多阶段大规模网络攻击下的网络安全态势评估方法研究

唐赞玉[1] 刘 宏[2]

(吉首大学信息科学与工程学院 湖南 吉首 416000)[1] (湖南师范大学数学与计算机学院 长沙 410081)[2]

摘 要 针对传统的网络安全态势评估方法一直存在评估偏差较大的问题,为了准确分析网络安全状况,提出一种新的多阶段大规模网络攻击下的网络安全态势评估方法。首先根据多阶段大规模网络攻击下的网络安全多数据源的特点,建立基于信息融合的多阶段大规模网络攻击下的网络安全态势评估模型;然后对大规模网络攻击阶段进行识别,计算网络攻击成功的概率和网络攻击阶段的实现概率;最后利用CVSS中的3个评价指标对网络安全态势进行评估。实例分析证明,所提方法更加符合实际应用,评估结果准确且有效。

关键词 多阶段大规模网络攻击,网络安全态势,评估方法

中图法分类号 TP393 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2018.01.043

Study on Evaluation Method of Network Security Situation under Multi-stage Large-scale Network Attack

TANG Zan-yu[1] LIU Hong[2]

(College of Information Science and Engineering, Jishou University, Jishou, Hunan 416000, China)[1]

(School of Mathematics and Computer, Hunan Normal University, Changsha 410081, China)[2]

Abstract For the traditional network security situation assessment method, there is always a problem of large evaluation bias. In order to accurately analyze the network security situation, a network security situation assessment method of multi-stage large-scale network attack under the new network security was proposed. Firstly, based on the characteristics of multiple data sources under multi-stage large-scale network attack, the network security situation assessment model of multi-stage large-scale network attack was established based on information fusion. Next, large-scale network attack stage was identified, and the success probability of network attack and implementation probability of network attack phase were calculated. Finally, three indexes in CVSS was used for network security situation assessment. The example analysis shows that the proposed method is more suitable for practical application, and the evaluation results are accurate and effective.

Keywords Multi-stage large-scale network attack, Network security situation, Assessment method

1 引言

随着计算机网络技术和通信技术的快速发展,计算机网络的资源共享进一步增强,互联网已经深入人类生产生活的方方面面,并影响着社会经济的发展和人们的生活方式[1-2]。网络给人们带来了便捷,但其自身存在的脆弱性不可避免地带来了各种潜在的安全风险。目前网络攻击行为日益猖獗,网络攻击方式也层出不穷,对个人、企事业单位,乃至国家机关都造成了极大的经济损失,网络的安全正面临着巨大挑战[3]。随着近年来各种网络破坏事件数目的不断增加和破坏程度的逐渐加大,网络安全技术引起了人们的重点关注,现如今各种攻击技术不断变异和提升(特别是多阶段大规模网络攻击)[4]。传统方法只是对已经发生的网络攻击行为进行报警和拦截,无法满足现实需要,人们需要认识、理解多阶段大规模网络攻击并预测网络安全状态及其未来发展趋势,这有助于网络管理员及时掌握当前网络状况,并对未来可能出现的威胁做好提前防护性准备,避免多阶段大规模网络攻击对网络的危害[5]。目前,基于攻击模式识别的多阶段大规模网络攻击下的网络安全态势评估方法[6]首先对多阶段大规模网络攻击下的网络报警数据进行分析,识别出其攻击的最终目的以及当前网络的攻击阶段;然后将当前网络所处的攻击阶段作为要素,对当前网络的安全态势进行评估;最后构建多阶段大规模网络攻击阶段状态的转移图,结合网络主机漏洞和相关配置,实现对当前网络的安全态势评估。网络安全态势评估逐渐成为当前网络安全风险评估中的重点研究课题,已经涌现了许多不同方法[7]。

文献[8]提出一种基于攻击图的多阶段大规模网络攻击下的网络安全态势评估方法,该方法首先对多阶段大规模网络攻击下的攻击行为信息进行分析,然后建立网络安全风险评估模型,计算多阶段大规模网络攻击成功的概率和攻击后果度量标准。该方法存在评估偏差较大的问题。文献[9]主要利用信息融合的方式实现多阶段大规模网络攻击下的网络安全态势评估,首先提出了以数据包信息为网络原始数据的多阶段大规模网络攻击威胁评估方法;然后对网络原有的漏洞和脆弱性进行评估;再结合网络的主客观权重,利用序列二次规划算法对其进行寻优;最后将三者进行信息融合得到当

