一种基于云模型主机安全评估方法

李金武

(郑州科技学院信息工程学院，河南郑州 450064)

摘 要: 本文提出了一种基于云模型的主机安全评估方法，该方法全面考虑了影响主机安全的连续型及离散型因素，设计了一套完整的指标因素集，并把离散参数加入云的不确定推理器，从而改进了单纯依靠连续型参数进行评估的推理算法. 改进的算法可以实现云的不确定性评估，能解决评估知识表达的不确定性，从而实现定性概念与定量数据之间的不确定性转换，进而为用户提供可靠的决策信息，并通过实验仿真验证了该方法的可行性.

关键词: 云模型; 主机安全; 指标因素

中图分类号: TP393 文献标识码: A 文章编号: 1009 - 4970(2017) 02 - 0059 - 05

DOI:10.16594/j.cnki.41-1302/g4.2017.02.015

随着计算机大范围的普及，个人计算机作为用户接触最多的终端设备，它的安全性直接影响用户的体验，所以对其安全性的研究必不可少. 对于个人计算机的安全性，可使用层次分析法、模糊层次分析法、专家打分法等直接给出定量的评估值[1-5]. 这些方法较多的依赖评估专家知识库，会造成不同的方法对同一台主机的评估会产生不同的评估量值，并且不能够解决评估中的不确定性问题. 虽然通过云模型可实现定量与定性的转换问题，并能解决评估的不确定性问题，但是大部分云评估模型只考虑影响主机的连续性能指标[6-8]，忽略了离散参数值对主机的影响，从而造成评估的偏差. 笔者综合考虑各方面安全性能指标，提出一种基于云模型的不确定性评估方法，经实验验证明，这是一种非常有效的计算机安全评估方法.

1 理论基础

1.1 云模型概念

设 U 是一个用精确数值表示的定量论域，X 为主机安全评估的评估模块，则 $X \subseteq U$(一维、二维或多维)，T 是评估结果的定性表述. 对于 $\forall x(x \in X)$，都有一个映射关系 $y = C_T(x)$ ，$y \in [0,1]$，叫做 x 对 T 的隶属度，则评估结果 T 从论域 U 到区间 $[0,1]$ 的映射在数据区间上的分布，称为云模型[9-10].

用 $Cloud(Ex,En,He)$ 表示一维云，使用三个数字特征刻画了自然语言概念之间模糊性与随机性的关联度. 期望 Ex 是最能表示评估模块定性概念的点; 熵 En 能反映评估模块定性概念所能接受的元素的取值范围; 超熵 He 可揭示评估模块定性概念里元素点的离散程度.

1.2 云发生器

云发生器即云的生成算法，正向云发生器由定性概念到定量数据进行转换，产生的具体过程如图 1(a) 所示[9-12]. 正向云发生器的生成算法步骤如下:

步骤 1: 产生一个期望值为 En，标准差为 He 的正态随机数 En';

步骤 2: 产生一个期望值为 Ex，标准差为 $|En'|$ 的正态随机数 x;

步骤 3: 计算 $y = e^{\frac{-(x-Ex)^2}{2(En)^2}}$;

步骤 4: (x,y) 反映了本次评估模块定性定量转换的全部内容，(x,y) 为评估云滴;

步骤 5: 重复步骤 1 ~ 4，产生 N 个云滴，算法结束.

逆向云发生器由定量数据到定性概念进行转换，即给出一组评估数据 $T\{ x1,x2,x3,\ldots,xi\}$，$i =$

收稿日期: 2016 - 09 - 18

基金项目: 国家自然科学基金地区项目(61462064) ; 郑州市科技局自然科学基金项目(20140616)

作者简介: 李金武(1984—) ，男，河南荥阳人，硕士，讲师. 研究方向: 网络安全及物联网通信技术.

