基于灰色综合关联分析的网络安全评估

刘晓玲[1] 谢仙斌[2] 张家录[1] 刘灵丽[1]

[1](湘南学院计算机科学系 郴州 423000)
[2](高斯贝尔数码科技股份有限公司 郴州 423000)

摘 要 随着网络应用的发展，网络安全评估已成为网络安全研究的一个重要课题。为了克服传统网络安全评估模型的不足，文章提出了基于灰色综合关联分析的网络安全综合评估模型。该模型将灰色关联分析法与层次分析法有机结合，首先通过德尔菲法建立评估指标体系，然后采用层次分析法确定各被评因素的权重，最后计算灰色关联度对网络安全进行评估。利用该方法对某高校网络进行仿真实验，结果表明，该方法评估结果准确，是一种高效、准确和实用的网络安全评估方法。

关键词 网络安全；安全评估；层次分析法；灰色关联分析
中图分类号 TP 393.18 **文献标志码** A

Network Security Assessment Based on Comprehensive Grey Relational Analysis

LIU Xiaoling[1] XIE Xianbin[2] ZHANG Jialu[1] LIU Lingli[1]

[1](*Department of Computer Science*, *Xiangnan University*, *Chenzhou* 423000, *China*)
[2](*Gospell Digital Technology Co*., *Ltd*., *Chenzhou* 423000, *China*)

Abstract With the development of network applications, the network security assessment has become an important subject of researches on network security. In order to overcome the defects of traditional network security evaluation models, the network security assessment model based on the comprehensive grey relational analysis, which is the organic combination of grey relation analysis and the analytic hierarchy process (AHP), was proposed in this paper. Firstly, the proposed model used the Delphi method to construct the network security assessment index system. Secondly, it utilized AHP to work out the specific weight of each index. Finally, the comprehensive grey relational degree was calculated to evaluate the network security. By means of simulating a campus network with MATLAB, the research results show that the evaluation is more accurate and the proposed assessment method is an efficient, accurate and practical network security assessment method.

Keywords network security; security assessment; analytic hierarchy process; grey relational analysis

收稿日期：2014-2-24
基金项目：湖南省教育厅科学研究项目(11C1176)，湖南省科技计划项目(2014FJ3010)，湖南省教育厅科学研究重点项目(14A135)。
作者简介：刘晓玲(通讯作者)，硕士，讲师，研究方向为计算机应用和网络安全，E-mail：lxlwork@126.com；谢仙斌，工程师，研究方向为网络通信和数字电视；张家录，教授，研究方向为非经典数理逻辑与近似推理、粗糙集理与应用；刘灵丽，副教授，研究方向为图像处理。

1 引　言

随着互联网技术的不断进步和计算机网络的普及，计算机网络面临的威胁也越来越大。计算机病毒、木马程序、黑客和 DoS/DdoS 攻击日益猖獗，网络安全事件层出不穷。科学地对计算机网络所面临的威胁程度进行评估，并采取有效措施对网络风险进行防范，最大限度地降低网络安全损失，已成为当前网络安全研究中的一个重要课题[1,2]。

网络的不同应用领域对安全要求不一致，例如，军事国防、金融等机构的网络安全等级要求很高，而民用网络的安全程度要求则相对较低。因此对网络安全状况进行科学准确的评估，有利于管理员针对网络状况采取不同的预防措施，从而提高网络的安全等级[3]。

传统的防火墙和入侵检测设备是单一的防御或检测设备，只能对攻击行为的某一局部进行检测，缺乏对整个网络系统的考虑，不能满足当前网络安全的需求。最近几年，在新的理论和方法的研究与发展中，很多学者将 SFTA（Software Fault Tree Analysis）分析法、FMECA（Failure Mode Effects and Criticality Analysis）危险度分析法和神经网络等方法用于网络安全评估领域[4]。但是，由于网络安全系统的复杂性，这些定量的方法不能很好地考虑网络系统客观环境和人为因素的影响，而且网络安全评估很难严格地定量化，因此利用完全定量的网络安全评价很难实现对网络的准确评估[5]。

