

基于危险理论的网络安全风险评估

李京

(青岛大学信息工程学院, 山东 青岛 266071)

摘 要:网络风险评估可以为采取积极主动的防御手段提供依据。为了提高网络安全风险评估的可信性,借鉴免疫系统与网络安全防范的相似性,基于危险理论,利用云模型对引起系统危险的性能参数进行表示,提出了一种新的网络安全风险评估方法。给出了算法设计思想和具体实现过程。在危险感知器的构造过程中,采用了一种无需确定度的逆向云生成算法。实验结果表明,本算法由于危险信号的引入,排除了一些对网络无危险的攻击,更能正确评估网络的安全风险,并且有效保留了风险评估过程中的不确定性,评估结果更加科学。

关键词:人工免疫;危险理论;网络安全;风险评估

中图分类号:TP18;TP393

文献标识码:A

文章编号:1673-629X(2012)08-0159-04

Evaluation Model for Network Security Risk Based on Danger Theory

LI Jing

(Department of Information Engineering, Qingdao University, Qingdao 266071, China)

Abstract: The evaluation of network risk provides a reliable basis for active network defense. In order to improve the trusty of network risk, a danger-theory based evaluation model for network risk was proposed, and cloud model was used to represent danger signal. The design ideas and implementation steps were given. An improved backward cloud algorithm with unknown certainty was used to generate danger perception. The experimental results prove that some attacks were eliminated because of the danger signal, so the proposed method can evaluate the network risk correctly and retain the maximum uncertainty of network assessment more reasonable.

Key words: artificial immunity; danger theory; network security; risk evaluation

0 引言

随着计算机网络在生活中的广泛应用,网络所面临的安全问题也日益突出。从网络防范的角度看,无论何种安全防范措施均无法保证网络的绝对安全。因此,对网络所面临的安全风险进行有效评估,发现所处的危险级别,进而采取相应的主动防御措施,是提高网络安全性的有效手段。

目前,网络风险评估模型可以分为两大类:静态评估方法和动态评估方法^[1-6]。静态评估方法如CRAMM, COBRA, OCTAVE等^[1],这些方法无法实现实时的网络风险评估,缺少自适应性;动态评估方法,如文献[2~6]分别使用概率统计法、层次分析法、模糊集理论等方法进行网络风险动态评估,提高了评估结果的可信性;文献[7]提出了建立在传统的自体与

非自体(SNS)基础上的免疫实时网络风险评估方法,但检测结果虚警率较高;文献[8]提出了一种基于免疫危险理论的网络安全风险评估方法,但危险信号的定义和定量计算不够明确。基于此,文中在SNS识别理论的基础上,引入云模型对网络安全风险评估过程中的危险信号进行描述和定义,提出了一种基于危险理论和云模型的网络安全风险评估模型,减少了虚警率和漏警率,提高了风险评估的准确性。

1 设计思想

人工免疫系统的自体/非自体理论(Self-Noself, SNS)认为:人体免疫系统通过对自身的抗原(自体)的耐受(不产生免疫应答),和对外来的抗原(非自体)产生免疫应答并进行清除,以维护人体免疫系统的稳定性^[7]。SNS理论存在着自体集合过大,自体和非自体难以区分等缺陷。事实上,经实践证明,只有少数非自体抗原可能对人体是有害的^[7,8]。免疫危险理论^[8]认为,应答只对有害的非自体抗原进行,而不是对任何非自体都进行应答,因此无需大量的训练时间,从而可

收稿日期:2011-12-30;修回日期:2012-04-02

基金项目:山东省自然科学基金资助项目(ZR2009GQ008);山东省教育科技项目(J08LJ02)

作者简介:李京(1971-),女,四川攀枝花人,讲师,硕士,主要研究方向为云计算、网络安全、电子商务。

以大大减少免疫应答的规模和次数。此外,对于之前被认定为自体,但是随着时间的推移,有可能对机体产生危害的抗原,危险理论也会进行应答,从而减少了漏报率;同时它不会属于非己,但无害的抗原应答,减少了误报率。因此,基于危险理论的网络风险评估,可以排除一些对网络而言无需关注的信息,进而大大减小了应答的规模,因而,更具有应用可行性。