到稿日期:2017-06-26 返修日期:2017-10-10 本文受国家自然科学基金项目(61662025)资助。

唐赞玉(1978—),女,硕士,讲师,主要研究方向为计算机网络、分布计算和自动控制等,E-mail:tzyu2166@163.com(通信作者);刘 宏(1963—),男,硕士,教授,主要研究方向为分布式计算、人工智能等。

前的网络安全态势。该方法存在可靠性和适用性较差的问题。文献[10]提出的网络安全态势评估方法主要以攻击模式识别为基础，首先对多阶段大规模网络攻击下的网络报警数据进行分析，识别出其攻击最终目的以及当前网络所处的攻击阶段；然后将当前网络所处的攻击阶段作为要素，对当前网络的安全态势进行评估；最后构建多阶段大规模网络攻击阶段状态的转移图，结合网络主机漏洞和相关配置信息，实现对网络安全态势的评估。该方法存在评估结果准确度较低的问题。

为了能够更加准确地反映多阶段大规模网络攻击的实际情况，提高预测的准确性，提出一种新的多阶段大规模网络攻击下的网络安全态势评估方法。实验结果表明，所提方法能够对网络安全态势进行准确可靠的评估，具有良好的实用性。

2 多阶段大规模网络攻击下的网络安全态势评估方法研究

2.1 多阶段大规模网络攻击下的网络安全态势评估模型

根据网络安全多数据源的特点，建立基于信息融合的多阶段大规模网络攻击下的网络安全态势评估模型。具体过程如下：

根据网络自身的特点，将多阶段大规模网络攻击下的网络安全态势评估指标分为两类：网络安全信息(N)和多阶段大规模网络攻击信息(I)，并针对多阶段大规模网络攻击下的网络安全态势评估指标进行以下建模。

网络安全信息 N 主要包括网络主机节点信息和网络拓扑信息，其表达式为：

$$N=(H,T) \tag{1}$$

其中，H 表示网络主机节点的所有信息集合，网络主机节点既包括普通网络服务器或普通台式机，又包括具有独立操作系统的网络组件，例如路由器、交换机等。对于网络中的任意一个主机节点信息 $h\in H$，可以用一个四元组(id，w_H，$svcs$，$vuls_H$)来表示。其中，id 表示网络主机节点的唯一标识符；w_H 表示网络主机节点的权重值；$svcs$ 表示在网络主机节点上运行的多媒体应用服务；$vuls_H$ 表示在网络主机节点上存在的漏洞信息，通常包括软件漏洞、硬件漏洞以及网络主机的配置错误等。

假设网络拓扑信息集合表示为 T，它包括网络中所有物流链接关系的集合，其表达式为：

$$T\subset H\times H \tag{2}$$

多阶段大规模网络攻击信息表示为 I，它包括已知的多阶段大规模网络攻击信息和检测出多阶段大规模网络攻击的信息，其表达式为：

$$I=(I_p,I_q) \tag{3}$$

其中，I_p 表示已知的多阶段大规模网络攻击信息，网络中的任何一个已知的多阶段大规模网络攻击信息满足 $i_p\in I_p$，用一个四元组(id'，$vuls_t$，Log_p，V)来表示，其中 id' 表示多阶段大规模网络攻击信息的唯一标识符；$vuls_t$ 表示多阶段大规模网络攻击所依赖的网络漏洞；Log_p 表示已知多阶段大规模网络攻击在检测设备上预知的日志集合；V 表示多阶段大规模网络攻击的威胁值。

式(3)中的 I_d 表示检测到的多阶段大规模网络攻击信息，网络中的任何一个检测到的多阶段大规模网络攻击信息均满足 $i_d\in I_d$，可以用一个二元组表示为(id''，Log_d)，其中 id'' 表示在网络攻击检测设备的唯一标识符；Log_d 表示在网络攻击检测设备时间内检测到的多阶段大规模网络攻击信息的日志集合。

