DOI：10.7652/xjtuxb201308009

应用三角模糊矩阵博弈的网络安全评估研究

高翔，祝跃飞，刘胜利
（解放军信息工程大学数学工程与先进计算国家重点实验室，450002，郑州）

摘要：针对网络攻防双方在攻防博弈分析中无法对双方的损益情况做出准确判断的问题，将三角模糊数的概念引入到博弈模型，用三角模糊数来表示难以用精确数值表示的攻防双方各策略的损益值，并且提出了基于三角模糊矩阵的博弈算法。通过算法复杂度分析，证明了整个算法的时间复杂度可以满足网络安全评估的需求。实例表明，基于该算法生成的策略可以保证攻击者的最低收益为14.44，而对于防御系统，最优的防御是采取安装软件升级补丁的策略，这样可以大大加强主机系统的安全性。与传统的基于博弈论的安全评估方法相比，引入三角模糊概念更加符合实际应用情况，提高了评估结果的准确性和有效性。

关键词：安全评估；三角模糊数；模糊矩阵博弈；网络安全
中图分类号：TP301 **文献标志码**：A **文章编号**：0253-987X(2013)08-0049-05

Network Security Assessment Based on Triangular Fuzzy Matrix Game

GAO Xiang, ZHU Yuefei, LIU Shengli
(State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450002, China)

Abstract: The concept of triangular fuzzy number is introduced into the game model to solve the problem of cannot making accurate judgments on both offense and defense payoffs in game analysis. The payoffs, which are difficult to be described with accurate numbers, are expressed with triangular fuzzy numbers, and the game algorithm based on triangular fuzzy matrix is thus proposed. The complexity analysis verifies the time complexity to meet the requirements of network security assessment. The strategy based on the algorithm can ensure the minimum income of attacker to approach to 14.44; and for the defense system, the best defense strategy that greatly enhances the host system security is to adopt Install Patches. Compared with the traditional security assessments following game theory, introducing the concept of the triangular fuzzy number facilitates suiting the applications and improving the accuracy and validity of assessments.

Keywords: security assessment; triangular fuzzy number; fuzzy matrix game; network security

随着计算机网络的迅猛发展，网络安全问题越来越多地得到人们的关注。传统的安全防御技术（入侵检测、防火墙以及用户认证等）属于被动安全防御，缺乏主动性和对攻击的预测能力，已不能满足人们的需要。为了保证网络的正常运行，国内外学者纷纷致力于研究主动的安全分析与评估方法，目的是主动发现安全隐患，根据评估结果采取对应的措施以减少经济损失，而基于模型的评估方法已经

收稿日期：2012-11-12。 作者简介：高翔（1984—），男，博士生；祝跃飞（通信作者），男，教授。 基金项目：国家自然科学基金资助项目（60902102）；郑州市科技创新团队资助项目（10CXTD150）。
网络出版时间：2013-04-22 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20130422.1539.008.html

成为该领域里的主要研究内容。

目前，常见的基于模型的网络安全评估方法有攻击树模型[1]、攻击图模型[2]、脆弱性状态图[3]、威胁传播模型[4]等，从不同角度分析和评估系统安全，反映了攻击者和网络系统的状态变化。但是，这些模型在对网络攻击进行描述和评估时，多是从网络攻击者的角度来进行攻击建模研究，对攻击起积极作用的因素进行分析研究，而对攻击起抑制作用的防御因素很少涉及。博弈论作为一种决策分析理论，可以从攻击和防御两个方面对网络安全问题进行分析和评价，所以得到广泛应用。文献[5]利用随机博弈形式分析了一个企业网络的安全问题，得到攻击者和防御者双方纳什均衡和各自的最优策略。文献[6]基于完全信息的静态博弈设计并且分析了一种 DDos 防御系统，同时优化了该系统的性能。文献[7]将网络攻防相互博弈的过程看成一种完全信息静态博弈，并建立了一个网络攻防博弈模型。文献[8]针对目前基于博弈的网络安全评价技术大多采用静态博弈，提出一种完全信息动态博弈主动防御模型，借助攻防博弈树分析网络安全问题。