1,2,...,N，计算评估模块定性概念的数字特征值 $Cloud(Ex,En,He)$ [9-12]，其产生过程如图 1(b) 所示. 逆向云发生器的生成算法步骤如下:

步骤 1: $E_x=\bar{x}=\frac{1}{N}\sum_{i=1}^{N}x_i$，$B=\frac{1}{N}\sum_{i=1}^{N}|x_i-\bar{x}|$，$S^2=\frac{1}{N-1}\sum_{i=1}^{N}(x_i-\bar{x})^2$;

步骤 2: $E_x=\bar{x}$;

步骤 3: $E_n=\left(\frac{\pi}{2}\right)^{\frac{1}{2}}\times B$;

步骤 4: $H_e=(S^2-E_n^2)^{\frac{1}{2}}$.

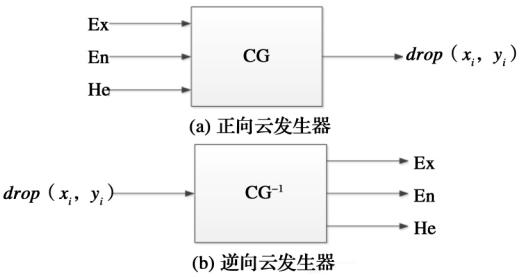

图 1　云发生器产生过程

1.3　云规则发生器

云规则发生器包括规则前件和规则后件，前件云是以评估分值中的特定点为条件，通过云发生器得出的属于评估模块定性概念的隶属度，又称 X 条件云 [9-12]，其产生过程如图 2(a) 所示. 规则前件云的生成步骤如下:

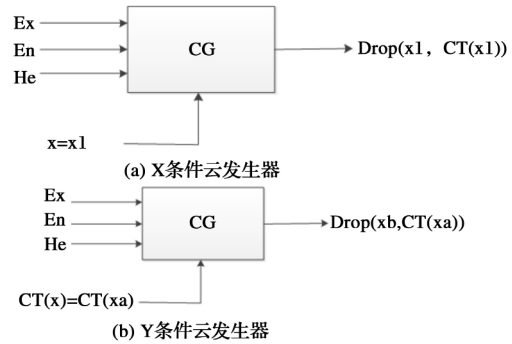

图 2　云规则发生器产生过程

步骤 1: 产生一个期望值为 En，标准差为 He 的正态随机数 En';

步骤 2: 计算 $C_T(x)=e^{\frac{-(x_0-E_x)^2}{2(E'_n)^2}}$;

步骤 3: 重复步骤 1 ~ 步骤 2，产生 N 个云滴，即 $Drop\{(x_0,C_T(x1)),(x_0,C_T(x2)),...,(x_0,C_T(xi))\}$，$i=1,2,...,N$，算法结束.

后件云是以某一隶属度为条件，通过云发生器生成属于这一隶属度的云滴的分布，又称 Y 条件云 [9-12]，其产生过程如图 2(b) 所示. 规则后件云的生成步骤如下:

步骤 1: 产生一个期望值为 En，标准差为 He 的正态随机数 En';

步骤 2: 计算 $x=E_x\pm E'_n\sqrt{-2\ln C_T(x_0)}$;

步骤 3: 重复步骤 1 ~ 步骤 2，产生 N 个云滴，即 $Drop\{(x1,C_T(x_0)),(x2,C_T(x_0)),...,(xi,C_T(x_0))\}$，$i=1,2,...,N$，算法结束.

2　主机安全评估模型

2.1　模型设计思想

影响主机安全的因素可分为两类: 动态连续参数和静态离散参数. 对于动态因素，当主机遭受攻击时，该参数的性能指标会发生变化，它的变化幅度直接影响该主机的安全程度; 对于静态因素，从主机系统所处的环境状态考虑，主机系统环境的好坏直接影响该主机的安全程度. 模型的基本任务是,根据系统参数状态值，借助设计的云发生器，判断系统的安全状况，以此评估主机的未来态势，主机安全评估模型如图 3 所示.