假设 SA 表示多阶段大规模网络攻击下的当前网络安全态势值，它主要由多阶段大规模网络攻击信息 I 和网络安全信息 N 两部分构成，其表达式为：

$$SA=(N,I) \tag{4}$$

2.2 多阶段大规模网络攻击下的网络安全态势量化分析

依据 2.1 节的多阶段大规模网络攻击下的网络安全态势评估模型，首先对大规模网络攻击阶段进行识别，然后计算网络攻击成功的概率和网络攻击阶段的实现概率。

选取网络源 IP 地址、大规模网络攻击的目的 IP 地址、网络源端口号、大规模网络攻击的目的端口号、大规模网络攻击时间这 5 个属性作为确定大规模网络攻击关联度的依据，定义大规模网络攻击关联度函数的计算表达式为：

$$cor(a,b)=\frac{\sum_{k=1}^{n}\alpha_k Feature_k(a,b)}{\sum_{k=1}^{n}\alpha_k} \tag{5}$$

其中，$Feature_k(a,b)$表示网络中第 k 个特征属性之间的关联度；α_k 表示网络中第 k 个特征属性的对应权重值。

根据式(5)，当网络收到新的安全事件警报时，将其与多阶段大规模网络攻击的不同场景进行匹配，计算网络新收到的安全时间与其之间的关联度，然后利用多阶段大规模网络攻击的关联度进行网络安全事件聚类，从而获得大规模网络攻击不同场景的相应报警集合。

假设 $P(a)$ 表示多阶段大规模网络攻击发生的概率；$Vlus_s$ 表示被入侵网络主机中存在的信息漏洞库，则多阶段大规模网络攻击成功的概率的计算公式如下：

$$P(ac)=\begin{cases}P(a), & vlus_t\in Vlus_s\\ 0, & \text{其他}\end{cases} \tag{6}$$

假设 $P_i(ac)$和 $P_j(ac)$分别表示多阶段大规模网络攻击行为 $Alter_i$ 和 $Alter_j$ 的成功入侵概率，则多阶段大规模网络攻击节点实现概率 $P(s)$的计算公式如下：

$$P(s)=\begin{cases}P_i(ac)+P_j(ac)-P_i(ac)P_j(ac), & d=0\\ P_i(ac)P_j(ac), & d=1\end{cases} \tag{7}$$

其中，$d=0$ 表示网络攻击下的网络状态节点 s 为或节点；$d=1$ 表示网络攻击下的网络状态节点 s 为与节点。

2.3 多阶段大规模网络攻击下的网络安全态势评估

根据多阶段大规模网络攻击成功的概率和网络攻击阶段的实现概率计算结果，利用 CVSS 中的 3 个评价指标对网络安全态势进行评估。

采用 CVSS 给出的基于网络机密性、网络完整性和网络可用性 3 个指标评价的网络漏洞威胁得分，来衡量单个网络漏洞对当前网络的影响，其威胁得分表示为：

$$Impact(v)=10(1-D)(1-J)(1-A) \tag{8}$$

其中，D，J，A 分别表示网络机密性、网络完整性、网络可用性的威胁影响得分。

由式(8)可知，多阶段大规模网络攻击的每一个攻击场景需要运用多个网络漏洞，将多阶段大规模网络攻击阶段实现概率 $P(s)$、多阶段大规模网络攻击阶段利用的所有单个网络漏洞威胁得分 $Impact(v)$以及多阶段大规模网络攻击阶段发生的节点权重值 $Weight$ 进行综合量化处理，可以得到网络攻击下不同攻击场景对当前网络安全态势的影响 $sa(path_i)$，其计算表达式如下：

$$sa(path_i)=\sum_{j=1}^{m}P_j(s)Impact(v)Weight \tag{9}$$

其中，m 表示多阶段大规模网络攻击场景 $path_i$ 以及实现的攻击阶段，且满足以下条件：

$$P_j(s)\leqslant 1 \tag{10}$$

$$Impact(v)\leqslant 10 \tag{11}$$

$$\sum Weight=1 \tag{12}$$

根据上述条件计算，可得：

$$sa(path_i)\leqslant 10 \tag{13}$$

假设当 $sa(path_i)\in[0,4.0]$ 时，多阶段大规模网络攻击对当前网络造成的危害属于低风险等级；当 $sa(path_i)\in[4.0,7.0]$ 时，多阶段大规模网络攻击对当前网络造成的危害属于中度风险等级；当 $sa(path_i)\in[7.0,10]$ 时，多阶段大规模网络攻击对当前网络造成的危害属于高风险等级。

