DOI:10.19304/j.cnki.issn1000-7180.2015.01.007

一种新的网络安全态势评估方法

杨宏宇，褚润林，李东博
（中国民航大学 计算机科学与技术学院，天津 300300）

摘 要：提出了基于隶属云的网络安全态势评估方法. 首先从传输服务、资产、脆弱性、安全事件和物理设备五个维度入手，构建一种多层次、多维度、可扩展的网络安全评估指标体系，并给出各维度指标的预处理方法. 然后设计了包含数据层、信息层和知识层的三层模型框架，给出了指标标准化及权重计算方法、安全态势计算流程并给出态势计算方法. 最后设计了网络安全态势评估实验平台并进行了仿真验证实验. 实验结果表明提出的方法对网络安全态势评估具有很好的有效性和合理性.

关键词：网络安全；指标体系；隶属云；态势评估
中图分类号：TN402 **文献标识码**：A **文章编号**：1000－7180(2015)01－0029－06

A New Method for Network Security Situation Assessment

YANG Hong-yu, CHU Run-lin, LI Dong-bo
(School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: This paper presents a method of network security situation assessment based on membership cloud model. Firstly, a multi-level and multi-dimensional extensible network security evaluation index system were built in terms of transport services, assets, vulnerabilities, security events and physical equipments, and an index pretreatment method was designed for each dimension. Secondly, a three-layer model framework which included the data layer, the information layer and the knowledge layer was designed, and the index standardization and weight calculation method, the security situation calculation process were given, and the network security situation assessment algorithm was designed. Finally, we designed the network security situation assessment platform and simulated the experiment on the platform. The experimental results show that the effectiveness and rationality of our method is fine.

Key words: Network security; index system; cloud model; situation assessment

1 引言

随着网络安全事件的逐渐增多[1-3]，被动的防御技术已经不能满足用户的需要，网络安全态势评估作为网络监控的一门新技术[4]，已经成为了目前信息安全的研究热点之一. 态势评估不仅能反映网络在一段时间的整体安全性，还能为预测网络安全态势做准备工作，对于提高网络安全性有重要的意义.

有关网络安全态势预测模型，相关的方法和理论还需要进一步完善[5-8]；

已有的研究大多数可视化程度不高，有些停留在评估算法研究上，没有对网络安全态势状况发展趋势进行预测分析. 本文提出一种基于隶属云的态势评估方法. 从宏观角度出发，将网络安全区分成传输服务、资产、脆弱性、安全事件以及物理设备五个维度，通过计算和分析获取各维度的安全态势指标，最终以隶属云图的形式直观地展现各维度的态势以及整个网络的安全综合态势.

收稿日期：2014－03－28；**修回日期**：2014－05－22
基金项目：国家自然科学基金(60776807，61179045)；国家科技重大专项(2012ZX03002002)；国家“八六三”计划重点课题(2006AA12A106)；天津市科技计划重点项目(09JCZDJC16800)；中国民航科技基金(MHRD201009，MHRD201205)

2 网络安全态势评估指标体系

2.1 评估指标体系基本框架

结合层次分析法思想，针对网络安全的自身特点，定义物理安全指标、传输服务指标、资产指标、脆弱性指标，威胁指标函数来描述整体网络态势（指标体系基本框架如图 1 所示）.

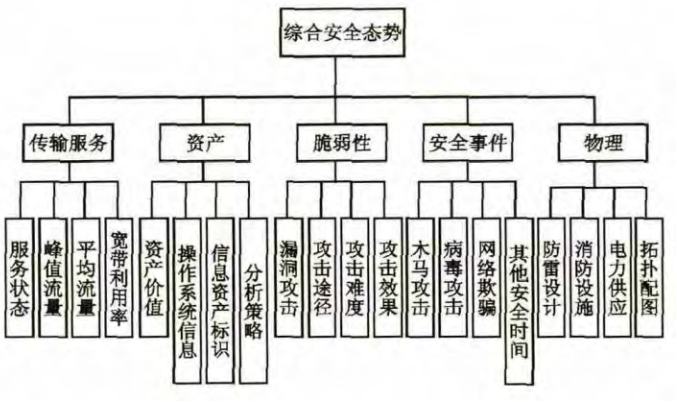

图 1 评估指标体系基本框架

网络整体态势 S：评估某时间段内所有影响网络安全态势的因素，综合得出反映网络整体安全态势的向量 $S=<C,V,T,R,P>$[1]，其中 C 是传输服务指标，V 是资产指标，T 是脆弱性指标，R 是安全事件指标，P 是物理指标[9].