实现主机安全评估的方法如下:

(1) 确定影响主机安全的参数(动态参数和静态参数);

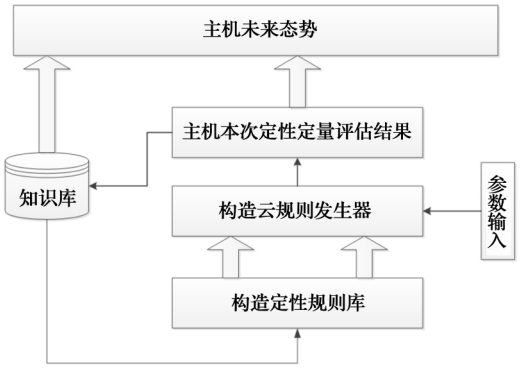

图 3　主机安全评估模型

(2) 定义系统状态集(正常、较正常、较不正常、不正常)为四个状态云，安全程度{安全、较安全、较危险、危险};

(3) 构造云标尺和云规则发生器;

(4) 定量输入处理，根据定量输入处理算法，对某时刻的输入计算激活强度，确定其在云标尺上的位置，并利用逆向云发生器计算数字特征，产生云滴，从而进行评估.

2.2　系统主要性能指标

定义系统性能指标 $S=Sc+Sd$(“+”表示取并

集). 其中 Sc 为动态连续参数，$Sc=\{C,M,B,D,...\}$，C 代表 CPU 利用率，M 代表内存利用率，B 代表网络带宽利用率，D 代表磁盘活动情况等; Sd 为静态离散参数，$Sd=\{\mathrm{Pr},Pa,L,V,...\}$，Pr 代表异常活动进程个数，$Pa$ 代表发送和接收的数据报文个数，L 代表网络连接个数，V 代表主机脆弱性个数等.

通过某一个指标的异常变化很难评估主机的安全性，因此本文从动态和静态的多个性能指标的异常变化综合考虑主机的安全性. 对连续参数，可以采集某个时间范围内的多个属性值，并利用逆向云做出定性评价，进而匹配规则库. 对于离散参数，若参数值发生变化，则用变化匹配规则库.

2.3 云标尺及规则库建立

因为不同的系统性能指标表达的概念不一样，所以本文不划分概念名称，只划分概念个数. 笔者针对各系统，将性能指标划分为 3 个概念，比如: 将 CPU 利用率划分为“高、中、低”三个概念. 系统性能指标的云模型的数字特征可以结合知识库，并通过公式计算得出. CPU 利用率和内存利用率二维云标尺示意图如图 4 所示; 同时把主机的安全级别划分为安全、基本安全、不太安全和不安全四个等级，根据“3En”规则计算得出安全级别的云模型数字特征. 主机安全云标尺示意图如图 5 所示. 表 1 给出了部分系统性能指标和主机安全概念云的数字特征值. 结合专家知识库和以往研究数据，本文优先考虑 CPU 和内存对主机的影响，定义如下的语言规则:

规则 1: 如果 CPU 利用率高，内存利用率高，则主机不安全;

规则 2: 如果 CPU 利用率高，内存利用率中，则主机不安全;

规则 3: 如果 CPU 利用率高，内存利用率低，则主机不太安全;

规则 4: 如果 CPU 利用率中，内存利用率高，则主机不太安全;

规则 5: 如果 CPU 利用率中，内存利用率中，则主机不太安全;

规则 6: 如果 CPU 利用率中，内存利用率低，则主机基本安全;

规则 7: 如果 CPU 利用率低，内存利用率高，则主机不太安全;

规则 8: 如果 CPU 利用率低，内存利用率中，则主机基本安全;

规则 9: 如果 CPU 利用率低，内存利用率低，则主机安全.