在以上基于博弈论的研究成果中，网络攻防双方通过各自采取不同策略时的损益进行比较分析，得到最优策略。然而，由于人的认知水平有限以及信息的不完全性等因素的影响，使得人们事先无法对攻防双方的损益情况做出准确判断。因此，本文在分析矩阵博弈原理的基础上，将三角模糊数概念引入博弈模型，用三角模糊数来表示难以用精确数值表示的攻防双方各策略的损益值，这样使经典博弈理论扩展到模糊领域，提出了基于三角模糊矩阵的博弈算法，并以一个网络安全评估应用实例进行说明。

1 三角模糊矩阵与博弈算法

博弈论又称对策论，研究理性参与人如何用智慧和机制在竞争冲突的环境下的决策行为，通过数学模型和逻辑推理来探讨局中人的决策行为。

1.1 基本概念

定义 1 博弈论模型可形式化定义为三元组 $\boldsymbol{G}=\{N,S_i,P_i\}$，其中 N 是博弈局中人集合；S_i 是局中人 $i(i\in N)$ 的策略集，指局中人 i 可能采取的可行的策略集合；P_i 是局中人 i 的支付函数，指带给局中人 i 的损益。

定义 2 对于博弈 $\boldsymbol{G}=\{N,S_i,P_i\}$ 的 3 要素，满足下列 3 条件的称为矩阵博弈。

(1)局中人集 $N=\{1,2\}$。

(2)局中人 1 策略集 $S_1=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$ 由有限个策略组成，局中人 2 策略集 $S_2=\{\beta_1,\beta_2,\cdots,\beta_n\}$ 由有限个策略组成。任取 $\alpha_i\in S_1$，$1\leqslant i\leqslant m$，任取 $\beta_j\in S_2$，$1\leqslant j\leqslant n$，则 (α_i,β_j) 构成一个策略组合。

(3)对于一个策略组合 (α_i,β_j)，局中人 1 的期望支付为 $P_1(\alpha_i,\beta_j)$，局中人 2 的期望支付为 $P_2(\alpha_i,\beta_j)$，且满足 $P_1(\alpha_i,\beta_j)+P_2(\alpha_i,\beta_j)=0$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$。

上述矩阵博弈属于非合作博弈，又称为二人有限零和博弈，两个局中人的策略数都是有限的，并且对任意策略组合 (α_i,β_j)，两人的支付和为 0。在网络对抗中，攻击者和防御系统为 2 个局中人，攻击者的得益就是防御系统的损失，防御系统的得益就是攻击者的损失，而双方的策略数有限，可以认为网络对抗是二人有限零和博弈，即矩阵博弈，也可以称为对抗矩阵。

设对抗矩阵为

$$\boldsymbol{A}=(a_{ij})_{m\times n}=\begin{pmatrix}a_{11}&a_{12}&\cdots&a_{1n}\\a_{21}&a_{22}&\cdots&a_{2n}\\\vdots&\vdots&&\vdots\\a_{m1}&a_{m2}&\cdots&a_{mm}\end{pmatrix}$$

矩阵 $\boldsymbol{A}$ 的第 i 行分别与攻击者的策略 α_i 相对应，矩阵 $\boldsymbol{A}$ 的第 j 列分别与防御系统的策略 β_j 相对应，可以令 $a_{ij}=P_1(\alpha_i,\beta_j)$，$1\leqslant i\leqslant m$，$1\leqslant j\leqslant n$。

如果攻击者采用第 i 个策略，则至少可以得到的收益为 $\min\limits_{1\leqslant j\leqslant n}a_{ij}$，即对抗矩阵第 i 行元素中的最小元素，同时希望所得收益越大越好，那么得到的收益不少于 $v_1=\max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n}a_{ij}$。同理，防御系统采用第 j 个策略，则至多可以失去为 $\max\limits_{1\leqslant i\leqslant m}a_{ij}$，即对抗矩阵第 j 列元素中的最大元素，而防御系统希望支付越小越好，那么它的损失不大于 $v_2=\min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m}a_{ij}$。

定义 3 矩阵博弈的纯策略纳什均衡点 (α_i^*,β_j^*) 是指满足如下策略组合

$$a_{ij^*}\leqslant a_{i^*j^*}\leqslant a_{i^*j};i=1,2,\cdots,m;j=1,2,\cdots,n \tag{1}$$

