文章编号：1000-8608(2020)03-0306-11

面向风险评估的关键系统识别

杨宏宇*，秦　赓

（中国民航大学 计算机科学与技术学院，天津　300300）

摘要：为有效识别关键业务系统并评估业务系统对全业务流程造成的安全风险和影响，提出一种全业务流程关键业务系统识别模型.首先，建立业务流程关联树与业务流程关联网络，得到评价属性矩阵与系统关联度矩阵.其次，由评价属性矩阵与系统关联度矩阵构造关联评价属性矩阵，改进优劣解距离法(technique for order preference by similarity to an ideal solution，TOPSIS)中加权方法和相对接近度计算方法，基于TOPSIS改进方法计算业务系统的重要性系数，进而识别全业务流程中关键业务系统.最后，评估业务系统发生信息安全事件时对全业务流程连续性的影响.实验结果表明，该方法能够准确地识别出全业务流程中的关键业务系统，有助于高效评估业务系统对全业务流程造成的影响.

关键词：业务流程；风险评估；业务系统；TOPSIS；系统识别

中图分类号：TP309　　**文献标识码：**A　　**doi：**10.7511/dllgxb202003012

0　引　言

系统风险评估是对业务系统所面临的威胁与可能给业务流程带来的影响进行分析，根据系统遭受威胁后性能指标的变化大小评估得到系统面临风险的情况.在一个系统中，每个子系统和业务环节的安全性是影响全业务流程连续性的主要因素之一，为了提高系统风险评估的针对性和有效性，必须从全系统业务流程中识别和分析关键系统.目前大多数研究的对象为单一系统[1-2]，但网络攻击的主要目标是系统业务流程中的关键系统，这些系统可以运行在路由器、交换机与服务器等网络设备中[3-4].因此，如何识别全业务流程中的关键系统，并对其安全性进行分析已经成为系统安全领域的研究热点.

Belov等[5]提出了一种面向业务系统的评估模型，将业务系统中资产重要性作为参数，评估系统发生信息安全事件时业务流程所面临的风险，但是该方法在设置参数时具有一定的主观性，影响最终评估结果.业务系统的安全性由许多评价属性决定，优劣解距离法(technique for order preference by similarity to an ideal solution，TOPSIS)、秩和比法与综合指数法作为多属性决策的重要方法已经在机械生产[6]、军事分析[7]和经济学[8]等领域广泛应用，且已有将其应用到系统安全评估方面的研究成果.Wang等[9]通过改进TOPSIS中的加权方法，降低权重误差，评估系统安全等级，但该方法独立评估每个系统，忽略了系统之间的关联性.Zhang等[10]在TOPSIS方法中引入双极容度理论，虽然解决了评价属性之间的关联问题，但是忽略了系统之间的关联性.Li等[11]利用灰色关联度算法快速识别关键网络节点，但该方法需要给出最优参考目标，影响最终结果.Yang等[12]提出了一种基于秩和比法的评估模型，评估目标节点变化前后的系统安全性，但节点变化时会改变原有连接方式.Karuppasamy等[13]利用秩和比法分析目标节点性能并识别关键节点，对目标样本具有很好的识别效果，但该方法没有考虑目标之间的关联性.Hamamreh等[14]通过综合指数法对网络物理层进行安全风险评估，但该方法没有对网络节点加权，导致评估结果不理想.上述研究方法没有考虑业务系统间的关联性，且加权方法较主观，导致识别结果不够准确，不能有效解决对关键系统的识别、安全性分析

收稿日期：2020-01-08；　**修回日期：**2020-04-09.
基金项目：国家自然科学基金资助项目(U1833107).
作者简介：杨宏宇*(1969-)，男，博士，教授，E-mail：yhyxlx@hotmail.com；秦　赓(1992-)，男，硕士生，E-mail：qingeng6611@qq.com.

和对全系统业务流程的风险评估等问题.

一个复杂系统的全业务流程包含多个业务系统，业务系统作为支撑全业务流程稳定连续运行的主体，其安全性对业务流程能否正常运行起到了关键作用. 一个复杂业务系统一般由多个系统组成，其中关键系统是最重要的业务系统，其遭受攻击后带来的影响比其他系统更严重，与评估所有系统相比，识别并分析关键系统更具有针对性，能够为风险评估提供更有效的目标支持. 为此，本文提出一种面向风险评估的全业务流程关键系统识别方法，通过构建业务流程关联树和业务流程关联网络，改进 TOPSIS 中的加权方法与相对接近度计算方法，基于 TOPSIS 的改进方法计算出系统重要性系数，进而识别关键业务系统.