2.2 指标体系的构建

通过分析五个维度安全态势的构成属性，提取从不同安全工具检测的安全指标，构建层次式树状指标体系如下：

(1)传输服务维指标

传输服务维指标主要包含网络系统的两个方面：服务和流量. 其指标的设定如表 1 所示.

表 1 传输服务维指标

传输服务维指标	服务	服务状态
	流量	峰值流量
		平均流量
		宽带利用率

(2)资产维指标

资产指标包括网络系统的资产指数和标准符合度，其指标设定如表 2 所示.

表 2 资产维度指标

资产	资产指数	资产价值
		操作系统打分
	标准符合度	信息资产敏感度标识
		分析策略信息

(3)脆弱维指标

通过对公共漏洞和暴露[10-11]（common vulnerability and exposures，CVE）和通用漏洞评分系统[12-13]（common vulnerability scoring system，CVSS）标准的分析，建立脆弱维指标，指标分为两级，一级指标为脆弱性综合态势，二级指标包含漏洞数量、攻击途径、攻击难度以及攻击效果. 每个二级指标都有可选值，具体分值如表 3 所示.

表 3 脆弱维指标组成及其对应分值

一级指标	二级指标	二级指标可选值	分值
脆弱性	漏洞数量	通过统计得到	
	攻击途径	远程/本地/无漏洞	0.4/0.7/1.0
	攻击难度	高/中/低/无漏洞	0.1/0.6/0.8/1.0
	攻击效果	完全/部分/不受影响/无漏洞	0.7/0.8/0.9/1.0

(4)安全事件维指标

本文将攻击行为按照效果分为木马攻击、病毒攻击、网络欺骗类和其他安全事件四大类，表 4 为安全事件指标组成表.

表 4 安全事件指标组成表

一级指标	二级指标	三级指标
威胁指数	木马攻击	目的资产、非授权性、隐蔽性、事件数目
	病毒攻击	目的资产、严重程度、传播性、可清除性
	网络欺骗类	目的资产、严重程度、可清除性
	其他安全事件	目的资产、严重程度、可清除性

(5)物理设备维指标

物理安全是网络安全的最基本保障，其安全风险主要是指由于网络周边环境和物理特性引起的网络设备和线路的不可用，而造成网络系统的不可用. 根据《计算机信息系统国际联网保密管理规定》，网络物理设备维指标主要包括以下 5 种：

①物理位置选择；

②物理访问控制；

③防盗窃和防破坏；

④防雷击、防火、防水及防潮；

⑤电力供应.

3 基于隶属云的网络安全态势评估模型

设 U 是一个用精确数值量表示的论域，U 上对应的定性概念 A，对于任意一个论域中的元素 x，都存在一个趋于稳定的随机数 $y\in[0,1]$，称 x 对 A 的隶属度，则隶属度在论域上的分布称为隶属云[14-15].

3.1　基于隶属云的态势评估模型框架

本文将态势评估模型分成三层：数据层、信息层和知识层（如图 2 所示）.

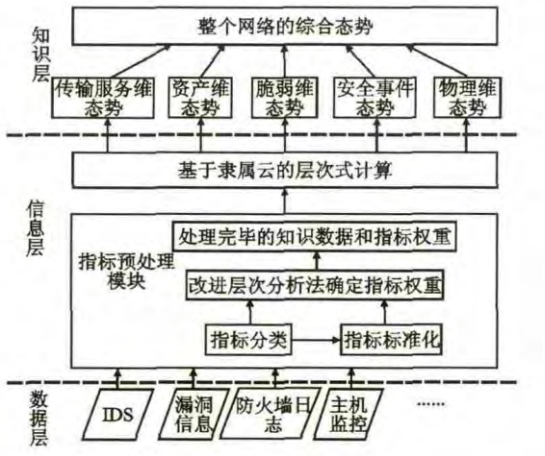

图 2　网络安全态势评估模型框架

该模型的输入由数据层的多个安全设备提供. 网络安全态势评估流程如图 3 所示.

图 3　基于隶属云的网络安全态势评估流程

3.2　基于隶属云的安全态势计算方法

安全态势计算包括三个重要因素[16]，分别是指标因素集、态势评估集、指标权重集.