假设有下面对抗矩阵

$$\boldsymbol{A}=\begin{pmatrix}0&1&4\\-1&2&7\\-4&1&8\end{pmatrix}$$

纯策略纳什均衡为 (α_1,β_1)。

定义 4 设有矩阵博弈 $\boldsymbol{G}=\{N,S_i,P_i\}$，其中 $S_1=\{\alpha_1,\alpha_2,\cdots,\alpha_m\}$，$S_2=\{\beta_1,\beta_2,\cdots,\beta_m\}$，则攻击者和防

御系统的混合策略分别为

$$X_m=\left\{\boldsymbol{x}=(x_1,x_2,\cdots,x_m)\mid x_i\geqslant 0,\ i=1,2,\cdots,m,\ \sum_{i=1}^{m}x_i=1\right\}$$

$$Y_n=\left\{\boldsymbol{y}=(y_1,y_2,\cdots,y_n)\mid y_j\geqslant 0,\ j=1,2,\cdots,n,\ \sum_{j=1}^{n}y_j=1\right\}$$

令 $E(\boldsymbol{x},\boldsymbol{y})$为混合策略 $\boldsymbol{x}=(x_1,x_2,\cdots,x_m)$和 $\boldsymbol{y}=(y_1,y_2,\cdots,y_n)$下攻防博弈双方的期望收益。设攻击者和防御系统的期望收益分别为 $E(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$ 和 $-E(\boldsymbol{x},\boldsymbol{y})=\boldsymbol{x}\boldsymbol{A}\boldsymbol{y}^{\mathrm{T}}$，则矩阵博弈的混合策略纳什均衡点$(x^*,y^*)$与下式等价

$$E(\boldsymbol{x},y^*)\leqslant E(x^*,y^*)\leqslant E(x^*,\boldsymbol{y})\quad \forall\boldsymbol{x}\in X_m,\quad \forall\boldsymbol{y}\in Y_n \tag{2}$$

定义 5[9]　称 $M=(l,h,u)$为三角模糊数，如果它的隶属函数为 $\mu_M(\boldsymbol{x}):R\to[0,1]$，即

$$\mu_M(\boldsymbol{x})=\begin{cases}\dfrac{x}{h-l}-\dfrac{l}{h-l}, & x\in[l,h]\\ \dfrac{u}{u-h}-\dfrac{x}{u-h}, & x\in[h,u]\\ 0, & \text{其他}\end{cases}$$

式中：$\boldsymbol{x}\in R$，$l\leqslant h\leqslant u$，l 和 u 分别为 $\boldsymbol{x}$ 的下界和上界，当 $\boldsymbol{x}=h$ 时，$\mu_M(\boldsymbol{x})=1$。三角模糊数对应的隶属度函数如图 1 所示。如估计攻击者的收益的最悲观估计为 10，最乐观估计为 20，且最有可能为 15，记为 $M=(10,15,20)$。

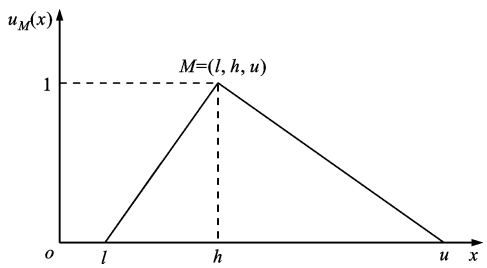

图 1　三角模糊数对应的隶属度函数

在网络攻防博弈中，由于系统本身所具有的模糊性和不确定性，攻防博弈双方的策略多具有模糊性，支付函数 P_i 亦为不精确的模糊数，所以可以定义支付函数 P_i 为三角模糊数的矩阵为三角模糊矩阵。

定义 6[9]　三角模糊数的运算规则。设任意两个三角模糊数 $M_1=(l_1,h_1,u_1)$，$M_2=(l_2,h_2,u_2)$，其模糊运算规则如下。

(1)加法运算

$$M_1\oplus M_2=(l_1+l_2,h_1+h_2,u_1+u_2)$$

(2)减法运算

$$M_1\Theta M_2=(l_1-l_2,h_1-h_2,u_1-u_2)$$

(3)乘法运算

$$M_1\cdot M_2=(l_1\cdot l_2,h_1\cdot h_2,u_1\cdot u_2)$$

定义 7　系统的损失代价 S_{DC} 表示某类攻击对系统资源的损害程度，这里可以认为攻击者获得的收益即为防御系统的损失。本文将系统安全属性的损害分为完整性代价 C_{i}、机密性代价 C_{c} 和可用性代价 C_{a}，用$(P_{\mathrm{i}},P_{\mathrm{c}},P_{\mathrm{a}})$来表示对这 3 种安全属性代价的偏重，并且满足 $P_{\mathrm{i}}+P_{\mathrm{c}}+P_{\mathrm{a}}=1$。安全属性代价用三角模糊数来表示，损益代价的高、中、低分别表示为 30～20、20～10、10～0。攻击者对主机系统造成的损失为

