基于模糊综合评价理论的网络安全风险量化评估方法研究

Research on Quantitative Evaluation Method of Network Security Risk Based on Fuzzy Comprehensive Evaluation Theory

高贵银[1]，曹京卫[2]，余思阳[2]，徐　瑶[2]，杨　飞[1]（1. 中讯邮电咨询设计院有限公司，北京 100048；2. 中国联合网络通信集团有限公司，北京 100033）

Gao Guanyin[1]，Cao Jingwei[2]，Yu Siyang[1]，Xu Yao[2]，Yang Fei[1]（1. China Information Technology Designing & Consulting Institute Co.，Ltd.，Beijing 100048，China；2. China United Network Communications Group Co.，Ltd.，Beijing 100033，China）

摘　要：

网络安全风险评估越来越受到人们的关注，而将模糊综合评价理论应用到网络安全风险评估中已经成为一个研究热点。针对模糊综合评价法在网络安全风险评估应用中存在的因主观性太大而影响评估结果准确性的问题，在评估因子的隶属度设定和权重设计方面提出了一种客观的分析方法，并通过模拟实验验证了方案的可行性。

关键词：

网络安全；资产风险；量化评估；模糊综合评价

doi：10.12045/j.issn.1007-3043.2023.08.016

文章编号：1007-3043（2023）08-0071-04

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

Network security risk assessment is receiving increasing attention，and applying fuzzy comprehensive evaluation theory to network security risk assessment has become a research hotspot. Aiming at the problem of subjectivity affecting the accuracy of evaluation results in the application of fuzzy comprehensive evaluation method in network security risk assessment，an objective analysis method for the membership degree and weight design of evaluation factors is proposed，and the feasibility of the scheme is verified through simulation experiments.

Keywords：

Network security；Asset risk；Quantitative evaluation；Fuzzy comprehensive evaluation

引用格式：高贵银，曹京卫，余思阳，等. 基于模糊综合评价理论的网络安全风险量化评估方法研究[J]. 邮电设计技术，2023（8）：71-74.

0　前言

随着计算机网络技术的高速发展，网络安全问题日益突出，引起了社会各界的广泛关注。目前的以防火墙、病毒检测技术和入侵检测技术等为主的安全防护手段，只能在检测到攻击行为后为网络提供安全防护，无法通过风险预估提前告警，这使得安全防护工作极为被动，也增加了网络被攻破的风险。因此，网络安全风险量化评估显得尤为重要。

模糊综合评价法是一种基于模糊数学理论的综合评价方法，能够将一些模糊的、不易定量的因素定量化。前期已有一些研究成果将模糊综合评价方法应用于网络安全风险量化评估中，但在评估因子对风险指标的隶属度设定上存在太多的主观因素。本文通过对模糊综合评价理论和网络安全评估因素深入的研究，在评估因子的隶属度设定和权重设计方面给出了新的思路，并通过模拟实验验证方案的可行性。

收稿日期：2023-06-22

1　模糊综合评价方法

模糊综合评价法是在模糊集合理论的基础上发展起来的一种量化评估方法，能够对受到多种因素制约的事物或对象做出总体的量化评价。它能较好地

解决模糊的、难以量化的问题，适合各种复杂的、非确定性场景的量化评估。由于它的评价结果是一个矢量，而不是一个点值，因此包含的信息比较丰富，可以比较准确地刻画被评价对象。

模糊综合评价法基本原理：首先确定适合评价对象的评价指标集和因素集；再分别确定各因素的权重系数及隶属度向量，获得模糊评判矩阵；最后把模糊评判矩阵与因素的权向量进行模糊运算并做归一化处理，得到模糊综合评价结果。其一般步骤如下：

a）选取评价指标体系。模糊综合评价指标体系是进行综合评价的基础，评价指标的选取是否适宜，将直接影响综合评价的准确性。

b）确定评价因素集。为便于权重分配和评议，根据具体场景，可以设置多级评价因子，例如，在网络安全风险评估中，可设置第1级评价因子，包括威胁维度、资产维度和漏洞维度。其中，威胁维度又可设置第2级评价因子，包括拒绝服务攻击、木马攻击和蠕虫病毒等。

c）评价因素的权重设计。评价系统中各评价因素对评价结果的影响不同，评价因素的权重值反映了该因素的重要性，权重值越大，则其重要性越高。各评价因素的权重值往往通过专家经验法或者层次分析法确定，其中每一级评价因素须满足权重和为1。

d）构建隶属矩阵。模糊综合评价模型的关键在于确定隶属度函数。评价因素的隶属度表达了各评价因子与风险指标的对应关系。确定隶属度函数的方法有多种，例如F统计方法、专家评价法等。

e）隶属矩阵和权重的合成。采用适合的合成因子对其进行合成，并对结果向量进行解释。

模糊综合评价方法能够把复杂问题简单化，把模糊概念清晰化，把定性评价转化为定量评估。将模糊综合评价方法应用到网络安全风险评估领域能较好地解决风险因素错误复杂、风险值难以量化评估的问题。