然而,基于危险理论的网络风险评估中,危险信号如何定义是一个非常重要的问题。危险性的大小是一个模糊问题,如危险性高,危险性低。文中认为,危险是由变化引起的,由变化感知危险。系统指标(参数)变化如果在正常范围内,则是安全的,只有超过正常范围的参数变化才认为是有害的。系统处于危险状态,则认为系统存在网络安全风险。因此,可以通过监视主机系统参数的变化来进行危险感知。但问题在于什么样的变化程度才是“危险”,是一个不确定和模糊问题。当计算机受到入侵时,系统的参数会发生变化。

由此可见,危险程度是个定性概念,而引起危险的系统参数变化是定量值。云模型把模糊性和随机性以及二者之间的关联性有效结合在一切,是一种定性和定量表示之间的不确定性转换工具^[9,10]。因此,文中在 SNS 识别理论的基础上,引入云模型对危险信号进行描述和定义,进而对网络的安全风险程度进行衡量。

2 算法实现的关键技术和过程

2.1 云模型的基本概念

云模型是一种定性定量之间的转换模型,由李德毅院士提出,它能够实现某个用语言值表示的定性概念与其用数值表示的定量概念之间的不确定转换。云模型主要反映知识表示的模糊性和随机性以及二者之间的关联性。云模型由许许多多的云滴组成,用三个特征向量:期望值 Ex 、熵 En 、超熵 He 来表示,记作 $C(Ex, En, He)$ 。它们反映了定性知识的定量特性。期望 Ex 反映了定性知识的信息中心值,熵 En 反映了定性概念随机性的度量。超熵 He 是熵 En 的熵,反映了云的厚度,即云的离散程度。 He 越小,说明随机性越小。

云模型中通过正向云发生器把定性概念变换为定量数值表示,也就是由云的数字特征产生云滴。而通过逆向云发生器完成从定量值到定性概念的转换,即将一组定量数据转换为以数字特征 (Ex, En, He) 来表示的定性概念,即由云滴群得到云的数字特征的过程^[11]。

2.2 文中危险的表示和描述

当主机遭受到攻击时,其主要性能指标(如 CPU

占用率、内存占用率)必然会发生变化,同时,这些性能指标变化的幅度决定了网络安全风险的大小。此外,网络入侵的发生具有很大的随机性,而对网络风险的评估多采用自然语言来描述,从而导致风险评估结果又具有一定的模糊性。同时,在遭受到入侵的时候,各参数之间的变化是相互关联的(比如, CPU 占用率的提高往往跟内存占用率有关系)。总之,网络安全风险程度是一个定性概念,而引起网络安全风险变化的各个性能指标参数值是定量的。因此,必须实现定量定性之间的转换,以及考虑模糊性和随机性的关联,才能更准确地评估网络安全风险。云模型构成定性和定量相互间的转换,并把模糊性和随机性及二者的关联性进行了有效集成,是进行网络风险评估的有效工具。

在网络系统中,通过监视系统变量的变化可以进行危险感知。可以作为危险信号的指标有:内存占用率过高、CPU 占用率过高等。文中采用云模型来描述系统变量的危险变化。具体做法如下:在系统正常状态下,通过逆向云生成算法得到系统正常状态云及其数字特征;然后对系统进行监视,采样系统变量,计算其隶属度。若此时的系统变量采样值隶属于正常状态云,则认为没有危险产生,网络是安全的;反之,则认为有危险信号产生,同时根据指标变量偏离程度,得出危险等级。

如果只采样一个系统指标,则无法准确衡量系统的危险程度,所以,需要综合多个指标。但不同的指标变化在网络安全风险中占用的权重不尽相同,因此,文中作如下定义:

$$\text{danger} = (s, w, \theta)$$

其中 $S = (C, M, F \dots)$ 代表被监视的系统变量集合, C 代表 CPU 占用率, M 代表内存占用率, F 代表流量参数。 $w = (w_1, w_2, \dots, w_i) (0 < w_i < 1)$ 代表每一种危险变量所占的判别权重; θ 是危险的阈值,当超过阈值后,则认为系统有危险发生。

2.3 网络风险评估模型

文中模型建立在传统的 SNS 识别的基础上,同时引入基于云模型表示的危险信号。只有当“危险”与 nonself 同时出现时,才进行响应。

文中评估模型如图 1 所示:

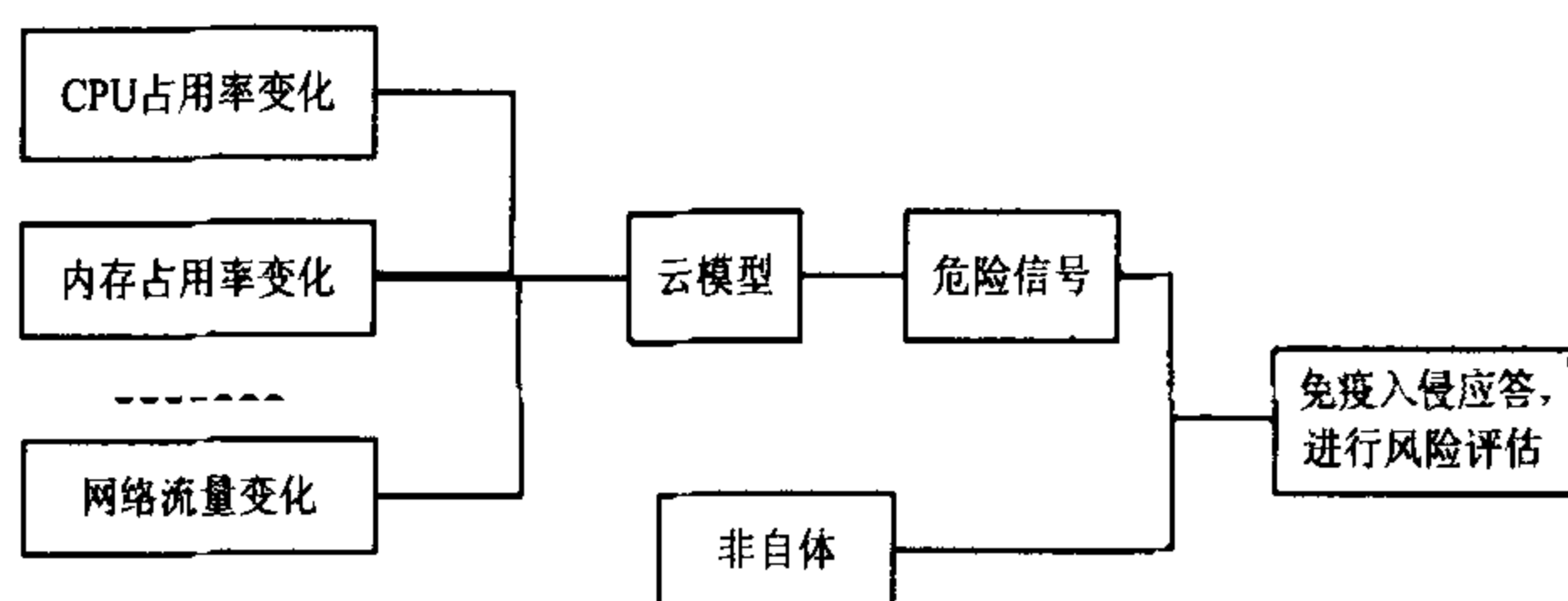


图 1 文中网络风险评估模型

3 网络风险评估的具体实现

3.1 生物免疫与入侵的关系

基于免疫的入侵检测中,生物体可以比喻为整个网络,生物免疫的淋巴细胞类比为网络中的各个主机,免疫系统中的抗原类比为入侵检测中的网络行为。其中,自体抗原映射为正常网络行为、非自体抗原映射为非法网络行为。生物免疫系统中抗体识别抗原的过程,就被类比为检测器检测网络行为是否正常的过程。在风险评估中,用检测器模拟免疫细胞,也就是用检测器检测网络信息流。抗原用来映射所有的网络数据包,抗体用来映射检测器。当一个数据包经过网络,检测器开始工作。当抗体与抗原匹配,表示检测到了异常。

3.2 抗原和抗体的形式化描述

定义抗原集合 $Ag \subset D, D = \{0,1\}^l (l > 0)$, 其中表示对网络信息流包进行特征提取得到的长度为二进制串。

定义自体集合 $Self \subset Ag$, 非自体集合 $Nonself \subset Ag$, 则有 $Self \cup Nonself = Ag, Self \cap Nonself = \emptyset$ 。Self 集为正常网络行为, Nonself 集为网络攻击行为。

3.3 抗原与抗体的匹配过程

抗原与抗体的匹配过程采用 f_{match} 函数定义如公式(1)所示, 1 表示匹配, 0 表示不匹配。文中采用可变阈值模糊 r 匹配算法^[12]。算法通过自适应调整匹配阈值, 大大降低了黑洞数量, 提高了检测率。

$$f_{match}(x, y) = \begin{cases} 1, & \text{if } \exists i, j (x.d_i = y_i, x.d_{i+1} = y_{i+1}, \dots, \\ & x.d_j = y_j, j - i \geq r, \\ & 0 < i < j \leq l, i, j, r \in N) \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