$$S_{\mathrm{DC}}=C_{\mathrm{i}}P_{\mathrm{i}}+C_{\mathrm{c}}P_{\mathrm{c}}+C_{\mathrm{a}}P_{\mathrm{a}} \tag{3}$$

参考麻省理工学院林肯实验室的攻击分类，攻击者的策略 α_i 以及安全属性代价的偏重见表 1。

表 1　攻击策略以及安全属性代价的偏重

策略	描述	P_{i}	P_{c}	P_{a}
Root	获取管理员权限	0.2	0.4	0.4
User	获取普通用户权限	0.2	0.4	0.4
Data	非授权访读写数据	0.3	0.4	0.3
DOS	拒绝服务攻击	0.0	0.0	1.0
Probe	扫描攻击	0.0	1.0	0.0

定理 1[10]　矩阵博弈中，纯策略纳什均衡点存在的充分必要条件为

$$v_1=\max_{1\leqslant i\leqslant m}\min_{1\leqslant j\leqslant n}a_{ij}=\min_{1\leqslant j\leqslant n}\max_{1\leqslant i\leqslant m}a_{ij}=v_2$$

另外，对任一个矩阵博弈，纯策略纳什均衡点不一定存在，若存在，它不一定唯一。

定理 2[10]　矩阵博弈中，混合策略纳什均衡点存在的充分必要条件为

$$v_1=\max_{x\in X_m}\min_{y\in Y_n}E(\boldsymbol{x},\boldsymbol{y})=\min_{y\in Y_n}\max_{x\in X_m}E(\boldsymbol{x},\boldsymbol{y})=v_2$$

定理 3[10]　对任一个矩阵博弈 $\boldsymbol{G}=\{N,S_i,P_i\}$，一定存在混合策略纳什均衡。

1.2　基于三角模糊矩阵的博弈算法

三角模糊矩阵 $\boldsymbol{A}$ 中元素 a_{ij} 的取值通过式(3)计算得到。博弈算法首先要将矩阵中的三角模糊数转化为非模糊数，即将三角模糊矩阵转化为常规矩阵。这里采用模糊概率处理三角模糊数[11]，即在网络对抗中，攻防双方的损益用 l、h、u 和模糊概率来描述。

根据 l、h、u 的偏离程度来确定模糊概率，以 h 为界分等概率情况来考虑。由 l 和 h 的偏离程度，

确定攻防损益是 h 的可能性为 l 的 N 倍，同样由 h 和 u 的偏离程度，确定攻防损益是 h 的可能性为 u 的 M 倍，则 l、h、u 的模糊概率分别为

$$\left.\begin{aligned} p_{ij}(l_{ij}) &= \frac{1}{2(1+N)} \\ p_{ij}(h_{ij}) &= \frac{N+2NM+M}{2(1+N)(1+M)} \\ p_{ij}(u_{ij}) &= \frac{1}{2(1+M)} \end{aligned}\right\} \tag{4}$$

基于三角模糊矩阵的博弈算法如下。

输入：三角模糊矩阵 $\boldsymbol{A}$。

输出：纳什均衡。

Step1：由式(4)计算三角模糊数的模糊概率。

Step2：将三角模糊数转化为非模糊数，则 a_{ij} 的期望值为

$$a_{ij} = E_{ij}(l_{ij},h_{ij},u_{ij}) = p_{ij}(l_{ij})l_{ij} + p_{ij}(h_{ij})h_{ij} + p_{ij}(u_{ij})u_{ij}$$

由 a_{ij} 构成非模糊矩阵 $\boldsymbol{A}=(a_{ij})_{m\times n}$。

Step3：令 $v_1 = \max\limits_{1\leqslant i\leqslant m}\min\limits_{1\leqslant j\leqslant n} a_{ij}$，$v_2 = \min\limits_{1\leqslant j\leqslant n}\max\limits_{1\leqslant i\leqslant m} a_{ij}$，根据定义 3，若 $v_1=v_2$，则存在纯策略纳什均衡点，纯策略纳什均衡为 (α_i,β_j)；若 $v_1\neq v_2$，转 Step4。