2 基于模糊综合评价的量化评估方法

2.1 网络安全风险评估要素

网络安全风险是指资产外部的威胁因素利用资产本身的固有漏洞对资产价值造成的损害。网络安全风险评估就是资产价值、资产固有漏洞以及遭受威胁的确定过程。从风险评估的角度来看，资产价值、安全漏洞和安全威胁构成了逻辑上不可分割的有机整体，是风险评估必不可少的3要素。

2.1.1 资产评估

在网络系统中，资产主要是指硬件、软件和信息资产。对资产维度的评估主要是对资产的价值以及资产上所运行服务的重要程度进行评估。

国际标准ISO/IEC13335规定的资产等级如下：1级为“可忽略的”，2级为“低”，3级为“中”，4级为“高”，5级为“严重”。为了对资产的重要性进行评估，首先需要定义网络中的所有资产，然后由资产管理人员根据资产的价值进行定性或定量评估。

2.1.2 威胁评估

威胁维度的评估主要考虑网络系统中的安全事件。对攻击事件的威胁评估，可以按照一定的分类标准，针对网络系统自身的特点进行评估。

由贾焰作为主要起草人、以中国通信标准化协会为归口单位的标准《网络威胁指数评估方法》（YD/T 2389-2011），对网络攻击进行了详细分类，并根据网络威胁指数计算结果将网络威胁划分为5个等级：优、良、中、差、危。

2.1.3 漏洞评估

安全漏洞是信息资产自身的一种缺陷。在选取漏洞维度的评估要素时，主要考虑网络系统自身的漏洞情况，即在不考虑攻击的情况下，分析网络系统自身的脆弱性。

目前国内外有很多漏洞评估方法，依据给出的评估结果形式的不同，大致可分为定量评估和定性评估。通用漏洞评估系统（CVSS）是目前被广泛使用的漏洞评估系统，该系统对安全漏洞危害严重性进行打分，最终得到一个定量的漏洞危害评分结果，其分值范围为0~10。中国国家信息安全漏洞库（CNNVD）对各种安全漏洞划分了危害等级，包括超危、高危、中危和低危。

2.2 网络安全风险评估方法

模糊综合评价方法能够把复杂问题简单化，把模糊概念清晰化，把定性评价转化为定量评估。将模糊综合评价方法应用到网络安全风险评估领域能较好地解决风险因素错综复杂、风险值难以量化评估的问题。

模糊综合评价理论通常包含有因素集和指标集，通过因素集与指标集之间的模糊关系矩阵（即隶属度矩阵）可以得到各评价因素对于风险指标的隶属度向量，从而得到评价因素的综合评价结果。隶属度与隶

属度矩阵是模糊综合评价的关键性概念。

为尽量消除因为评估的主观性和离散数据所带来的偏差，首先对资产、漏洞和威胁维度进行定性或者定量评估，然后根据评估结果确定评估因素与风险指标的隶属度。其基本步骤如下。

步骤1：确定模糊综合评价指标集。

评价指标集是评价者对被评价对象可能做出的各种总的评价结果组成的评语等级的集合，一般可将风险指标划分为5级，即：

$$V=\{1\,2\,3\,4\,5\}$$

步骤2：确定评价因素集。

在网络安全风险评估领域，一级评价因子包括资产类、威胁类，漏洞类，即：

$$U=\{\text{资产 漏洞 威胁}\}$$

有时候，一级评价因子还包括因子的评价因素集，例如：威胁维度评价因子根据攻击类型的不同还可细分为多种二级评价因子：

$$U_3=\left\{\begin{array}{c}\text{拒绝服务攻击}\\ \text{木马攻击}\\ \text{病毒攻击}\\ \text{僵尸网络攻击}\\ \text{网络欺骗类攻击}\\ \text{恶意探测攻击}\\ \text{其他}\end{array}\right\}$$