1　关键系统识别模型

关键系统识别模型由关联建立模块、数据获取与处理模块、关键系统识别模块和系统分析模块组成. 该模型的流程如图 1 所示.

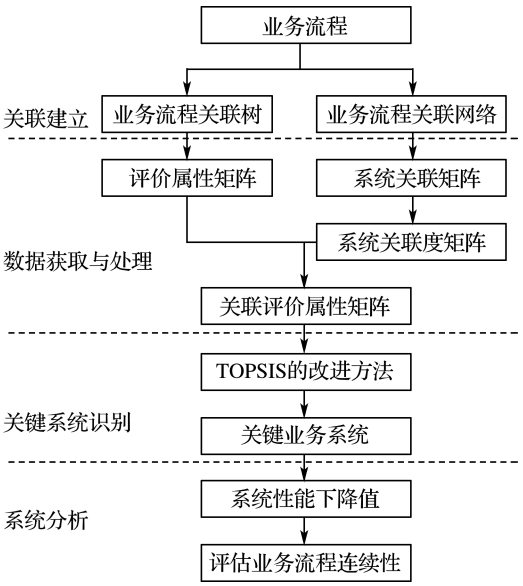

图 1　关键系统识别流程

Fig. 1　Key system identification process

1.1　关联建立

建立业务流程关联树具体方法如下：

(1)获取业务流程下包含的所有业务系统.

(2)确定业务系统的评价属性.

(3)建立关联树，将业务流程作为树的根节点，业务系统作为业务流程的孩子节点，评价属性作为关联树的叶节点，得到业务流程关联树(图 2).

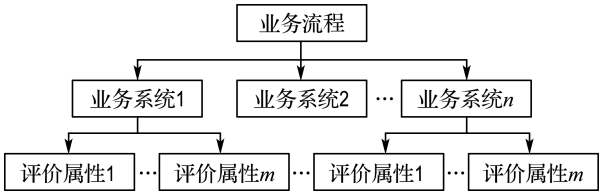

图 2　业务流程关联树

Fig. 2　Business process association tree

建立业务流程关联网络具体方法如下：

(1)将业务系统抽象为一组节点.

(2)若业务系统之间有数据交换，则认为这些业务系统之间存在关联，用一条有向边将存在关联的业务系统相连，有向边指向接收数据信息的业务系统.

(3)将全业务流程中所有存在关联的业务系统相连，得到业务流程关联网络(图 3).

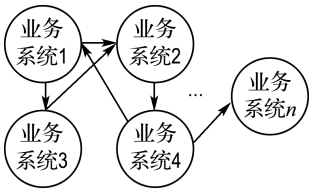

图 3　业务流程关联网络

Fig. 3　Business process association network

1.2　数据获取与处理

建立业务流程关联树与业务流程关联网络后，通过获取评价属性的取值，进一步建立评价属性矩阵与系统关联矩阵. 根据系统关联矩阵建立系统关联度矩阵，最后得到关联评价属性矩阵.

在数据获取与处理模块，将图形信息转化为数字信息.

(1)获取评价属性矩阵

系统的安全性受诸多评价属性影响，无法逐一讨论，故本文选取主要的评价属性作为评估系统安全性的依据. 根据《信息安全技术　信息系统安全等级保护基本要求》(GB/T 22239—2008)，本文将数据、设备与系统访问量作为影响业务系统安全性的评价属性.

①数据评价属性取值方法

从可用性、完整性和保密性 3 方面对数据评价属性进行分析. 对可用性、完整性和保密性进行划分，并为其赋值. 数据安全属性结构如图 4 所示，赋值结果如表 1 所示.