层次分析法（Analytic Hierarchy Process，AHP）是一种定性与定量相结合的决策分析方法[6]。它由美国运筹学家、匹兹堡大学 Santy 教授于 20 世纪 70 年代提出[7]。这种将思维过程数据化的方法不仅简化了系统分析和计算，而且便于决策者保持思维过程的一致性。同时它具有原理简单、结构化和层次化等特点。而灰色理论则是我国学者邓聚龙于 1982 年提出的，它主要以部分信息已知、部分信息未知的小样本、贫信息和不确定性系统为研究对象，通过对已知信息的生成和提取分析，最终实现对系统运行行为的正确认识和有效控制。与其他不确定性常用研究方法（概率统计和模糊数学）相比，灰色理论具有要求数据信息少且对数据无特殊要求等特点[8,9]。

在对网络安全风险分析的基础上，结合网络安全评估的实际需求，本文提出了基于层次分析和灰色关联分析的灰色综合关联分析的网络安全综合评估模型。该模型将灰色关联分析法与层次分析法有机结合，具有高度的逻辑性和灵活性，能把一定的模糊性因素进行量化，可有效解决网络安全多因素、多层次和非定量化条件下的评估问题。与其它评估模型相比较，灰色综合关联分析法在网络安全的评估方面有较大的优势，评价结果更准确，结论更有说服力。

2　基于灰色综合关联分析的数学模型

灰色综合关联分析是将灰色系统理论和层次分析法进行有机结合。该方法首先通过构建评估模型层次结构，然后利用层次分析法求得各层次、各因素间的权重，接着利用灰色关联分析求得灰色综合关联度，最后依据关联度值的大小确定评估结果。下面分别简要地介绍层次分析和灰色关联分析。

2.1　层次分析

层次分析法主要包括三个步骤：（1）分解。将一个复杂的系统抽象化为一个有序的、层次的结构模型；（2）判断。将同一层次的评价指标进行两两比较，构造判断矩阵，计算各评价指标的相对权重；（3）综合。对各层指标的组合权重进行计算，得到各指标相对于总目标的权重值，然后排序。

根据层次分析的中心思想建立数学模型：首先把影响系统的因素划分为不同的层次，建立层

次结构模型，并确定层次间的递阶结构及各因素的从属关系；其次对被评因素进行两两比较，采用 Santy 教授提出的 1～9 标度法构造判断矩阵；然后计算被评因素的相对权重。最后根据矩阵论，利用方根法求出判断矩阵的特征向量和最大特征值 λ_{max}，并作一致性检验 CI。其计算公式为：

$$CI=\frac{\lambda_{max}-n}{n-1} \tag{1}$$

其中，n 为判断矩阵的阶次；λ_{max} 为判断矩阵的最大特征根。

当随机一次性比率 CR 满足如下式：

$$CR=\frac{CI}{RI}\prec 0.10 \tag{2}$$

其中，CI 为判断矩阵的一致性指标；RI 为平均随机一致性指标。当 $CR\prec 0.10$ 时，说明该判断矩阵具有满意的一致性，结果可接受。反之，该判断矩阵的一致性较差，不能接受。

2.2 灰色关联分析

灰色关联分析是一种基于灰色理论的分析方法，运用它可以通过关联系数或综合关联度等特征量分析内在联系，达到发现影响网络安全因素的主要关系及主要特征的目标。它对样本无苛刻要求、计算量较小，可以保证量化结果与定性分析结果一致。灰色综合关联分析过程概况为：

(1) 构造行序列 X_i。将影响网络安全评估的各项因素所对应的观测数据 $x_i(k)$ $(k=1,2,\cdots,n)$ 组成行序列 X_i，即：$X_i=(x_i(1),x_i(2),\cdots,x_i(n)),i=1,2,\cdots,m)$。

(2) 根据行序列 X_i 计算初值像 X_i'。初值像就是对序列 X_i 进行无量纲化处理的结果。确定初值像以后，选择初值像中的参考对象组成参考序列 $X_0'=(x_0'(1),x_0'(2),\cdots,x_0'(n)),i=1,2,\cdots,m$，并将初值像中的其他序列组成比较序列。

(3) 计算差序列和两极最大差及最小差。差序列表示两个序列的差异大小。根据初值像 X_i' 中的参考序列和比较序列，计算差序列 $\Delta_i(k)=|x_0'(k)-x_i'(k)|$，然后比较差序列求出两极最大差 $M=\max\limits_i\max\limits_k\Delta_i(k)$ 和两极最小差 $m=\min\limits_i\min\limits_k\Delta_i(k)$。

(4) 计算灰色关联系数 $r_i(k)$。其计算公式为：

$$r_i(k)=\frac{m+\xi M}{\Delta_i(k)+\xi M} \tag{3}$$

其中，$k=1,2,\cdots,n$；$i=1,2,\cdots,m$；ξ 为分辨系数，且 $\xi\in(0,1)$，分辨系数用来削弱因两极最大差过大而导致网络安全评估不准确的影响。

