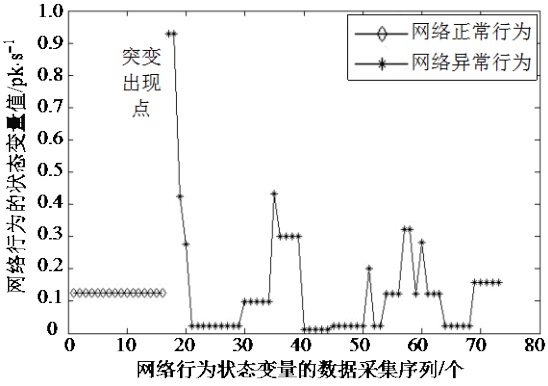


图1　Kdd-Cup 99网络从正常变化至异常时突变

在图1中，横坐标为网络吞吐量的采样时刻点，纵坐标为吞吐量经标准化处理后的数据值。在0～17采样点内，实际网络没有遭受任何攻击，但在第18个采样点时，网络因遭受Smurf、Back等DoS攻击，网络吞吐量出现了严重的突变现象。对该现象，本文将用突变理论给予解释，并构建一种描述网络异常行为的突变模型，提出相应的异常检测机制。

2　IP网络异常突变行为的描述模型

突变理论(catastrophe theory)主要研究系统的突变性、多态性、发散性等不连续性特征[12-13]。文献[12]已证明：当控制变量不大于4个时，突变模型最多有7种，其中主要包括折叠突变、尖点突变、燕尾突变模型等，而各突变模型的特性由它们的势函数确定。由文献[5]和[15]的初步研究结果可知：尖点突变模型的两个平衡状态不仅能准确地描述复杂系统的脆性状态，也能准确地描述IP网络的正常和异常状态，以及直观地反映IP网络中的正常和异常状态间的转化过程。由文献[13]尖点突变模型可表示为：

$$\begin{cases} \text{势函数：} v(x)=x^4+aux^2+bvx \\ \text{平衡曲面：} \quad 4x^3+2aux+bv=0 \\ \text{分叉集：} \quad 8a^3u^3+27b^2v^2=0 \end{cases} \tag{1}$$

式中，a、b是系数；x是描述模型行为的状态变量，而u和v是影响模型变化的控制变量。由u和v对行为模型控制作用的不同，u和v可分别定义为分裂因子和正则因子。它们对模型行为的影响如下：

1) 当$u>0$时，v变化，x随之平滑变化。

2) 当$u<0$时，v变化，x可能不连续变化，即出现突变现象。

为了标准化突变模型，将式(1)中的平衡曲面和分叉集函数进行平移变换，有：

$$\begin{cases} 4x^3+2a(u-u')x+b(v-v')=0 \\ 8a^3(u-u')^3+27b^2(v-v')^2=0 \end{cases} \tag{2}$$

式中，u'和v'是控制变量在模型发生突变时的临界值。

2.1　IP网络异常行为描述模型

图1表明，当网络严重遭受DoS攻击时，网络负载和异常流量增大，网络吞吐量发生突变。为了描述该现象，可根据网络流量、负载、吞吐量之间的关系，将吞吐量作为状态变量，负载和异常流量作为控制变量。本文中，吞吐量、网络负载、异常网络流量样本可表示如下：

$$S_c=\{(X_1^i,U_1^i,V_1^i)|i=1,2,\cdots,n\} \tag{3}$$

对已采集到的上述样本作如下平移预处理：

$$v=v_1-v'$$
$$u=u_1-u'$$

$$x=x'$$

式中，v'、u'和x'分别为控制变量v、u和状态变量x的异常临界值。x'、u'、v'、a和b仍然为尖点模型的因子，其中x'、u'和v'直接由采集数据确定，而a和b需由模型求解。

对参数a和b，可采用多元函数求解极值法求解得到最优值[5]。本文首先定义一种平方和形式的如下函数：

$$f(a,b)=\sum_{i=1}^{n}\{[4(x_1^i)^3+2a(u_1^i-u')x_1^i+b(v_1^i-v')]^2+ [8a^3(u_1^i-u')^3+27b^2(v_1^i-v')^2]^2\} \tag{4}$$