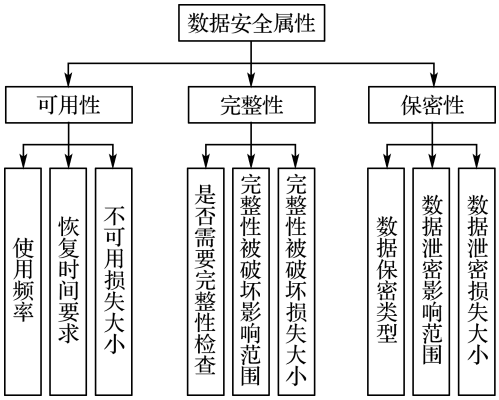

图 4 数据安全属性分类

Fig. 4 Data security attribute classification

表 1 数据安全属性取值

Tab. 1 Data security attribute value

安全属性	类别	描述	取值
可用性 A	使用频率 A_1	低	0.25
		一般	0.50
		频繁	0.75
		非常频繁	1.00
	恢复时间要求 A_2	大于 10 min	0.25
		3～10 min	0.50
		小于 3 min	0.75
		实时切换	1.00
	不可用损失大小 A_3	间接损失	0.25
		较小	0.50
		中等	0.75
		较大	1.00
完整性 I	是否需要完整性检查 I_1	不需要	0
		需要	1.00
	完整性被破坏影响范围 I_2	内部	0.50
		外部	1.00
	完整性被破坏损失大小 I_3	间接损失	0.25
		较小	0.50
		中等	0.75
		较大	1.00
保密性 S	数据保密类型 S_1	公开	0.25
		内部	0.50
		敏感	0.75
		高敏感	1.00
	数据泄密影响范围 S_2	内部	0.50
		外部	1.00
	数据泄密损失大小 S_3	间接损失	0.25
		较小	0.50
		中等	0.75
		较大	1.00

将业务系统中的数据评价属性根据表 1 进行赋值，可得到业务系统数据安全属性矩阵：

$$\boldsymbol{D}=\begin{pmatrix} A_1 & A_2 & A_3 \\ I_1 & I_2 & I_3 \\ S_1 & S_2 & S_3 \end{pmatrix}$$

利用式(1)计算业务系统数据评价属性取值：

$$d=\frac{1}{9}\sum_{i=1}^{3}(A_i+I_i+S_i) \tag{1}$$

②设备评价属性取值方法

假设设备的健壮性为 H，将设备的健壮性作为系统中设备评价属性的取值. 设备健壮性计算公式如下：

$$H=H_0\,\mathrm{e}^{b(t_2-t_1)} \tag{2}$$

式中：H_0 为设备在投入使用时的初始健壮性，取值为 1.65；b 为设备老化系数；t_2 是设备在投入使用时的时间，t_1 是当前时间.

设备老化系数 b 与设备的预期使用时间有关，其计算公式如下：

$$b=(\ln H_\mathrm{e}-\ln H_0)/t_\mathrm{exp} \tag{3}$$

式中：H_e 为设备在报废时的健壮性，取值为 6.5；t_exp为设备的预期使用时间，其取值与设备的设计寿命、CPU 使用率、物理内存使用率有关，计算公式如下：

$$t_\mathrm{exp}=t_\mathrm{d}/f_1 f_\mathrm{e} \tag{4}$$

其中 t_d 为设备的设计寿命，f_1 为设备使用时 CPU 负荷系数，f_e 为设备使用时的内存系数. 具体取值如表 2 所示.

表 2 CPU 负荷系数与内存系数取值

Tab. 2 CPU load factor and memory factor value

CPU 使用率/%	CPU 负荷系数	内存使用率/%	内存系数
0～40	1.00	0～25	0.80
40～60	1.05	25～40	1.00
60～70	1.10	40～60	1.05
70～80	1.25	60～80	1.15
80～100	1.60	80～100	1.30

③系统访问量评价属性取值方法

根据当前系统访问量 V_now 与系统最大访问量 V_max 的比值将系统工作状态划分为 4 个等级，本文用二进制表示，1000 表示 1，1100 表示 2，1110 表示 3，1111 表示 4. 然后，通过矩阵计算得到系统当前访问量对系统的影响值，并作为系统访问量评价属性的取值. 系统状态等级划分如表 3 所示.

表 3　系统状态等级

Tab. 3　System status level

等级	二进制取值	描述
1	1000	$0<V_{now}/V_{max}\leqslant 0.2$，系统空闲
2	1100	$0.2<V_{now}/V_{max}\leqslant 0.5$，系统正常
3	1110	$0.5<V_{now}/V_{max}\leqslant 0.7$，系统繁忙
4	1111	$V_{now}/V_{max}>0.7$，系统拥挤

设矩阵 $\boldsymbol{C}$ 代表系统访问量的实际取值，矩阵 $\boldsymbol{R}$ 代表系统访问量的最大取值，矩阵 $\boldsymbol{M}$ 代表系统访问量的最小取值. 根据系统状态等级划分表的二进制取值，建立矩阵并计算系统访问量评价属性的取值，其取值过程如下：

首先，将矩阵 $\boldsymbol{C}$ 与矩阵 $\boldsymbol{R}$ 中的每一位相对应，进行异或运算，得到矩阵 $\boldsymbol{Q}$.