(5) 求灰色综合关联度。将灰色关联系数与层次结构权重相结合，计算灰色综合关联度。灰色综合关联度 r_i 反应了参考序列 X_0' 和比较序列的关联程度，其计算公式为：

$$r_i=\sum_{k=1}^{n}w_ir_i(k) \tag{4}$$

其中，$i=1,2,\cdots,m$；w_i 为权重，可以根据层次分析法确定。由灰色综合关联分析法计算比较序列对参考序列之间的相互关联度，其计算值的大小反应两者之间的相互影响程度的大小，值越大则表示其对参考序列的影响程度也越大。

3 基于灰色综合关联分析的网络安全评估

3.1 网络安全评估的依据

网络安全工作的核心任务是网络安全评估，评估的正确率对网络安全可靠性起着至关重要的作用。实体安全、运行安全、信息安全和软件安全是网络安全的重要因素。以国家规定的相关网络安全评测标准为依据，采取相关的措施对网络系统处理、传输和存储信息的完整性、保密性和可用性等安全属性进行科学、公正的过程评估，并根据网络安全评估结果，提出有效的防范措施，旨在最小化网络风险程度。

3.2 网络安全评估指标体系的建立

网络是个复杂的系统，影响其安全的因素

比较多。为了保证评估结果的客观性和准确性，本文首先利用德尔菲法建立网络安全评估指标体系结构，其次对初步建立的评价指标进行分类，并设计网络安全评价指标咨询表，然后咨询有关专家意见，最后根据专家意见对指标进行调整和筛选。本文以湖南某高校网络为例，依据专家意见从物理安全、逻辑安全和管理安全三个主要方面建立三级层次结构的网络安全评估指标体系结构，如图 1 所示。物理安全、逻辑安全和管理安全 3 项作为被评因素；同时选取防电磁泄露措施、网络机房安全、供电安全、线路安全、容错安全、设备安全、数据备份、数据恢复、软件安全、防病毒措施、数据加密、入侵防范、安全组织体系、安全管理制度、人员安全培训和应急响应机制 16 项指标作为被评子因素。用 y_1 至 y_3 表示各被评因素，x_1 至 x_{16} 表示各被评子因素。

3.3　网络安全评估等级的建立

本文将网络安全评估等级总分设为 1，一共分五个级别，分别为很安全(0.9≤评估值≤1)、安全(0.8≤评估值＜0.9)、基本安全(0.7≤评估值＜0.8)、不安全(0.6≤评估值＜0.7)、很不安全(评估值＜0.6)。具体说明见表 1。