为了使S_c点集满足式(2)，$f(a,b)$须取最小值。如果$f(a,b)$等于0，S_c就能满足式(2)。由此可对$f(a,b)$分别求a和b的偏导，并建立方程组：

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

将$S_c=\{(X_1^i,U_1^i,V_1^i)|\ i=1,2,\cdots,n\}$代入式(5)，即可得如下等效方程组：

$$\begin{cases}\sum_{i=1}^{n}[(u_1^i-u')x_1^i][4(x_1^i)^3+2a(u_1^i-u')x_1^i+b(v_1^i-v')]+ 12a^2(u_1^i-u')^3[8a^3(u_1^i-u')^3+27b^2(v_1^i-v')^2]=0\\ \sum_{i=1}^{n}[(v_1^i-v')x_1^i][4(x_1^i)^3+2a(u_1^i-u')x_1^i+b(v_1^i-v')]+ 54b(v_1^i-v')^2[8a^3(u_1^i-u')^3+27b^2(v_1^i-v')^2]=0\end{cases} \tag{6}$$

求解该方程组，即可得m组(a_i,b_i)解，其中a和b是含参数x_1'、u'和v'的解。然后将m组解分别代入表达式$f''_{ab}-f''_{aa}f''_{bb}$和$f''_{aa}$，存在唯一解满足$f''^2_{ab}-f''_{aa}f''_{bb}<0$和$f''_{bb}>0$，说明$f(a,b)$存在唯一极小值点，即存在最优解$(a,b)$使得$S_c$满足式(2)，于是$x_1'$、$u'$和$v'$也为最优。本文将求解参数$(a,b)$问题转化为求解未知异常临界值$(x_1,u',v')$问题，采用该方法即可推导出参数$a$和$b$是异常临界值$(x_1,u',v')$的函数。

2.2 网络异常行为临界值计算

由上述分析可知，建立描述网络异常行为的尖点模型的关键在于如何准确地求出其行为异常临界值(x',u',v')。从原始采样数据中获得异常和正常数据集，很难确保数据未受攻击或拥塞等异常事件的影响。为此，本文拟采用聚类方法区分原始数据序列x中的正常和异常数据[14]。该方法依据数据间相似度(以数据点之间的距离为参照)区分正常数据和异常数据，并排除孤立点或噪声点对分类的影响。由此，采样数据经分类预处理后，即可得到状态变量的正常值和异常数据。由于异常数据间的相似程度很高，因此可取该组数据的平均值为状态变量的异常临界值。将之前得到的最优解(a,b)和IP网络实际数据(X_1^i,U_1^i,V_1^i)代入式(2)，即可解得控制变量的临界值u'和v'。由此，即可求解x、u'和v'的函数值a、b，从而可以建立一个完整的尖点模型。

3 IP网络异常检测机制

上述研究表明，网络异常时行为存在突变现象，根据突变理论对采集的网络数据进行分析，可建立一种准确描述网络行为的尖点模型，如图2所示。该模型可清晰地确定网络正常行为和异常行为的分界区，并根据该行为模型参量异常的逻辑关系建立异常检测机制。