根据否定选择原理和自体耐受过程, 检测器在经过自体耐受后, 成为成熟抗体, 执行检测任务。当检测到非自体抗原后, 抗体进行克隆选择, 生成的新抗体进一步通过否定选择和克隆选择, 得到成熟的抗体检测体集合。

3.4 危险感知器的构造

在网络正常运行状态下, 选取时间间隔 T , 对系统参数进行连续采样, 将样本点的各维(即各系统参数)规格化到 $[0,1]$ 之间(这里尽可能多的进行采样, 以便结果更加准确)。经过采样, 样本点就构成一个云。由于网络安全风险评估中, 只能得到一组采样数据值, 同时, 确定性很难获得, 所以, 文中求云的数字特征时, 采用了一种改进的未知确定度的逆向云发生器算法(算法1), 然后采用正向云生成算法, 得到该正常概念云。与正常状态云偏离, 即表明有危险发生。

下面以内存数据为例介绍算法。其它系统参数的

计算类似。

算法1 逆向云发生器算法。

输入: 样本点 M_i , 其中 $i=1,2,3,\dots,n$; M_i 指的是内存在不同的时间, 采样得到的 n 个数据。

输出: 内存占用率的数字特征 (Ex, En, He) 。

算法步骤:

1) 根据 M_i 计算其样本均值 $\bar{M} = \frac{1}{n} \sum_{i=1}^n M_i$, 样本方

$$差 s^2 = \frac{1}{n-1} \sum_{i=1}^n (M_i - \bar{M})^2;$$

2) $\widetilde{Ex} = \bar{M}$;

3) $\widetilde{En} = (\bar{M}^2 - \frac{s^2}{2})^{\frac{1}{4}};$

4) $\widetilde{He} = (\bar{M} - (\bar{M}^2 - \frac{s^2}{2})^{\frac{1}{2}})^{\frac{1}{2}};$

5) 输出 $(\widetilde{Ex}, \widetilde{En}, \widetilde{He})$ 作为 (Ex, En, He) 的估计值。

4 系统仿真实验与分析

实验在网络实验室进行了仿真实验, 利用文中算法对网络实验室的 20 台主机进行采样监控并评估, 操作系统为 Windows2003。入侵实验使用的数据是 kdd-cup.data-10-per-centKDDCup99 数据集^[13]。系统参数如下: 可变阈值范围从 13 到 20, $=128$, $T=30$ 秒, $n=1000$ 。实验结果表明, 本系统平均检测率可以达到 97.5%, 虚警率平均可以降低到 3.2%, 检测性能表现良好。

本模型与 insre 模型^[14] 对风险的检测结果如图 2 所示。左边横坐标表示网络风险, 右边横坐标表示攻击强度。图 2 是网络面临的实际攻击强度与风险评估模型所分析结果的对比结果。