定义指标因素集为 $U=\{U_0,U_1,\cdots U_n\}$，其中 U_i 为影响最终指标的第 i 个指标；

定义指标权重集为 $W=\{W_1,W_2,\cdots W_n\}$，其中 W_i 满足 $W_i>0$ 或者 $W_i=0$，并且满足 $W_1+W_2+\cdots+W_m=1$；

定义态势评估集为 $V=\{V_1,V_2,\cdots V_n\}$.

按需要把评估指标分为多层结构，从系统指标层次的第 n 层开始，将用基于隶属云重心评判法[17]得到的评判结果传递给上一层. 再依次分层评估，直至得到目标层指标的评估结果. 具体评估步骤设计如下：

（1）态势指标集的确定

在指标体系中，每个评估指标都有着不同的重要程度，需要对每一个评估指标设定它的权重值来体现其不同的重要性，从而达到可比较的、客观的要求.

（2）各个指标体系的隶属云表示

在已知的网络安全态势评估指标体系中，有些采用确定性的数值表示，有些采用规范的语言值表示. 根据上述表示方法，随机抽取 n 组数据，进而组成相应的决策矩阵，用一个隶属云表示 n 个确定的数值型指标. 具体表示为

$$Px=\frac{Px_1+Px_2+\cdots Px_n}{n} \tag{1}$$

$$Pn=\frac{\max(Px_1,Px_2,\cdots Px_n)-\min(Px_1,Px_2\cdots Px_n)}{6} \tag{2}$$

此外，还可以用一个隶属云来表示规范的语言值型的指标. 本文用一维综合隶属云来表示一个指标，即 n 个语言值（隶属云）. 其中，

$$Px=\frac{Px_1Pn_1+Px_2Pn_2+\cdots Px_nPn_n}{Pn_1+Pn_2+\cdots Pn_n} \tag{3}$$

$$Pn=Pn_1+Pn_2+\cdots Pn_n \tag{4}$$

（3）系统状态的表示

用 n 个隶属云可以表示 n 个性能指标，由此采用一个 n 维综合隶属云就能表示 n 个指标所反映的当前系统状态. 隶属云的形状和重心随着当前系统的状态发生改变. 隶属云重心就是其重心位置（隶属云的期望值）与重心高度之乘积. 系统状态信息的变化可以通过观察隶属云重心的变化随时掌握. 本文用向量 $\boldsymbol{C}$ 表示 n 维综合隶属云重心，$\boldsymbol{C}=(C_1,C_2,\cdots,C_n)$，其中，$C_i=l\times h,i=1,2,\cdots n$. l 表示隶属云重心的位置，h 表示隶属云重心的高度，即权重值. 若当前系统发生了变化，则隶属云重心也会随之发生，即变化为 $C^1,C^1=(C_1{}^1,C_2{}^1,\cdots,C_n{}^1)$.

（4）衡量隶属云重心变化

用向量 $\boldsymbol{l}=(P_{x1}^0,P_{x2}^0,\cdots,P_{xn}^0)$ 表示 n 维综合隶属云重心位置，$\boldsymbol{h}=(h_1,h_2,\cdots,h_n)$ 表示隶属云重心高度. 则隶属云重心向量为

$$\boldsymbol{C}^0=\boldsymbol{l}\times\boldsymbol{h}=(C_1{}^0,C_2{}^0,\cdots,C_n{}^0) \tag{5}$$

同理，可以求出某个状态下的 n 维综合隶属云重心向量 $\boldsymbol{C}=(C_1,C_2,\cdots,C_n)$.

为了更好地衡量两种不同状态下综合隶属云重心之间的不同，引入加权偏离度 d. 在当前状态的前提下，对 $\boldsymbol{C}^0$ 进行归一化处理有 $C^G=(C_1{}^G,C_2{}^G,\ldots$

$C_n{}^G$). 其中，$C_i{}^G$ 的计算公式为

$$C_i^G = \begin{cases} (C_i - C_i^0)/C_i^0 & C_i \leqslant C_i^0 \\ (C_i - C_i^0)/C_i & C_i > C_i^0 \end{cases} \tag{6}$$

加权偏离度 d 计算公式为

$$d = \sum_{i=1}^{n} W_i^* C_i^G \tag{7}$$

式中，W_i^* 为相应的权重值. 将 d 输入到隶属云发生器中即可得出效能值.

(5) 评语集的实现

评语数目越多，评语集越准确. 这里 1 个评语集由 11 个评语构成. 用隶属云实现每个评语，并将其表现在语言值标尺上，形成的定性评测隶属云发生器如图 4 所示.