为了便于得到行为模型参量异常的逻辑关系，将异常检测中的一些相关事件分别定义如下。

1) 事件A定义为：测试数据数据中，若表征控制变量的数据$(u，v)$分布在行为模型的交叉集内，则事件A的逻辑值为1，其数学表达式为：

$$\{(u,v)|8a^3u^3+27b^2v^2\leqslant 0,a\in R,b\in R\} \tag{7}$$

2) 事件B定义为：如果正则因子v到达异常临界值，则其逻辑值为1。

3) 事件C定义为：测试数据中，如果表示状态变量的数据x超过其异常临界值，则其逻辑值为1。

4) 事件D定义为：如果最终检测结果为异常，则其逻辑值为1。

5) 事件E定义为：如果检测模型把可疑正常行为判为正常状态，则其逻辑值为1。

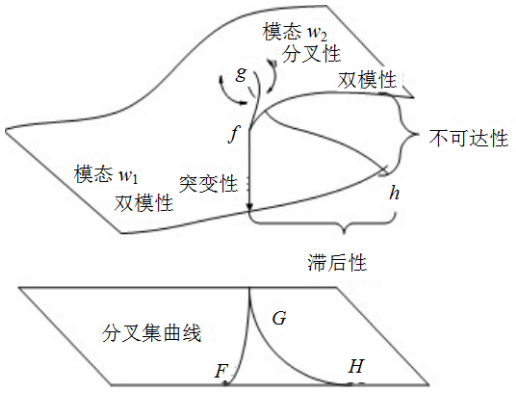


图2 尖点突变模型的平衡曲面和分叉集

综合上面的事件定义，即可建立一种检测异常行为机制。考虑到整个检测过程中事件的完备性，应该双向地描述IP网络行为在正常和异常间的转化

过程。假设正常网络状态分布在模态1上，异常状态分布在模态2上(如图2所示)，则正常和异常间的相互转化过程可描述如下：

1) 网络行为(x,u,v)从模态w_1转化至模态w_2的过程中，各事件逻辑转换关系如表1所示。

表1　从正常变至异常过程的状态真值表

A	B	C	D(异常报警)	E(可疑正常)
0	0	0	0	0
1	0	0	0	1
1	1	0	0	1
0	1	1	1	0

2) 网络行为(x,u,v)从模态w_2转化至模态w_1的过程中，各事件逻辑转换关系如表2所示。

表2　从异常变至正常过程的状态真值表

A	B	C	D(异常报警)	E(可疑正常)
0	1	1	1	0
1	1	1	1	0
1	0	1	1	0
0	0	0	0	0

通过表1得逻辑表达式：

$$\begin{cases} D_1 = \overline{A}BC \\ E_1 = A\overline{C}\,\overline{D} \end{cases} \tag{8}$$

通过表2得逻辑表达式：

$$D_2 = C(B + A\overline{B}) \tag{9}$$

综合上述两种情况，IP网络异常行为检测机制的逻辑表达式为：

$$\begin{cases} D = D_1 + D_2 \\ E = E_1 + E_2 \end{cases} \tag{10}$$

经简化后得：

$$\begin{cases} D = C(B + A\overline{B}) \\ E = A\overline{C}\,\overline{D} \end{cases} \tag{11}$$

4　实验和分析

4.1　数据预处理

本文仍以Kdd-Cup 99数据集为例，验证分析本文提出的检测机制。该数据集由训练数据(包含正常数据及类型已知的异常数据)和测试数据组成，其中训练数据包含DoS、Probe、R2L、U2R等4类攻击[11]，且训练数据和测试数据各自独立。Kdd-Cup 99数据集中，每个网络连接由41维属性标识。显然，41维属性之间存在较大的信息冗余，所以本文拟采用文献[16]提出的关键属性标识每个网络连接。根据各关键属性对网络性能影响的不同，可将它们进一步划分为表示网络状态的属性(如建立了的服务连接次数等)、影响网络状态变化u的属性(如单个TCP连接的数据流量及错误连接碎片数目等)和影响网络状态的控制变量v的属性(如一次连接受到威胁的次数和出现SYN、REJ错误的连接次数)等3类。在属性编号映射表中，该3类属性对应的编号分别为{10,12,24,29,30,31}、{1,5,6,8,23,24}和{13,22,33,36,38,39,40}[11]。验证性实验中采用的训练数据(training data)、测试数据(corrected data)的数据量和它们对应的异常类型如表3所示。虽然从41维属性挑选关键属性可降低建立检测模型的复杂度，但关键属性间仍存在量纲不一致的情况。为此，本文采用归一化思想对状态变量和控制变量数据进行相关处理。

表3　实验训练和测试数据规模

攻击类型	训练数据/条	测试数据/条
DoS	16 510	16 957
Probe	2 010	2 097
R2L	583	553
U2R	76	29

4.2　突变模型的建立

4.2.1　网络异常行为的突变性

本文采用图示法对4.1节提供的数据进行描述，结果如图1所示。从图1可看出，突变点产生于网络的正常和异常分界点上。此外，还可根据数理统计中的t假设检验方法，判别网络异常时行为是否有突变现象[18]。本文进一步对Kdd-Cup 99中的训练数据作滑动t假设检验，由处理后的数据可得：从正常到异常的过程中，网络性能存在显著性差异，即异常行为存在突变现象。