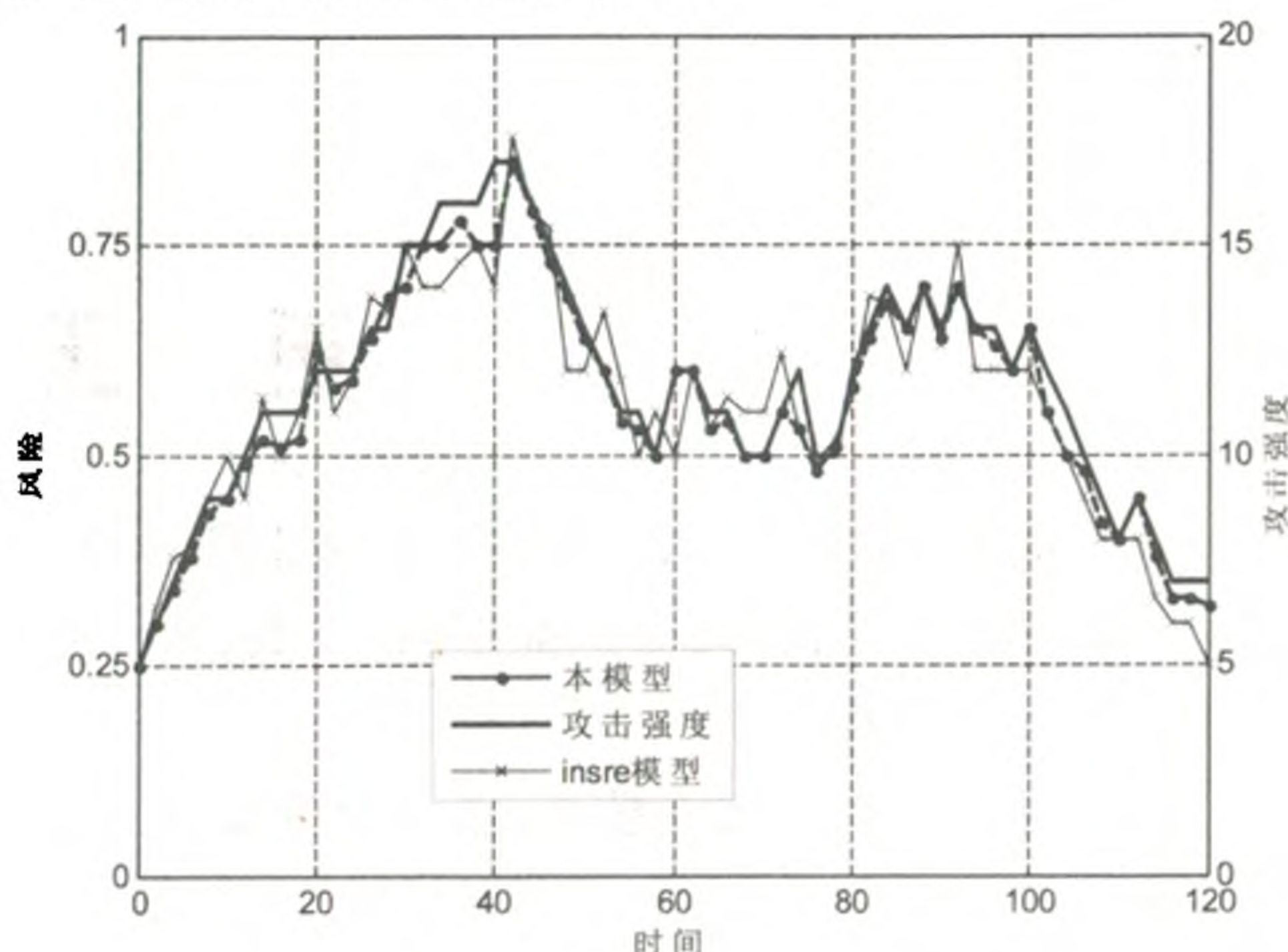


图2 网络遭受攻击时的风险图

从图中也可以看出, 本模型更能真实反映网络面临的安全风险。与传统基于免疫的网络安全风险检测

方法相比^[12],由于危险信号的引入,排除了一些对网络无危险的攻击,更能精确检测判断网络遭受攻击的风险。

对网络安全风险的评估结果如表 1 所示。

表 1 网络安全风险评估结果

性能参数平均采样值		云特征	网络风险
Cpu 占用率	内存占用率	(<i>Ex</i> , <i>En</i> , <i>He</i>)	评估结果
2.1%	5.1%	(3,2.1,0.7)	低
8.0%	13.4%	(10,3.7,1.2)	较低
42.8%	35.1%	(38,4.0,1.3)	较高
50.1%	56.6%	(50,2.0,0.3)	高

从表 1 可以看出,本方法可以给出正确的网络安全风险评估结果。同时,从云的数字特征 (*Ex*,*En*,*He*) 可以看出,网络风险较低、较高状态下,熵 *En* 和超熵 *He* 都相对较大。熵 *En* 较大说明此定性概念随机性较大,网络处于此状态的范围较大。超熵 *He* 较大,说明评估结果的不确定性较大。这恰好与现实生活一致:对网络处于安全/不安全状态的认识,不同人评估结果差异较小;而网络处于较安全/较不安全状态时,不同人评估结果差异性较大,也就是说,不同的人对到底什么是较安全/较不安全,认定差异的可能性较大,而对什么是安全/不安全认定的差异较小。因此,基于危险理论和云模型的网络风险评估不仅给出了正确的评估结果,而且保留了评估过程中的不确定性,结果更加科学。

5 结束语

文中借鉴免疫危险理论,提出了一种基于免疫危险理论和云模型的网络安全风险评估方法,实验结果表明了其可以更准确地进行网络风险评估。如何进一步优化选择代表系统性能指标的参数,是下一步继续

研究的方向。

参考文献:

[1] Visintine V. An Introduction to Information Risk Assessment [J]. SANS Institute Journal,2006,8(5):101-118.