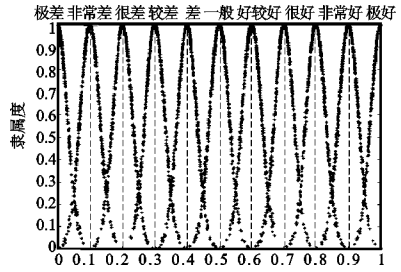

图 4 定性评测隶属云发生器

当 d 值输入到定性评测隶属云发生器后，会有两种可能：一种是激活了两个程度相差不大的两个评语值的隶属云对象，此时可生成一个新的隶属云对象，测评结果取它的期望值，再由系统用户或专家给出与之对应的定性表述；另一种是激活两个程度相差很大的评语值的隶属云对象，此时可以将激活程度大的作为最终评测结果.

4 态势评估实验平台的实现

4.1 指标体系的层次性表示

由于评估指标体系是树状的，具有明显的层次性，为了在数据库中体现出这种层次关系，本文提出将当前节点的子节点、父节点和层次关系信息存储在相应的节点属性中. 其中，根节点的父节点字段值为空，当前指标体系根节点为网络安全态势综合值；叶节点的子节点个数字段为空，代表指标体系结构中最下层节点指标.

4.2 原始数据收集

结合网络安全态势评估的特点，以及网络安全态势评估的复杂性，本实验平台分别从监听类数据源、监控类数据源、扫描类数据源以及现实调查数据源进行原始数据的采集. 结构图如图 5 所示.

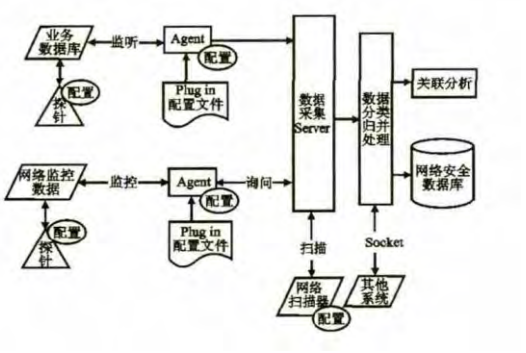

图 5 数据收集模块体系结构图

4.3 安全态势计算

由于原始数据是从多种数据源采集而来，其范围的选择和处理方法上也存在显著的区别，从而导致计算方法需要相应的改变. 鉴于此，设计实现了态势计算模块，其结构如图 6 所示.

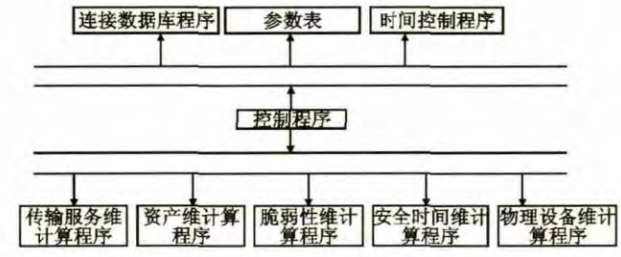

图 6 态势计算模块结构

各维度之间以并行方式进行计算. 处理流程如图 7 所示.

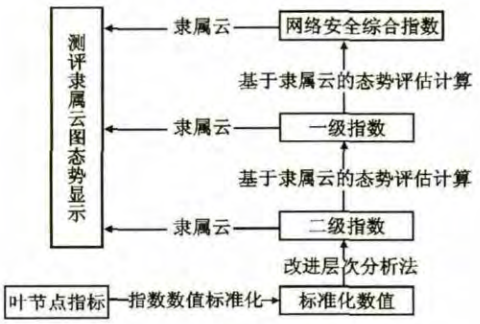

图 7 计算模块处理流程

5 实验结果与分析

现有的网络安全设备有很多，如入侵检测系统、FireWall、HoneyPot 等，收集这些设备产生的网络安全日志，可以获取到网络的安全状态信息. 采用 4.2 节中设计的原始收集模块，在校园网络中连续采集一周的多源数据作为仿真实验数据.

依据 3.2 节中的基于隶属云的态势计算方法，分别对网络安全指标体系中的传输服务、资产、脆弱性、安全事件、物理设备五个维度进行计算和分析.