3.4　基于灰色综合关联分析的网络安全评估

网络安全评估一般采用专家组打分评估的方式，以消除个人评估导致的片面性，从而保障评估结果的科学性和客观性。网络安全评估的指标

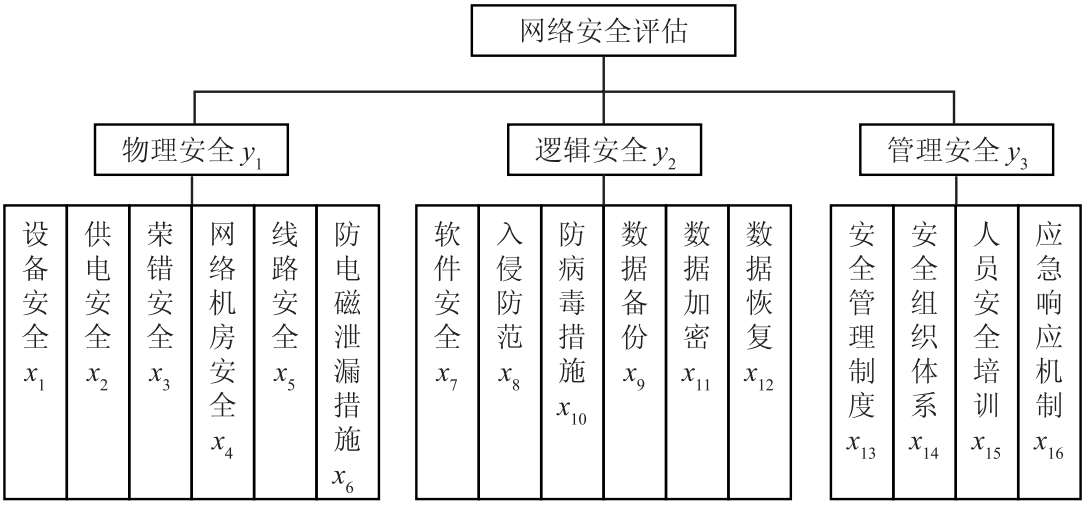

图 1　网络安全评估指标体系层次结构

Fig. 1.　The hierarchy of network security evaluation index system

表 1　网络安全评估标准

Table 1.　Network security evaluation criteria

等级	评估值(x)	说明
很安全（Ⅰ）	0.9≤x≤1	网络具有很强的安全保障能力
安全（Ⅱ）	0.8≤x＜0.9	网络具有较强的安全保障能力
基本安全（Ⅲ）	0.7≤x＜0.8	网络具有一定的安全保障能力
不安全（Ⅳ）	0.6≤x＜0.7	存在安全隐患
很不安全（Ⅴ）	0≤x＜0.6	网络应用安全形势严峻

取值可以根据网络的类型、规模和具体指标内容来确定，本文采用 0～1 记分制。专家组对每个指标进行评分，取其算术平均值计算每个指标的评判结果。表 2 是湖南某高校网络安全评估指标专家最终评分结果。

将表 2 中的校园网安全评估评分序列(0.8,0.8,0.7,0.6,1,0.5)、(0.85,0.8,0.75,0.8,0.85,0.9)和 (0.9,0.7,0.8,0.85)进行无量纲化，本文采用标准化无量纲化方法，计算公式为：

$$y_i=\frac{x_i-\bar{x}}{s} \tag{5}$$

其中：

$$\bar{x}=\frac{1}{n}\sum_{i=1}^{n}x_i,$$

$$s=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(x_i-\bar{x})^2},$$

得到灰色关联分析比较数据列为 y_1=(0.3809, 0.3809,−0.1902, −0.7613, 1.5231, −1.3324)、y_2=(0.4762, −0.4762, −1.4286, −0.4762, 0.4762, 1.4286)和 y_3=(3.9954, −5.1370, −0.5708, 1.7123)。

参考数据列分别为(1,1,1,1,1,1)、(1,1,1,1,1,1)和(1,1,1,1)，Δ_1=(0.6191, 0.6191, 1.1902, 1.7613, 0.5231, 2.3324)、Δ_2=(0.5238, 1.4762, 2.4286, 1.4762, 0.5238, 0.4286)、Δ_3=(2.9954, 6.1370, 1.5708, 0.7123)，取分辨系数 ξ=0.5，根据(3)式求得每个子因素的灰色关联系数：r_{11}=0.9483, r_{12}=0.9483, r_{13}=0.8212, r_{14}=0.7241, r_{15}=0.9737, r_{16}=0.6475; r_{21}=0.9735, r_{22}=0.7695, r_{23}=0.6362, r_{24}=0.7695, r_{25}=0.9735, r_{26}=1; r_{31}=0.5767, r_{32}=0.3799, r_{33}=0.7538, r_{34}=0.9250。

然后通过层次分析法来计算权重集，各层次分析计算结果如下：

	y_1	y_2	y_3
y_1	1	1/3	1
y_2	3	1	1
y_3	1	1/3	1

W=(0.2000, 0.6000, 0.2000)，λ_{max}=3.0000，CI=0，判断矩阵具有完全一致性。

	x_1	x_2	x_3	x_4	x_5	x_6
x_1	1	3	3	3	5	5
x_2	1/3	1	1	1	3	3
x_3	1/3	1	1	1	3	3
x_4	1/3	1	1	1	3	3
x_5	1/5	1/3	1/3	1/3	1	1
x_6	1/5	1/3	1/3	1/3	1	1

W=(0.3977, 0.1612, 0.1612, 0.1612, 0.0593, 0.0593)，λ_{max}=6.0120，CI=0.0024，RI=1.12，CR=0.0021＜0.1。

	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}
x_7	1	3	3	5	5	5
x_8	1/3	1	1	1	3	3
x_9	1/3	1	1	1	3	3
x_{10}	1/5	1	1	1	1	1
x_{11}	1/5	1/3	1/3	1	1	1
x_{12}	1/5	1/3	1/3	1	1	1

W=(0.4328, 0.1612, 0.1612, 0.1026, 0.0711, 0.0711)，λ_{max}=6.1891，CI=0.0378, RI=1.12,