步骤3：确定评价因素的权重向量。

通常情况下，每种评估因子在风险评估中所占权重不同。风险级别越高的因子，其权重也就越大。可以通过专家估计法确定每种评估因子的权重值。

在本方法中，一级评价因子的权重向量为：

$$B=\{b_1\,b_2\,b_3\}$$

威胁因素包含的各二级评价因子，其权重向量为：

$$B_3=\{b_{31}\,b_{32}\,b_{33}\,b_{34}\,b_{35}\,b_{36}\,b_{37}\}$$

各级评价因素应分别满足：

$$\sum_{i=1}^{n}B_i=1$$

步骤4：确定隶属函数。

在模糊集理论中运用隶属度来刻画客观事物中大量的模糊界限，而隶属度可用隶属函数来表达。为了确定模糊运算需要为每一个评估因子确定隶属函数。评估因子对评价指标的隶属度可通过各评估因子对应的评估标准进行量化。

其中，资产因子可依据资产对应的资产等级属性，而资产等级属性可通过专家评价法确定，将资产等级映射到步骤1的风险指标集，从而得出其隶属函数：

$$R_{1i}=\{r_{11}\,r_{12}\,r_{13}\,r_{14}\,r_{15}\}$$

漏洞因子可根据国家信息安全漏洞库定性评级结果映射到风险指标集，得出漏洞因子的隶属函数：

$$R_{2i}=\{r_{21}\,r_{22}\,r_{23}\,r_{24}\,r_{25}\}$$

威胁因子应首先根据其二级评价因子的评估值计算其与风险指标集的隶属度，然后通过计算其平均值，得出威胁因子的隶属函数：

$$R_{3i}=\{r_{31}\,r_{32}\,r_{33}\,r_{34}\,r_{35}\}$$

所有评估因素对应的隶属函数组合起来，构造出总的隶属函数R：

$$R=\left\{\begin{array}{l}r_{11}\,r_{12}\,r_{13}\,r_{14}\,r_{15}\\ r_{21}\,r_{22}\,r_{23}\,r_{24}\,r_{25}\\ r_{31}\,r_{32}\,r_{33}\,r_{34}\,r_{35}\end{array}\right\}$$

其中，$R(u_i,v_j)=R_{ij}$表示评估因子u_i对指标v_j的隶属度，每种评估因子的隶属度总和需满足归一化：

$$\sum_{j=1}^{n}R_{ij},(i=1,2,\cdots m)$$

考虑到定性评估结果的离散性和不精确性，使风险级别较高的评估因子也有隶属于中级级别风险的可能性。例如，当资产风险级别为3时，那么其隶属于2级风险级别的程度为10%，隶属于3级风险级别的程度为80%，隶属于4级风险级别的程度为10%，漏洞因子和威胁因子同理。

步骤5：模糊评判。

由权重向量与隶属度函数乘积，得到模糊综合评价结果Y：

$$Y=B\times R=\{y_1\,y_2\,y_3\,y_4\,y_5\}$$

该评价结果表征隶属于各风险指标的概率。

3 模拟实验

为验证所提方法的有效性与可行性，选取实验室2台机器作为目标主机，搭建模拟测试环境，环境信息如表1所示。

首先通过专家评议法确定资产等级，共邀请5位评审专家，最终确定资产等级为“中”。

表1　模拟测试环境的环境信息

主机名称	主机A	主机B
主机IP	10.99.2.52	10.99.2.53
配置	4C8G	4C8G
操作系统	CentOS7	CentOS7
应用程序	Dubbo2.7.21、FluxBB1.5.11	Mysql5.7、Redis3.1

然后使用天融信漏洞扫描引擎对2台目标主机进行扫描，发现主机A存在Dubbo代码问题漏洞，该漏洞在国家信息安全漏洞库评级为超危；主机B未发现安全漏洞。

最后使用kali系统对2台主机进行渗透攻击，主机A所部署的FluxBB论坛被暴力破解攻破。

考虑到定性评估结果的离散性和不精确性，使风险级别较高的评估因子也有隶属于中级级别风险的可能性。因此根据资产、漏洞和威胁维度的评估结果分别得出2台目标主机的隶属度函数为：

$$R_A=\begin{Bmatrix}0 & 0 & 0.1 & 0.8 & 0.1 & 0\\ 0 & 0 & 0 & 0.1 & 0.9\\ 0 & 0 & 0.1 & 0.8 & 0.1\end{Bmatrix}$$

$$R_B=\begin{Bmatrix}0 & 0 & 0.1 & 0.8 & 0.1 & 0\\ 0 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 0\end{Bmatrix}$$