4.2.2　IP网络异常行为模型实例化

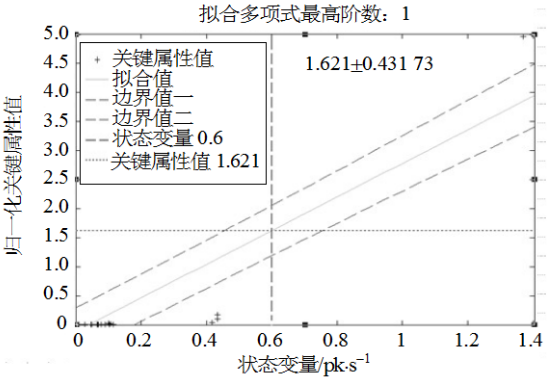
突变理论中存在多种突变模型，具体的突变模型由该模型的势函数确定。如果能得到描述网络异常行为的突变模型的势函数，便可求出平衡曲面和分叉集，分析网络异常行为的变化。

下面结合4.1节的数据，推导描述网络异常行为的模型。目前建立突变模型势函数的方法有如下两类：1) 处理状态变量的输出观测序列[15]，结合随机过程的一维分布函数，依据突变理论的反常方差建立势函数[12]；2) 根据复杂系统之间的演变关系确定描述网络异常行为模型的势函数[16]。方法1)需要求出反常方差中的所有参数，但实际条件难以满足。因此本文拟采用方法2)对实验数据进行拟合。通过分析两个系统输出的演化关系，即可推算出具体的

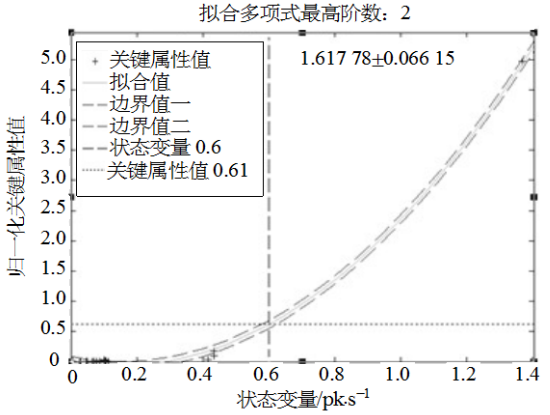
突变模型。本文拟定的两个系统输出为：1) 5.1节中的状态变量属性值(系统1)；2) 5.1节中的所有关键属性(系统2)。突变模型势函数的阶数由非线性最小二乘拟合方法确定[15]，对拟合结果进行置信的估计如图3所示。由图3可看出，最准确的多项式阶数为3，其中拟合标准误差为$|\varepsilon|=8.6\times10^{-3}$，拟合多项式为：