综上所述，在多阶段大规模网络攻击下的网络安全态势评估计算表达式如下：

$$SA=\sum_{i=1}^{n}sa(path_i) \tag{14}$$

其中，n 表示检测到的多阶段大规模网络攻击下所有攻击场景的总和。

3　实验结果分析

为了证明所提方法的可行性和优越性，搭建以下实验网络环境，如图 1 所示。网络实验环境中主要包括网络防火墙装置、交换机装置、网络入侵检测装置、Web 服务器装置、文件服务器装置、网络工作站和一台攻击主机。

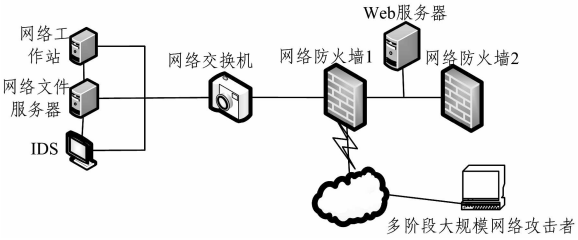

图 1　实验环境的网络拓扑结构图

Fig. 1　Network topology of experimental environment

图 1 中，网络 IDS 安装了 SNORT 的网络入侵检测系统装置，网络 Web 服务器与网络工作站均安装 Windows 操作系统，网络文件服务器的操作系统是 Linux。在攻击者实施多阶段大规模网络攻击时，当前网络中运行 IDS 和网络防火墙装置产生的报警数据以及网络中每一台主机拥有的网络安全时间可以用于检测审核日志。

攻击者对当前网络实行了一次多阶段大规模的网络木马攻击后，网络攻击者再对当前网络实行攻击时，首先扫描并找寻有效的网络主机：当攻击者发现网络有效主机的 Web 服务器装置时，通过 Apache Web Server 分块编码远程溢出的主机漏洞信息对其实施攻击，获得当前网络的访问权限；然后，攻击者利用当前网络文件服务器装置上的设置问题，采用 NFS Shell 等程序，通过 NFS 协议修改当前网络文件服务器装置上的重要文件信息，在网络上寻找由被攻击网络工作站安装的可执行二进制代码，同时在其中安装一个木马运行程序；最后，网络攻击者通过当前网络的工作站将攻击木马激活，获得网络工作站的控制权。结合多阶段大规模网络攻击的安全检测警报信息和网络安全时间审核日志，采用本文所提方法对当前网络中的各个节点依次进行当前网络评估模型的建立、当前网络安全态势量化分析、当前网络安全态势评估，从而能够计算并求得当前网络的安全态势值。以当前网络主机的 Web 服务器为例，在网络检测到该网络主机受到网络攻击时，计算得到攻击发生的概率为 $m(a)=0.924$；在检测该网络主机受到多阶段大规模网络攻击之前，攻击发生的概率为 $m(b)=0.906$，这两个攻击同属于多阶段大规模网络攻击的 Attack Model A1，这两个攻击之间的关联度 $cor(a,b)=1$，由此可得当前网络攻击值处于多阶段大规模网络攻击的 Attack Model A1 模式的第二阶段，该阶段的网络攻击支持概率计算表达式如下：

$$\begin{aligned}s(A1\_state2)&=m(a)m(b)cor(a,b)\\&=0.924\times 0.906\times 1=0.837\end{aligned} \tag{15}$$

利用式(15)的计算结果，结合多阶段大规模网络攻击阶段的攻击威胁 $t(A1\_state2)=0.42$，得到该攻击对当前网络 Web 服务器节点的安全态势影响为：

$$e=s(A1\_state2)t(A2\_state2)=0.837\times 0.42=0.352 \tag{16}$$

此时只检测到该网络攻击，由此可知当前网络的 Web 服务器的安全态势只受到该攻击的影响，则此时的网络安全态势值 $SA=e=0.352$。最后结合当前网络中各个节点的权重值，计算在网络攻击下当前整个网络的安全态势值。当前网络各个节点的权重值计算结果主要取决于各节点的重要程度。假设当前网络的 Web 服务器、文件服务器和工作站的权重值分别为 0.2，0.3 和 0.5，则多阶段大规模网络攻击下的网络安全态势值如表 1 所列。