得到各维度隶属云重心向量的计算结果分别为

$$\begin{aligned}\boldsymbol{C}_{U_1} &= (C_1, C_2, C_3, C_4)\\ &= (0.169, 0.147, 0.126, 0.243),\\ \boldsymbol{C}_{U_2} &= (C_1, C_2, C_3, C_4)\\ &= (1.62, 1.663, 0.155, 0.126),\\ \boldsymbol{C}_{U_3} &= (C_1, C_2, C_3, C_4)\\ &= (0.24, 0.125, 0.138, 0.194),\\ \boldsymbol{C}_{U_4} &= (C_1, C_2, C_3, C_4)\\ &= (0.273, 0.105, 0.189, 0.09),\\ \boldsymbol{C}_{U_5} &= (C_1, C_2, C_3, C_4)\\ &= (0.147, 0.195, 0.175, 0.175).\end{aligned}$$

然后，根据式(5) ～ (7)，计算出各个维度距离理想状态下的加权偏离度分别为：$d_1 = -0.315$，$d_2 = -0.207$，$d_3 = -0.303$，$d_4 = -0.343$，$d_5 = -0.308$，在将它们依次输入到测评隶属云发生器，激活形成各维度安全态势图如图 8 至图 12 所示.

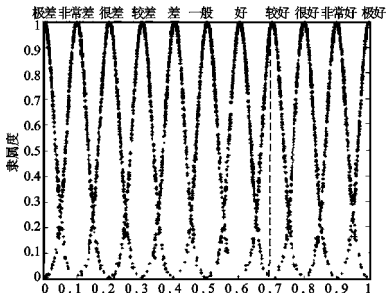

图 8　传输服务维安全态势图

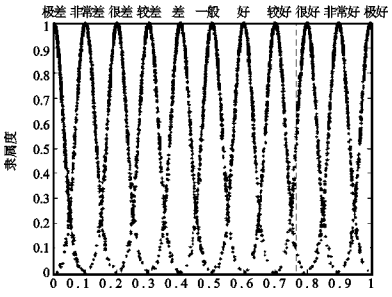

图 9　资产维安全态势图

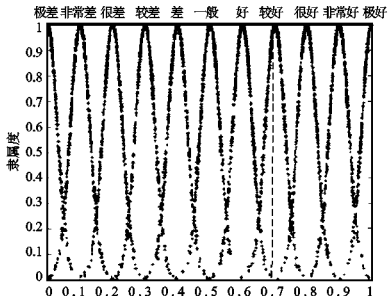

图 10　脆弱维安全态势图

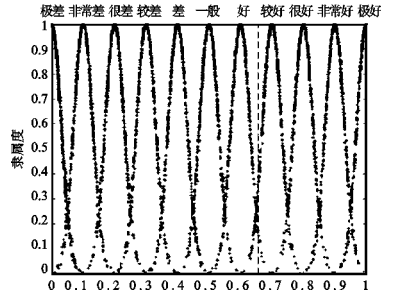

图 11　安全事件维态势图

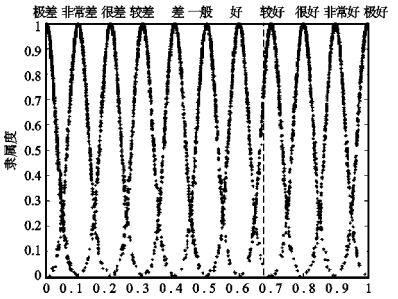

图 12　物理设备维安全态势图

由图 8 至图 12 可以分析得出，传输服务维、资产维、脆弱维激活的隶属云对象“很好”和“较好”，激活情况为前文提到的第二种，故取“很好”作为它们的安全态势语言表述，将各评语值用精确数值表示分别为：$P_1 = 1 - 0.315 = 0.685$，$P_2 = 1 - 0.207 = 0.793$，$P_3 = 1 - 0.303 = 0.697$.

安全事件维、物理设备维激活的隶属云对象为“好”和“较好”，激活情况也为第二种，取“较好”作为他们的态势语言表述，将各评语值用精确数值表示为：$P_4 = 1 - 0.343 = 0.657$，$P_5 = 1 - 0.308 = 0.692$.

此时，根据式(7)可以求出该综合态势值：$\sum_{i=1}^{n}(P_i W_i) = 0.713$. 将其输入评测隶属云发生器，激活的隶属云对象为“较好”和“很好”，前者的激活程度大，故总体效能表述为“较好”. 生成的网络安全综合态势图如图 13 所示.