$$f(x)=2.383\ 1x^3-0.692\ 72x^2+0.105\ 9x-0.094\ 279 \tag{16}$$

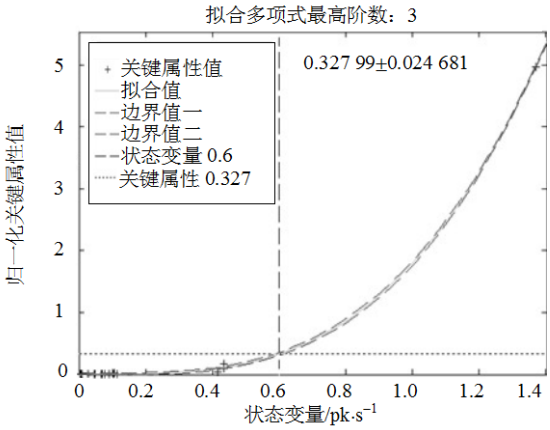
以上实验结果表明，尖点突变模型更能准确地描述网络异常行为。



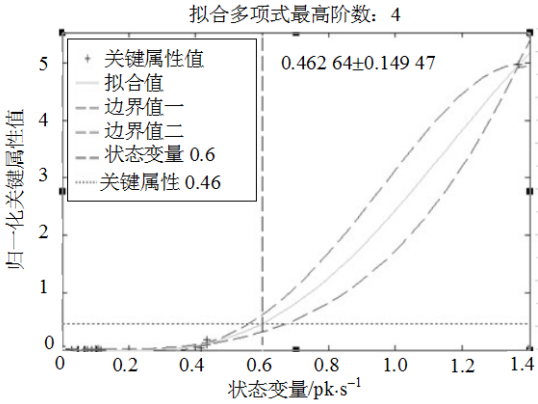
a. 最高阶数为1的置信估计



b. 最高阶数为2的置信估计检验



c. 最高阶数为3的置信估计



d. 最高阶数为4的置信估计

图3 网络行为模型置信检验图

为不失一般性，把尖点突变模型的势函数写成式(1)。结合实验数据和3.2节的方法求得参数(a,b)的值为$(-0.077\ 8,-0.002\ 6)$；状态变量、控制变量的异常临界值(x,u,v)为$(0.075,0.000\ 4,0.020\ 4)$。

4.3 检测结果及分析

以Kdd-cup测试数据为例，将本文检测机制的验证结果与其他方法对比。本文采用检测率(被检测出的异常数占总异常数的比率)和误检率(被检测为异常的正常行为在所有正常行为中的比率)作为评判指标。为了评估本文提出的异常检测机制的有效性，本文将其与基于贝叶斯(BN)、决策树(C4.5)的异常检测方法[16]相比，其中BN和C4.5方法采用的属性参数和本文采用的关键属性类型相同。本文异常检测方法与BN、C4.5检测方法的性能对比结果如表4所示。

表4 本文检测方法与BN和C4.5检测结果对比

异常类型	算法	检测率/(%)	误检率/(%)
DoS	本文方法	97.96	1.5
	BN	99.88	0
	C4.5	99.87	0.14
Probe	本文方法	62.5	2.34
	BN	82.63	3.06
	C4.5	82.88	0.05
R2L	本文方法	85.57	1.71
	BN	89.33	0.32
	C4.5	87.34	0.01
U2R	本文方法	74.42	1.71
	BN	65.5	0.12
	C4.5	24.14	0

从表4可知：基于尖点突变的异常检测机制对DoS、R2L的检测效果与BN、C4.5的检测方法相当；对U2R的异常检测，本文提出的检测机制比BN、C4.5两种方法的检测率要高。通过分析U2R发现，在所有的攻击中，U2R攻击的次数明显偏少，攻击的时间间隔较长，攻击行为很类似于正常行为。BN和C4.5等传统异常检测机制建立在正常行为之上，对于类似于正常行为的攻击，其检测率较低正是由于

上述特性决定的。而本文提出的基于突变理论的异常检测方法建立在正常和异常行为之上，并充分利用突变理论的自身特性，能够适用于内部作用尚属未知的系统，故对U2R异常，本文的检测方法比BN和C4.5方法要好。对Probing攻击检测，本文的检测方法的效果不是很好，这是因为受突变理论自身特性影响，Probing攻击并非直接对网络造成实质性的性能影响，而只对其他攻击提供一些信息。在误检率方面，BN和C4.5方法与本文提出的检测方法效果相当。

5 结 束 语

对于IP网络异常检测，本文提出了一种基于尖点突变模型的异常检测机制。在建立异常检测机制的过程中，给出了判定IP网络行为是否存在突变性的方法。通过对异常和正常行为进行聚类，以非线性最小二乘数据拟合等方法，建立了一个准确描述和检测网络异常行为的突变模型。对所得模型进行置信估计，确定尖点模型可准确描述突变异常的网络行为。异常检测机制结合突变模型的不连续突变性和多个平衡稳定状态，可动态地确定状态和控制变量异常阈值，对状态变量和控制变量异常变化进行检测，并以多个异常逻辑关系的检测机制判定整个网络是否发生异常。以Kdd-cup测试数据为例，将本文的异常检测方法与其他传统方法对比，结果表明，基于尖点突变的网络异常检测方法具有较强的优势。但是如何细化可疑正常状态，寻找避免突变异常发生的机制，将是下一步研究的重点。

参 考 文 献

[1] DESHPANDE S, THOTTAN M, HO T K, et al. A statistical approach to anomaly detection in interdomain routing[C]// Proc of BROADNETS 2006. San Jose, CA: [s.n.], 2006: 1-10.