Step4：由于在矩阵博弈中，一定存在混合策略纳什均衡，本文采用线性规划方法求解。求解过程如下。

(1) Maximize v_3

(2) Subject to

(3) for all $x\in X_m$

(4) $\sum\limits_{i=1}^{m} a_{ij}x_i \geqslant v, j=1,\cdots,n$

(5) $\sum\limits_{i=1}^{m} x_i = 1, x_i \geqslant 0, i=1,\cdots,m$

(6) Minimize v_4

(7) Subject to

(8) for all $y\in Y_n$

(9) $\sum\limits_{i=1}^{m} a_{ij}y_j \leqslant v, i=1,\cdots,m$

(10) $\sum\limits_{j=1}^{n} y_j = 1, x_j \geqslant 0, j=1,\cdots,n$

Step5：判断 v_3 和 v_4 的取值大小，若 $v_3=v_4$，则混合策略组合 (x^*,y^*) 为三角模糊矩阵 $\boldsymbol{A}$ 的解。

1.3 算法复杂度分析

基于三角模糊矩阵的博弈算法主要目的是计算出该矩阵的纳什均衡。算法复杂度分析可分为 3 个部分进行：①将三角模糊数转化为非模糊数，该过程是将矩阵 $\boldsymbol{A}=(a_{ij})_{m\times n}$ 中的全部元素转化为非模糊数，因此其算法复杂度为 $O(mn)$；②矩阵 $\boldsymbol{A}$ 若存在纯策略纳什均衡点则进行求解，由上述纯策略的计算过程可知，需要对各行或各列中的元素进行最大、最小比较，因此其算法复杂度为 $O(m+n+2)$；③利用非线性规划求解混合策略纳什均衡，已经证明该算法复杂度是多项式时间。由以上分析可见，整个算法的时间复杂度可以满足网络安全评估的需求。

2 网络安全评估应用示例

以一个主机安全防护系统为例，攻击者和防御系统都是该博弈的局中人。攻击者的策略 α_i 可以参照表 2，防御系统的策略 β_j 有多种方法，如关闭服务、安装软件升级补丁、系统病毒扫描、丢弃可疑数据包等。

确定攻击者和防御系统采用的策略后，根据式(3)计算各个攻防策略下主机系统的损失，损失代价用三角模糊数来表示，这里系统的损失代价即为攻击者的得益，得到攻击者收益矩阵如表 2 所示。例如攻击策略 Root 和防御策略中关闭服务的博弈结果，攻击者的收益可能为 9～12，且最有可能的收益为 10。

表 2 攻击者收益矩阵

策略	攻击者收益			
	关闭服务	安装软件升级补丁	系统病毒扫描	丢弃可疑数据包
Root	(9,10,12)	(9,10,12)	(15,18,20)	(22,26,30)
User	(9,10,12)	(9,10,12)	(17,18,19)	(16,18,20)
Data	(12,14,16)	(8,10,12)	(9,10,12)	(21,24,26)
DOS	(10,12,14)	(15,18,20)	(26,28,30)	(8,10,12)
Probe	(15,18,20)	(14,15,16)	(13,15,17)	(9,10,11)

根据 1.2 节的方法将三角模糊数转化为非模糊数，由相关专家给出的判断以及经验数值，认为 h_{ij} 出现的可能性是 l_{ij}、u_{ij} 的 2 倍，则确定模糊概率分别为 $p_{ij}(l_{ij})=\frac{1}{6}$、$p_{ij}(h_{ij})=\frac{4}{6}$、$p_{ij}(u_{ij})=\frac{1}{6}$，得到转化后的收益矩阵如表 3 所示。

根据博弈算法可知，矩阵博弈不存在纯策略纳什均衡，但是一定存在混合策略纳什均衡。通过计算得到混合策略纳什均衡为 $x_m=(0,0,0.32,0.37,0.31)$，$y_n=(0.24,0.51,0,0.25)$。即攻击者最优的攻击策略是以概率 0.32 选择策略 Data，以概率 0.37 选择策略 DOS，以概率 0.31 选择策略 Probe；