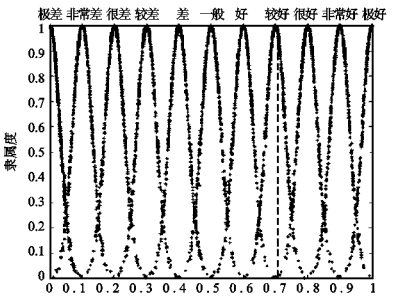

图 13　网络安全综合态势图

通过对上述数据的计算和分析，该网络在 9:00—13:00 这四个小时内的综合态势较好，但安全事件维态势较差，若要进一步提高该网络整体安全情况，则需要在安全事件维度方面重点提高.

本文设计的基于隶属云的网络安全态势评估模型与现有模型进行效能比较，结果如表 6 所示，由该表可以看出本文模型支持的效能指标更加全面，便于管理员更好的掌握网络的安全态势.

表 6 本文模型与相关模型的效能比较

效能 \ 模型	AHP 模型	专家决策	本文模型
指标体系编辑		√	√
权重分析	√	√	√
嵌入指标量化脚本			√
综合计算	√	√	√
分维度态势显示			√
定型指标和定量指标的综合分析			√

本文提出的态势评估方法从不确定性着手，集成模糊性和随机性，设计了较好的定性定量间转换的模型，最终将评价结果以隶属云图的方式直观地展现出来，有效地处理了不确定性，具有一定的科学性.

6 结束语

本文将隶属云的评估方法同改进层次分析法结合，提出了层次化隶属云的安全态势评估模型.

文中所设计的实验平台虽能很好地展示当前网络中传输服务、资产、脆弱性、安全事件以及物理设备五个维度的安全态势，但是在指标量化标准上，还需要做进一步的研究.

参考文献：

[1] 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)：763-771.

[2] 卓莹，龚春叶，龚正虎. 网络传输态势感知的研究与实现[J]. 通信学报，2010，31(9)：54-63.

[3] 张焱，黄曙光，朱俊茂，等. 网络传输态势感知的研究与实现[J]. 微电子学与计算机，2011，28 (8)：123-128.

[4] 朱丽娜，张作昌，冯力. 层次化网络安全威胁态势评估技术研究[J]. 计算机应用研究，2011，28(11)4303-4306.

[5] 张勇，谭小彬，崔孝林，等. 基于 Markov 博弈模型的网络安全态势感知方法[J]. 软件学报，2011，22(3)：495-508.

[6] KumrarV. A network security situation analysis framework based on information fusion[C]// Proceedings of 2011 6th IEEE Joint International Information Technology and Artificial Intelligence Conference (ITAIC 2011). China，Chongqing，2011：362-332.

[7] Xi Rongrong，Jin Shuyuan，Yun Xiaochun，et al. CNSSA：a comprehensive network security situation awareness system[C]// Proceedings of 2011 IEEE 10th International Conference. UK：Liverpool：482-487.

[8] 张丹，郑瑞娟，吴庆涛，等. 基于自律计算的网络安全态势感知模型[J]. 计算机应用，2013，33(2)：404-407.

[9] 王志平. 基于指标体系的网络安全态势评估研究[D]. 长沙：国防科技大学，2010.

[10] Common vulnerabilities and exposures [EB/OL]. [2014-05-15]. http://cve. mitre. org/.

[11] 薛佩军，史开泉，卢昌荆. F-生成规律与系统规律识别[J]. 系统工程与电子技术，2007，29(1)：53-56.

[12] John C，John T. Common vulnerability scoring system [EB/OL]. [2014-04-33]. http://www. first. org/cvss/v1/guide. html. 2004.

[13] Peter M，Karen S，Sasha R. A complete guide to the common vulnerability scoring system version 2. 0[EB/OL]. [2014-05-15]. http://www. first. org/cvss/cvss-guide. pdf.

[14] 范定国，贺硕，段富，等. 一种基于云模型的综合评判模型[J]. 科技情报开发与经济，2003，13(12)：157-159.

[15] 黄海生，王汝传. 基于隶属云理论的主观信任评估模型研究[J]. 通信学报，2008，29(4)：13-19.

[16] 柳炳祥，李海林. 一种基于云模型的综合评判方法[J]. 微计算机信息，2007，23(1/2)：234-262.

[17] 冯增辉，张金成，张凯，等. 基于云重心评判的战场态势评估方法[J]. 火力与指挥控制，2011，36(3)：13-15.

作者简介：

杨宏宇 男，(1969-)，博士，教授. 研究方向为网络信息安全. E-mail：yhyxlx@hotmail. com.

褚润林 男，(1989-)，硕士. 研究方向为网络信息安全.

李东博 男，(1987-)，硕士，工程师. 研究方向为网络信息安全.