[2] SRINIVASAN N, VAIDEHI V. Reduction of false alarm rate in detection network anomaly using mahalanobis distance and similarity measure[C]//Proc of ICSCN'07. Chennai, India: [s.n.], 2007: 366-371.

[3] FROBES G J, HALL F L. The applicability of catastrophe theory in modeling breeway traffic operators[J]. Transportation Research, 1990, 24A(5): 335-344.

[4] CHA D J A, HALL F L. Application of catastrophe theory to traffic flow variables[J].Transportation Research Part B: Methodological, 1994, 28(3): 235-250.

[5] 黄光球，胡晓婷, 刘通. 基于突变理论的网络异常行为分析方法[J]. 微电子学与计算机, 2006, 23(7): 24-27.
HUANG Guang-qiu, HU Xiao-ting; LIU Tong, An approach to analyzing network anomalous behaviors based on catastrophe theory[J], Microelectronics & Computer, 2006, 23(7): 24-27.

[6] WENKE L, STOLFO M S J. A data mining framework for building intrusion detection models[C]//Proc of 1999 IEEE Symposium on Security and Privacy. Oakland, CA, USA: [s.n.], 1999: 120-132.

[7] ZHONG Shi, KHOSHGOFTAAR T, NAEEM S. Clustering-based network intrusion detection[J]. International Journal of Reliability, Quality and Safety Engineering, 2007, 14(2): 169-187.

[8] GU Guo-fei, CARDENAS A, WENKE L. Principled reasoning and practical applications of alert fusion in intrusion detection systems[C]//Proc of ASIACCS'08. Tokyo, Japan: [s.n.], 2008: 136-147.

[9] ALARCON A V, BARRIIA J A. Anomaly detection in communication networks using wavelets[J]. IEEE Communications Proceedings, 2001, 148(6): 355-362.

[10] FRANKLIN N R, CARVER D, HUTCHINGS B L, Assisting network intrusion detection with reconfigurable hardware[C]//Proc of IEEE FCCM'02. Napa, California, USA: [s.n.], 2002: 111-120.

[11] KDD Cup 1999 Data. http://kdd.ics.uci.edu/

[12] 凌复华. 突变理论及其应用[M]. 上海: 上海交通大学出版社, 1987: 1-129.
LIN Fu-hua, Catastrophe theory and its applications[M]. Shanghai: Shanghai Jiaotong University Press, 1987: 1-129.

[13] 桑博得. 突变理论入门[M]. 凌复华 译. 上海: 上海科学技术文献出版社, 1983: 2-53.
SAUNDERS PT. Introduction to Catastrophe theory[M]. Translated by LIN Fu-hua. Shanghai: Shanghai Scientific and Technological Literature Publishing House, 1983: 2-53.

[14] DANIEL W K, ABM S. Unique distance measure approach for K-means clustering algorithm[C]//Proc of IEEE TENCON'07. Taipei, China: [s.n.], 2007: 1-4.

[15] 郭建. 突变理论在复杂系统脆性理论研究中的应用[D]. 哈尔滨: 哈尔滨工程大学, 2004.
GUO Jian, The application of catastrophe theory in the research of complex system brittleness theory[D]. Harbin: Harbin Engineering University, 2004.

[16] WANG Wei, GOMBAULT S, GUYET T. Towards fast detecting intrusion: using key attributes of network traffic [C]//Proc of ICIMP'08. Bucharest, Romania: [s.n.], 2008: 86-91.

[17] 郑苗苗, 吉根林. 一种处理混合型属性的无监督异常入侵检测方法[J]. 南京师范大学学报(工程技术版), 2008, 8(2): 68-73.
ZHENG Miao-miao, JI Gen-lin, An unsupervised anomaly intrusion detection for the mixed attributes[J]. Journal of Nanjing Normal University (Engineering and Technology Edition), 2008, 8(2): 68-73.

[18] 潘承毅, 何迎晖. 数理统计的原理与方法[M]. 上海: 同济大学出版社, 1999: 142-153.
PAN Cheng-yi, HE Ying-hui. Mathematical statistics principle and methods[M]. Shanghai: Tongji University Press, 1999: 142-153.

编　辑　蒋　晓