表 2 网络安全评估指标基本数据

Table 2. Basic data of the network security evaluation index

因素	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8
评分结果	0.8	0.8	0.7	0.6	1	0.5	0.85	0.8
因素	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
评分结果	0.75	0.8	0.85	0.9	0.9	0.7	0.8	0.85

CR＝0.0337＜0.1。

	x_{13}	x_{14}	x_{15}	x_{16}
x_{13}	1	1	3	3
x_{14}	1	1	3	3
x_{15}	1/3	1/3	1	2
x_{16}	1/3	1/3	1/2	1

W＝(0.3736, 0.3736, 0.1481, 0.1047)，λ_{max}＝4.0604，CI＝0.0201，RI＝0.9，CR＝0.0223＜0.1。

将各层的相应权重集代入(4)式得到各子因素的灰关联度：r_1＝0.8752，r_2＝0.8584，r_3＝0.5659。将得出的各子因素的灰关联度与被评因素权重集再次代入(4)式可得出该高校网络安全评估的灰色综合关联度：r＝0.8033。

根据网络安全评估标准，该校网络安全评估水平为“安全”，网络具有较强的安全保障能力，与该高校的网络安全级别完全吻合。

由子因素灰色关联度的值可以得其排序：$r_1 \succ r_2 \succ r_3$，由此可得出该高校网络安全中各被评因素从优到劣的顺序是：物理安全、逻辑安全和管理安全。r_3 关联度值最小(0.5659)，在校园网管理安全方面的工作相对比较薄弱，以后需要加大力度完善和强化管理安全的工作。逻辑安全的权重是 0.6000，占整个网络安全评估体系的分量最大，因此逻辑安全方面的管理、操作和预防工作是该校网络安全的重点和关键点。可见，该校今后的网络安全工作应当重点对管理安全方面的工作进行完善、优化，同时也要兼顾物理安全和逻辑安全等方面的管理，力求保证网络时刻处于“安全”和“很安全”的状态，为该校提供良好的网络环境。

4　结　论

本文首先综合层次分析法和灰色系统理论的优点，然后结合网络安全综合评估的实际需求提出了基于灰色综合关联分析的网络安全综合评估模型。实际应用证明，灰色综合关联分析法不但能有效解决网络安全多因素、多层次、非定量化条件下的评估问题，还能对网络安全状况进行整体系统的评估，而且可以保证评估结果更准确、结论更有说服力。

灰色综合关联分析法在网络安全评估的实际应用时应注意：

(1)本文的评估模型只选取了 16 项被评因素。对不同的网络类型、网络规模和网络应用，在进行评估时其层次结构和被评因素可能会有差异。因此在评估前需要了解具体网络的实际情况，才能科学合理地构建相应的网络安全评估指标体系结构，以保证评估的可靠性和客观性。

(2)灰色综合关联分析法能通过应用计算机高级语言进行编程，开发出友好的用户界面，用户只需要输入原始数据就可以快速得到评估结果，使用方便、快捷。

参 考 文 献

[1] 梁颖, 王慧强, 赖积保. 一种基于粗糙集理论的网络安全态势感知方法 [J]. 计算机科学, 2007, 34(8): 95-98.

[2] 卓先德. 网络安全评估的仿真与应用研究 [J]. 计算机仿真, 2011, 28(6): 177-180.

[3] 杨晓宇, 周佩玲, 傅忠谦. 人工免疫与网络安全 [J]. 计算机仿真, 2001, 18(6): 83-85.

[4] 刘蕾磊, 杨世平. 一种定量的网络安全评估模型 [J]. 南昌大学学报(理科版), 2010, 34(4): 401-404.

[5] 李健宏, 李广振. 网络安全综合评价方法的应用研究 [J]. 计算机仿真, 2011, 28(7): 165-168.

[6] 路萍, 吴斌. 层次分析法在高等院校科技评价系统中的应用 [J]. 北京工业大学学报, 2002, 28(3): 358-362.

[7] 文成林, 吕冰, 葛泉波. 一种基于分步式滤波的数据融合算法 [J]. 电子学报, 2004, 32(8): 1264-1267.

[8] 李硕, 戴欣, 周渝霞. 网络安全态势感知研究进展 [J]. 计算机应用研究, 2010, 27(9): 3227-3232.

[9] 周毅, 赵晓刚, 赵健宇. 基于灰色综合关联分析的高校校园安全评估 [C] // Proceedings of the 2011 International Conference on Education Science and Management Engineering , 2011: 1589-1592.