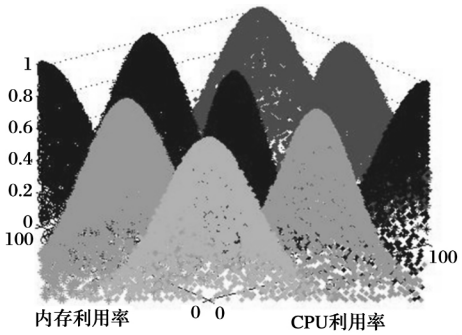

图 4 CPU 内存二维云模型规则示意图

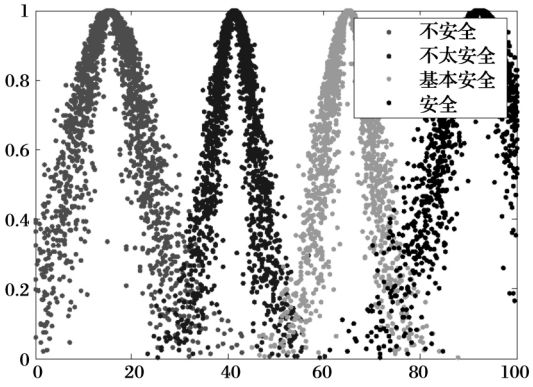

图 5 主机安全云标尺示意图

表 1 云模型数字特征值

特征值	CPU 利用率			内存利用率			宽带利用率			主机安全			
	高	中	低	高	中	低	高	中	低	安全	基本安全	不太安全	不安全
Ex	100	50	0	100	50	0	100	50	0	92.25	65.15	41.35	15.45
En	10/0.618	10	10/0.618	10/0.618	10	10/0.618	10/0.618	10	10/0.618	8.35	5.15	4.5	7.28
He	0.5/0.618	0.5	0.5/0.618	0.5/0.618	0.5	0.5/0.618	0.5/0.618	0.5	0.5/0.618	2.25	1.4	1.3	2.12

2.4 规则发生器设计

基于云模型的不确定性推理是根据已知的条件，利用云的不确定性推理器，在一定环境中推理出目标规则的过程. 基于云模型的不确定性推理分为单规则推理和多规则推理. 单规则推理可以形式化地描述为“IF A，THEN B”，“IF A1，A2，…，An，THEN B”，其中 A，B 是用云模型表示的自然语言值，例如“如果商品质量好，则价格高”，“如果某人饮食习惯好，睡眠质量高，则身体健康”. 显然，这些自然语言值不能够用精确的数值来表示.

多规则推理使用的是云的单条件多规则和多条件多规则的不确定性推理器. 在实际的推理中，大部分问题采用的多是云的多条件多规则推理.

2.5 定量输入处理过程

本模型采用多条件多规则推理. 在主机安全评估中，综合考虑了连续参数和离散参数. 对于连续参数，可以直接使用云规则发生器进行推理，并通过规则前件云得到所属概念的隶属度; 对于离散参数，因为其是确定的值，所以云规则发生器并不适用. 但可以稍加改进，使离散参数不经过规则前件，直接作为后件云的条件进行推理.

推理算法如下:

输入: 定量输入参数向量(X_{c1} , X_{c2} , … , X_{d1} , X_{d2}) ，采集时间周期 T，确定规则前件和规则后件;

输出: 定性和定量评估结果.

步骤 1: 将处于 t 时间点的各连续参数值 x_i(i = 1 ,2 ,3 , … , n) 代入相应的概念前件云，得到其所属几个概念的隶属度 μ_{ij}(i = 1 ,2 ,3 , … , n , j = 1 ,2 , … m) ;

步骤 2: 将某时间点的各连续参数值 x_i(i = 1 ,2 , 3 , … , n) ，根据 $3E_n$ 规则判断它激活的规则集 $Rset_i$, $3E_n$ 规则($E_{x_i} - 3E_n < x_i < E_{x_i} + 3E_n$) ;

步骤 3: 计算各连续参数激活规则集的交集为 $Rset = Rset_1 \cap Rset_2 \cap \cdots \cap Rset_n$;

步骤 4: 用 $Rset$ 和各离散参数再次匹配规则库中的规则，激活新的规则集为 $Rsetf$;

步骤 5: 对于 $Rsetf$ 中的每条规则 R_k:

(1) 将激活 R_k 的多个参数对应的激活隶属度 μ_{ij} 求“软与”或“软或”运算，得到一个综合激活隶属度 Cmd_i;

(2) Cmd_i 作为 R_k 规则后件云的条件，得到一个或两个云滴 $Drop_i$，加入云滴集 $Drop$.