表 1　多阶段大规模网络攻击下的网络安全态势值

Table 1　Network security situation values under multi-stage large-scale network attack

攻击阶段	攻击实时概率/%	Web 服务器	当前网络文件服务器	网络工作站	SA/U
A1_state1	0.912	0.039	0	0	0.0071
A1_state2	0.914	0.350	0	0	0.0721
A1_state3	0.886	0	0.372	0	0.1203
A1_state4	0.872	0	0.449	0	0.1288
A1_state5	0.867	0	0	0.446	0.2310

根据表 1 的计算结果绘制成图，如图 2 所示。其中横坐标表示当前网络的运行时间，纵坐标表示当前网络的安全态势值。网络安全态势值越大，说明当前网络中受到的多阶段大规模网络攻击的破坏性越严重。

由图 2 可知，多阶段大规模网络攻击对权重越大的主机进行攻击时，其对整体网络安全态势的影响程度就越严重，且随着攻击实施的不断深入，攻击者逐渐实现攻击的最终目的；同时，当前网络的安全态势值也逐渐变大，基本符合多阶段大规模网络攻击的真实情况。相较于文献[9]的方法，只考虑单个网络攻击对当前网络的影响和破坏未能全面考虑网络攻击的因果关系，从其对网络安全态势值进行计算的结果中可以看出，*A1_state4* 受到网络木马攻击时的安全态势值远远高于后续网络攻击实施阶段的值。采用所提方法计算的结果随着网络攻击阶段实施的不断深入而不断增加，由此证明所提方法比其他两种对比方法更具合理性。文献[10]中的方法的缺点是只有在当前网络已经出现并实施网络攻击时，才能计算出当前网络的安全态势值，并且其取值仅仅只有几个零散的点；而本文所提方法将多阶段大规模网络攻击阶段作为评估当前网络安全态势的要素，其取值具有连续性，这证明利用本

文方法绘制的多阶段大规模网络攻击下的网络安全态势评估图更具有实用价值和参考价值。

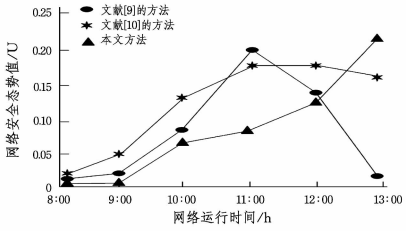

图 2 3 种不同方法的网络安全态势值对比结果

Fig. 2 Comparison results of network security situation values of three methods

采用所提的网络安全态势评估方法对当前网络安全态势的发展进行预测，对网络中的各个节点根据网络攻击阶段状态转移图进行状态转移概率评估来对网络下一时刻的安全态势进行相应的预测。采用网络的 Web 服务器装置举例说明，当网络入侵检测系统检测到当前网络主机受到攻击时，经过量化分析识别出攻击者正按照 A1 攻击模式实行攻击策略，然后通过对网络主机配置信息的漏洞进行扫描，发现其包括 Apache Web Server 分块编码远程的溢出的漏洞配置信息，计算当前网络状态是否满足式(10)－式(12)中的条件，如果满足，则说明该网络主机当前只受到该阶段的攻击，对当前网络的下一时刻安全态势进行预测分析，其表达式为：

$$SA = s(A1\_statel)ns(h)t(A1\_state2)$$
$$= 0.906 \times 1 \times 0.42 = 0.381 \quad (17)$$

其中，根据式(17)的计算结果，结合网络各个节点的权重值，得到网络安全态势的相应预测结果，如图 3 所示。

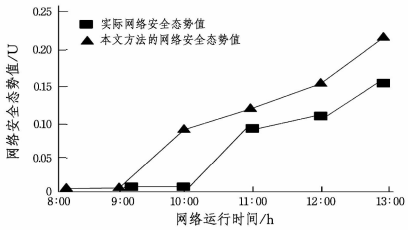

图 3 当前网络安全态势的预测分析图

Fig. 3 Forecast analysis chart of the current network security situation

由图 3 可知，所提方法能够较为准确地预测出受到多阶段大规模网络攻击时下一时刻网络攻击者的进一步攻击行为，并且能够对当前网络的安全态势值的未来变化趋势作出预判，有利于管理员对当前网络中出现的不同类型的网络安全事件及时作出相应防护和补救措施。所提方法能够通过多阶段大规模网络攻击阶段的转移较好地预测网络安全态势的发展趋势，具有较高的预测准确性。