[2] 李焕洲,王祯学,陈 麟. 信息系统安全风险的概率描述及基本特征[J]. 四川大学学报(自然科学版),2008,32(4):87-90.

[3] 陈秀真,郑庆华,管晓宏,等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报,2009,17(4):885-897.

[4] 柴争义,刘 芳,朱思峰. 新型智能入侵防御模型[J]. 华中科技大学学报,2010,38(1):22-24.

[5] 张永铮,方滨兴,迟 悦. 用于评估网络信息系统的风险传播模型[J]. 软件学报,2009,18(1):137-145.

[6] 赵冬梅,马建峰,王跃生. 信息系统的模糊风险评估模型[J]. 通信学报,2008,28(4):51-56.

[7] 韦 勇,连一峰. 基于日志审计与性能修正算法的网络安全态势评估模型[J]. 计算机学报,2009,32(4):763-772.

[8] 柴争义,郑丽萍,朱思峰. 基于免疫抗体浓度的网络入侵风险定量评估[J]. 高技术通讯,2010(10):1027-1032.

[9] Li Tao. An immunity based network security risk estimation [J]. Science in China Ser F Information Sciences,2010,48(5):557-578.

[10] Li Deyi, Liu Changyu, Gan Wenyan. A New Cognitive Model: Cloud Model[J]. International journal of intelligent systems, 2009,24(4):357-375.

[11] 张红斌,裴庆祺,马建峰. 内部威胁云模型感知算法[J]. 计算机学报,2009,32(6):784-791.

[12] 柴争义,刘 芳. 应用危险理论的网络安全风险感知模型[J]. 北京邮电大学学报,2010,33(3):40-43.

[13] University of California. KDDLib[EB/OL]. [2011-03-02]. <http://kdd.ics.uci.edu/databases/kddcup99.html>.

[14] 彭凌西,陈月峰. 基于危险理论的网络风险评估模型[J]. 电子科技大学学报,2010,36(6):1998-2001.

更正启事

本刊 2012 年第 22 卷第 6 期第 207-209 页的论文《阵列电机的 ARM 测控与显示系统实现》的第 4 作者遗漏,特此更正如下:施 威,原 亮,解双建,谢方方(军械工程学院计算机工程系 河北石家庄 050003)。

对以上失误深表歉意,在此向论文作者及其单位致歉,由此给作者及读者带来的不便敬请谅解。

《计算机技术与发展》编辑部

一种基于复数域的数据融合完整性保护算法

作者:
作者单位:
刊名:
英文刊名:
年, 卷(期):

[赵丹, 杨庚](#)
[南京邮电大学计算机学院, 江苏南京210003](#)
[计算机技术与发展](#)
[Computer Technology and Development](#)
[2012 \(8\)](#)



参考文献(14条)

- 1.Visintine V An Introduction to Information Risk Assessment 2006(05)
- 2.李焕洲;王树学;陈麟 信息系统安全风险的概率描述及基本特征 2008(04)
- 3.陈秀真;郑庆华;曾晓宏 层次化网络安全威胁态势量化评估方法 2009(04)
- 4.蔡争义;刘芳;朱思峰 新型智能入侵防御模型[期刊论文]•华中科技大学学报 2010(01)
- 5.张永铮;方滨兴;迟悦 用于评估网络信息系统的风险传播模型 2009(01)
- 6.赵冬梅;马建峰;王跃生 信息系统的模糊风险评估模型 2008(04)
- 7.韦勇;连一峰 基于日志审计与性能修正算法的网络安全态势评估模型[期刊论文]•计算机学报 2009(04)
- 8.蔡争义;郑丽萍;朱思峰 基于免疫抗体浓度的网络入侵风险定量评估[期刊论文]•高技术通讯 2010(10)
- 9.Li Tao An immunity based network security risk estimation 2010(05)
- 10.Li Deyi;Liu Changyu;Gan Wenran A New Cognitive Model:Cloud Model 2009(04)
- 11.张红斌;袁庆祺;马建峰 内部威胁云模型感知算法 2009(06)
- 12.蔡争义;刘芳 应用危险理论的网络安全风险感知模型[期刊论文]•北京邮电大学学报 2010(03)
- 13.University of California KDDlib 2011
- 14.彭斌西;陈月峰 基于危险理论的网络风险评估模型 2010(06)

本文链接: http://d.g.wanfangdata.com.cn/Periodical_wjfx201208041.aspx