防御系统最优的防御策略是以概率 0.24 选择策略关闭服务，以概率 0.51 选择策略安装软件升级补丁，以概率 0.25 选择策略丢弃可疑数据包。此策略保证攻击者的最低收益为 14.44，而对于防御系统来说，最优的防御策略是采取安装软件升级补丁，这样可以大大加强主机系统的安全性。

表 3　转化后的收益矩阵

策略	转化后的收益			
	关闭服务	安装软件升级补丁	系统病毒扫描	丢弃可疑数据包
Root	10.17	10.17	17.83	26.00
User	10.17	10.17	18.00	18.00
Data	14.00	10.00	10.17	23.83
DOS	12.00	17.83	28.00	10.00
Probe	17.83	15.00	15.00	10.00

3　结　论

网络安全评估技术是保障网络和信息系统安全的基础，目前博弈论相关理论被越来越广泛地应用于其中。本文对以三角模糊数形式给出的矩阵博弈进行了研究，提出了基于三角博弈矩阵的博弈算法，并以一个网络攻防博弈实例来进行验证。实验结果表明，引入三角模糊概念更加符合实际应用情况，防御者可以选择最优的防御代价来进行主动防御，从而对实际网络及时有效地主动防御和安全管理提供了有力保证。

参考文献：

[1] SCHNEIER B. Attack trees [J]. Dr. Dobb' Journal, 1999,24(12):21-29.

[2] 吴金宇，金舒原，杨智. 基于网络流的攻击图分析方法 [J]. 计算机研究与发展，2011,48(8):1497-1505.
WU Jinyu, JIN Shuyuan, YANG Zhi. Analysis of attack graphs based on network flow method [J]. Journal of Computer Research and Development, 2011,48(8):1497-1505.

[3] 冯萍慧，连一峰，戴英侠，等. 面向网络系统的脆弱性利用成本估算模型 [J]. 计算机学报，2006,29(8):1375-1381.
FENG Pinghui, LIAN Yifeng, DAI Yingxia, et al. An evaluation model of vulnerability exploitation cost for network system [J]. Chinese Journal of Computers, 2006,29(8):1375-1381.

[4] 陈锋，刘德辉，张怡，等. 基于威胁传播模型的层次化网络安全评估方法 [J]. 计算机研究与发展，2011,48(6):945-954.
CHEN Feng, LIU Dehui, ZHANG Yi, et al. A hierarchical evaluation approach for network security based on threat spread model [J]. Journal of Computer Research and Development, 2011,48(6):945-954.

[5] LYE K, WING J M. Game strategies in network security [J]. International Journal of Information Security, 2005,4(1):71-86.

[6] XU J, LEE W. Sustaining availability of Web services under distributed denial of service attacks [J]. IEEE Transactions on Computers, 2003,52(4):195-208.

[7] 姜伟，方滨兴，田志宏，等. 基于攻防博弈模型的网络安全评测和最优主动防御 [J]. 计算机学报，2009,32(4):817-827.
JIANG Wei, FANG Binxing, TIAN Zhihong, et al. Evaluating network security and optimal active defense based on attack-defense game model [J]. Chinese Journal of Computers, 2009,32(4):817-827.

[8] 林旺群，王慧，刘家红，等. 基于非合作动态博弈的网络安全主动防御技术研究 [J]. 计算机研究与发展，2011,48(2):306-316.
LIN Wangqun, WANG Hui, LIU Jiahong, et al. Research on active defense technology in network security based on non-cooperative dynamic game theory [J]. Journal of Computer Research and Development, 2011,48(2):306-316.

[9] 吴诗辉，杨建军，郭乃林. 三角模糊矩阵博弈的最优策略研究 [J]. 系统工程与电子技术，2009,31(5):1231-1234.
WU Shihui, YANG Jianjun, GUO Nailin. Study on the optimal strategies solution of triangular fuzzy matrix game [J]. Systems Engineering and Electronics, 2009,31(5):1231-1234.

[10] 汪贤裕. 博弈论及其应用 [M]. 北京：科学出版社，2008:60-68.

[11] 肖钰，李华. 基于三角模糊数的判断矩阵的改进及其应用 [J]. 模糊系统与数学，2003,17(2):59-64.
XIAO Yu, LI Hua. Improvement on judgement matrix based on triangle fuzzy number [J]. Fuzzy Systems and Mathematics, 2003,17(2):59-64.

（编辑　杜秀杰　赵大良）