通过专家评估法确定各评估因素的权重，得出权重向量：

$$B=\{0.3\ \ 0.4\ \ 0.3\}$$

最终确定其综合评价向量：

$$Y_A=B\times R_A=\{0\ \ 0.03\ \ 0.27\ \ 0.31\ \ 0.39\}$$

$$Y_B=B\times R_B=\{0\ \ 0.03\ \ 0.24\ \ 0.03\ \ 0\}$$

该综合评价向量表示各风险等级对应的风险值，也即资产隶属于各风险等级的概率。通过纵向比较，可以看出，主机A隶属于高风险等级的概率较大。另外，通过横向对比分析，主机A的风险值明显高于主机B。这主要是因为主机A存在超危漏洞，且遭受了渗透攻击，其脆弱性维度和威胁维度风险较高。实验表明，本文所提出的网络安全风险评估方法能够有效评估资产的风险情况。

4 总结

网络安全风险量化评估是一个非常复杂的问题，基于模糊综合评价理论的网络安全风险量化评估方法能够对资产风险做出真实、合理的量化评价，具有很大的发展潜力。本文针对模糊综合评价理论在网络安全领域的应用，在评价因素的权重和隶属度设计方面，提出了客观的分析方法，并通过模拟实验，验证了方案的可行性。本文的研究进一步完善了模糊综合评价方法在网络安全风险量化评估中的应用。

参考文献：

[1] MAYRENA R, TRUSSELL C B, GONZALEZ F, et al. Risk assessment predictive modeling for large collection systems: the L.A. experience[J]. Proceedings of the Water Environment Federation, 2011, 2011(5): 810-813.

[2] 汪楚娇，蒋志雄，王拓，等. 基于模糊数学的网络安全风险评估模型[J]. 网络安全技术与应用，2003(10)：22-25.

[3] 王志平. 基于指标体系的网络安全态势评估研究[D]. 长沙：国防科学技术大学，2010.

[4] 中华人民共和国工业和信息化部. 网络威胁指数评估方法：YD/T 2389-2011[S]. 北京：人民邮电出版社，2012.

[5] MELL P M, SCARFONE K A, ROMANOSKY S. A complete guide to the common vulnerability scoring system version 2.0[EB/OL].[2023-05-10]. https://www. nist. gov/publications/complete-guide-common-vulnerability-scoring-system-version-20.

[6] 贾焰，方滨兴. 网络安全态势感知[M]. 北京：电子工业出版社，2020.

[7] 翁宇. 基于模糊综合评判的教学质量评价方法[J]. 信息系统工程，2011(1)：92-93，97.

[8] 蔡军. 大规模网络安全威胁量化评估系统的研究与实现[D]. 长沙：国防科学技术大学，2009.

[9] 张炳，任家东，王苧. 网络安全风险评估分析方法研究综述[J]. 燕山大学学报，2020，44(3)：290-305.

[10] 王娟，张凤荔，傅翀，等. 网络态势感知中的指标体系研究[J]. 计算机应用，2007，27(8)：1907-1909，1912.

[11] 席荣荣，云晓春，金舒原，等. 网络安全态势感知研究综述[J]. 计算机应用，2012，32(1)：1-4，59.

[12] GARG H, KUMAR K. Some aggregation operators for linguistic intuitionistic fuzzy set and its application to group decision-making process using the set pair analysis[J]. Arabian Journal for Science and Engineering, 2018, 43(6): 3213-3227.

[13] 章宜玉，杨清. 基于模糊层次算法的移动互联网安全态势评估研究[J]. 计算机工程与应用，2016，52(24)：107-111.

[14] 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，2006(4)：885-897.

作者简介：
高贯银，毕业于北京师范大学，硕士，主要从事网络安全相关系统的研发工作；曹京卫，高级工程师，主要从事运营商网络信息安全的规划、建设与运营，网络安全产品、网络安全数据服务产品开发工作；余思阳，毕业于北京邮电大学，工程师，硕士，从事网络安全体系规划及产品研究工作；徐瑶，助理工程师，主要从事网络安全相关的开发、建设工作；杨飞，毕业于合肥学院，高级工程师，学士，主要从事网络安全技术的研究工作。