结束语 采用当前方法对多阶段大规模网络攻击下的网络安全态势进行评估时存在评估结果偏差较大的问题，因此提出一种新的多阶段大规模网络攻击下的网络安全态势评估方法，并通过实例分析证明了所提方法的适用性和预测结果的正确性，该方法能够更加准确地预测出网络下一时刻的安全态势。

参 考 文 献

[1] ZHANG K. Big Data Network Intrusion Traces of Process Data Monitoring Method Research[J]. Science Technology and Engineering, 2016, 16(14): 254-258. (in Chinese)
张凯. 大数据网络入侵过程的痕迹数据监测方法研究[J]. 科学技术与工程, 2016, 16(14): 254-258.

[2] TIAN G W. Optimal Identification Algorithm for Virus Attack in Super Dense Network[J]. Bulletin of Science and Technology, 2016, 32(6): 145-148. (in Chinese)
田关伟. 超密集网络中病毒攻击优化识别算法[J]. 科技通报, 2016, 32(6): 145-148.

[3] ZHANG J L. Network Security Risk Dynamic Evaluation Method Research[J]. Computer Simulation, 2016, 33(10): 356-360. (in Chinese)
张俊林. 网络安全风险动态评估方法研究[J]. 计算机仿真, 2016, 33(10): 356-360.

[4] WANG G H. Research on Network Security Situation Awareness Based on Genetic Algorithm[J]. Computer Measurement & Control, 2016, 24(12): 155-157. (in Chinese)
王国华. 基于遗传算法的网络安全态势感知研究[J]. 计算机测量与控制, 2016, 24(12): 155-157.

[5] HUANG H J. Network security evaluation based on cloud computing[J]. Electronic Design Engineering, 2016, 24(12): 115-117. (in Chinese)
黄海军. 基于云计算的网络安全评估[J]. 电子设计工程, 2016, 24(12): 115-117.

[6] WANG X, LI Q M, QI Y. Real Time Analysis Method of Network Security Risk Based on Markov Model[J]. Computer Science, 2016, 43(S2): 338-341. (in Chinese)
王笑, 李千目, 戚湧. 一种基于马尔科夫模型的网络安全风险实时分析方法[J]. 计算机科学, 2016, 43(S2): 338-341.

[7] CHEN H, WANG F, XIAO Z J, et al. Network security situation assessment model fusing multi-source data[J]. Computer Engineering and Applications, 2015, 51(17): 96-101. (in Chinese)
陈虹, 王飞, 肖振久, 等. 一种融合多源数据的网络安全态势评估模型[J]. 计算机工程与应用, 2015, 51(17): 96-101.

[8] MA C G, WANG C H, ZHANG D H, et al. A Dynamic Network Risk Assessment Model Based on Attacker's Inclination[J]. Journal of Computer Research and Development, 2015, 52(9): 2056-2068. (in Chinese)
马春光, 汪诚弘, 张东红, 等. 一种基于攻击意愿分析的网络风险动态评估模型[J]. 计算机研究与发展, 2015, 52(9): 2056-2068.

[9] LI F W, ZHANG X Y, ZHU J, et al. Network security situational awareness model based on information fusion[J]. Journal of Computer Applications, 2015, 35(7): 1882-1887. (in Chinese)
李方伟, 张新跃, 朱江, 等. 基于信息融合的网络安全态势评估模型[J]. 计算机应用, 2015, 35(7): 1882-1887.

[10] WANG K, QIU H, YANG H P. Network security situation evaluation method based on attack pattern recognition[J]. Journal of Computer Applications, 2016, 36(1): 194-198. (in Chinese)
王坤, 邱辉, 杨豪璞. 基于攻击模式识别的网络安全态势评估方法[J]. 计算机应用, 2016, 36(1): 194-198.

[11] HUANG Z H, WU L L, ZHANG B. Network Security Threats and Prevention on Cloud Computing[J]. Journal of Chongqing University of Technology(Natural Science), 2012, 26(8): 85-90. (in Chinese)
黄志宏, 巫莉莉, 张波. 基于云计算的网络安全威胁及防范[J]. 重庆理工大学学报(自然科学), 2012, 26(8): 85-90.