步骤 6: 将时间推移一个周期，即 $t = t + T$，重复步骤步骤 1 ~ 步骤 5.

步骤 7 : 根据步骤 5 产生的 $Drop$，由逆向云生成器算法得到本次评价 $Cloud$(E_x , E_n , H_e) ，从而得到其所属的云图.

3 实验结果及分析

对一台计算机采集多个时间点的 CPU 利用率和内存利用率数据，在 t 时间点采集的数据，记作(t , c , m) ，t 表示时间，c 表示 t 时间点 CPU 利用率，m 表示 t 时间点内存利用率. 对连续采集 n 个时间点的数据进行主机安全评估，其中部分时间点的数据如表 2 所示.

表 2 采集数据评估隶属度

采集数据	激活规则	综合隶属度	采集数据	激活规则	综合隶属度	采集数据	激活规则	综合隶属度
(t_1 ,7 ,37)	规则 5	0.00002	(t_5 ,10 ,38)	规则 5	0.00028	(t_9 ,6 ,38)	规则 5	0.000008
	规则 6	0.00001		规则 6	0.00003		规则 6	0.000003
	规则 8	0.40357		规则 8	0.41059		规则 8	0.47576
	规则 9	0.07885		规则 9	0.04134		规则 9	0.05148
(t_2 ,5 ,40)	规则 5	0.00005	(t_6 ,11 ,33)	规则 5	0.00025	(t_{10} ,9 ,34)	规则 5	0.00004
	规则 6	0.00008		规则 6	0.00008		规则 6	0.000008
	规则 8	0.54414		规则 8	0.16934		规则 8	0.21844
	规则 9	0.04278		规则 9	0.08100		规则 9	0.10024
(t_3 ,2 ,32)	规则 5	0.000004	(t_7 ,8 ,33)	规则 5	0.00007			
	规则 6	0.000003		规则 6	0.000008			
	规则 8	0.19413		规则 8	0.19516			
	规则 9	0.18834		规则 9	0.11648			
(t_4 ,5 ,36)	规则 5	0.00003	(t_8 ,14 ,35)	规则 5	0.00045			
	规则 6	0.000002		规则 6	0.00007			
	规则 8	0.36897		规则 8	0.18696			
	规则 9	0.07386		规则 9	0.07058			

(t_1 ,7 ,37) 表示 t_1 时刻的 CPU 利用率为 7% ，内存利用率为 37% . 依据推理算法，对于输入的 CPU 利用率参数 7，激活规则 4 ~ 规则 9 这六条规则; 对于输入的内存利用率参数 37，并激活规则 2，规则 3、规则 5、规则 6、规则 8 和规则 9 这六条规则. 综合考虑两个参数对主机安全的影响，

激活的规则集为{ 规则 5,规则 6,规则 8,规则 9}. 之后利用定量推理算法得出综合激活隶属度，把其作为对应主机安全评估云的输入，得到一个或两个云滴，并加入云滴集. 最终本次评估的云模型为 *Cloud*(65. 98,7. 02,5. 99)，即期望值为 65. 98，熵值为 7. 02，超熵值为 5. 99. 利用云的相似度评估算法可得出本次评估为基本安全[13]，评估结果如图 6 所示.

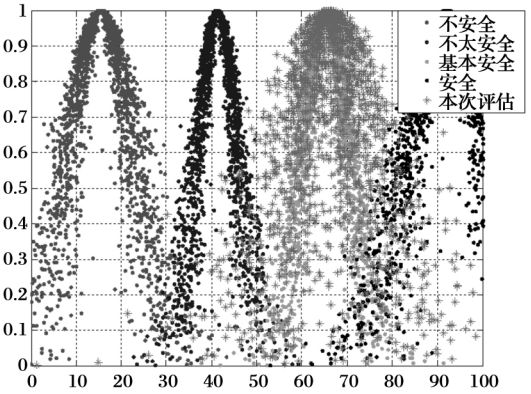

图 6 云模型评估结果图

4 结语

笔者综合考虑了影响主机安全的连续与离散型因素，确定了一种主机安全评估指标集，并利用云模型的“软化分”概念，构造定性评估的规则库，且引入云的不确定推理理论，从而设计了一种评估主机安全的推理算法. 经过实例验证，该评估方法比较高效，能实现定性与定量评估的结合，符合人群的决策思维.

参考文献

[1] 魏德宾,辛鑫. 基于 ANP 和云模型的军事通信系统效能评估[J]. 火力与指挥控制,2016,41(8):128 - 124.

[2] 翁迟迟,齐法制,陈刚. 基于层次分析法与云模型的主机安全风险评估[J]. 计算机工程,2016,42(2):1 - 6.

[3] 张友鹏,李远远. 基于云模型和证据理论的铁路信号系统风险评估[J]. 铁道学报,2016,38(1):75 - 80.

[4] 张鹏,谢晓尧. 基于云模型的信息系统测评安全结论判定[J]. 武汉大学学报: 理学版. 2014,60(5):429 - 433.

[5] 胡文嘉,谢晓尧. 基于二维云模型的主机安全等级评估研究[J]. 计算机应用与软件,2016,33(1):326 - 329.

[6] 尹航,李远富. 综合交通项目安全应急方案的云模型比选方法研究[J]. 中国安全科学学报,2016,26(7):102 - 107.

[7] 胡冠宇,乔佩利. 基于云群的高维差分进化算法及其在网络安全态势预测上的应用[J]. 吉林大学学报: 工学版,2016,46(2):568 - 577.

[8] 高洪波,张新钰,张天雷,刘玉超,李德毅. 基于云模型的智能驾驶车辆变粒度测评研究[J]. 电子学报,2016,44(2):365 - 373.

[9] Li D Y,Di K C,Li D R,Shi X M. Mining Association Rules with Linguistic Cloud Modesl [J]. Journal of Software,2000,11(2):143 - 158.

[10] Shi Z Y,Li H H,Cheng B L. The Research and Design of network security Evaluation Systems Based on cloud model [C]. International Conference on Fuzzy Systems and Knowledge Discovery,2012.

[11] 马满福,张正锋. 基于可拓云的网络信任评估[J]. 计算机应用,2016,36(6):1533 - 1537,1557.

[12] 谢立春,张春琴. 基于云模型的网络攻击检测方法及其性能分析[J]. 计算机科学,2015,42(11):378 - 380,389.

[13] 李金武,邓国辉. 基于云模型的分布式主机安全评估方法研究[J]. 福建电脑,2015,31(9):16 - 17,63.

责任编辑 徐 刚

An Assessment Method of Host Security Based on Cloud Model

LI Jin-wu

(College of Information Engineering, Zhengzhou University of Science & Technology, Zhengzhou 450064, China)

Abstract: This paper presents a method of host security assessment based on cloud model. This method comprehensively takes into consideration the continuous and discrete factors affecting host security, and implements a complete index factors set, and the discrete parameters are added into the cloud of uncertain reasoning. The reasoning algorithm based on the evaluation of continuous parameters is improved. By this reasoning algorithm, cloud uncertainty assessment is implemented to solve the uncertainty in assessment knowledge representation, and to realize the uncertainty conversion between qualitative concept and quantitative data, to provide reliable decision-making information to the user. The feasibility of this method is verified through experiment simulation.

Key words: cloud model; host security; index factors