其次，将矩阵 $\boldsymbol{M}$ 与矩阵 $\boldsymbol{R}$ 中的每一位相对应，进行异或运算，得到矩阵 $\boldsymbol{U}$.

最后，将矩阵 $\boldsymbol{Q}$ 转置，从而得到矩阵 $\boldsymbol{Q}^{\mathrm{T}}$. 同理，得到矩阵 $\boldsymbol{U}^{\mathrm{T}}$，利用式(5)得到系统访问量评价属性的取值：

$$V_{imp}=\sqrt{\mathrm{tr}(\boldsymbol{Q}\boldsymbol{Q}^{\mathrm{T}})}\,/\,\sqrt{\mathrm{tr}(\boldsymbol{U}\boldsymbol{U}^{\mathrm{T}})} \tag{5}$$

其中 tr 为求矩阵的迹运算.

假设 V_{now}/V_{max} 的比值分别为 0.18、0.28、0.36 和 0.58，由表 3 可得矩阵 $\boldsymbol{C}$、$\boldsymbol{R}$、$\boldsymbol{M}$，则上述步骤矩阵计算过程如下：

$$\boldsymbol{C}=\begin{pmatrix}1&0&0&0\\1&1&0&0\\1&1&0&0\\1&1&1&0\end{pmatrix},\ \boldsymbol{R}=\begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}$$

$$\boldsymbol{M}=\begin{pmatrix}1&0&0&0\\1&0&0&0\\1&0&0&0\\1&0&0&0\end{pmatrix},\ \boldsymbol{Q}=\begin{pmatrix}0&1&1&1\\0&0&1&1\\0&0&1&1\\0&0&0&1\end{pmatrix}$$

$$\boldsymbol{U}=\begin{pmatrix}0&1&1&1\\0&1&1&1\\0&1&1&1\\0&1&1&1\end{pmatrix},\ \boldsymbol{Q}^{\mathrm{T}}=\begin{pmatrix}0&0&0&0\\1&0&0&0\\1&1&1&0\\1&1&1&1\end{pmatrix}$$

$$\boldsymbol{U}^{\mathrm{T}}=\begin{pmatrix}0&0&0&0\\1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix}$$

$$\mathrm{tr}(\boldsymbol{Q}\boldsymbol{Q}^{\mathrm{T}})=\mathrm{tr}\begin{pmatrix}3&2&2&1\\2&2&2&1\\2&2&2&1\\1&1&1&1\end{pmatrix}=8$$

$$\mathrm{tr}(\boldsymbol{U}\boldsymbol{U}^{\mathrm{T}})=\mathrm{tr}\begin{pmatrix}3&3&3&3\\3&3&3&3\\3&3&3&3\\3&3&3&3\end{pmatrix}=12$$

$$V_{imp}=\sqrt{8}\,/\,\sqrt{12}=0.82$$

根据上述各评价属性的取值方法，得到数据、设备与系统访问量评价属性的取值，建立评价属性矩阵：

$$\boldsymbol{P}=\begin{pmatrix}p_{11}&p_{12}&\cdots&p_{1m}\\p_{21}&p_{22}&\cdots&p_{2m}\\\vdots&\vdots&&\vdots\\p_{n1}&p_{n2}&\cdots&p_{nm}\end{pmatrix}$$

其中 $0\leqslant p_{nm}\leqslant 1$. p_{nm} 为第 n 个业务系统第 m 个评价属性的数值，数值越接近 0 表示该评价属性越差；同理，数值越接近 1 表示该评价属性越好.

(2)获取系统关联矩阵

由业务流程关联网络可知业务系统之间是否存在关联，将业务系统抽象为节点，若存在从节点 i 出发指向节点 j 的有向边，则表示节点 i 到节点 j 有关联. 假设 T_{ij} 表示节点 i 到节点 j 之间的关联关系，$T_{ij}=0$ 代表节点 i 到节点 j 无关联，$T_{ij}=1$ 代表节点 i 到节点 j 有关联，得到系统关联矩阵 $\boldsymbol{T}$.

(3)获取系统关联度矩阵

根据业务流程关联网络，将图中以节点作为边终点的次数之和称为节点的入度，节点作为边始点的次数之和称为节点的出度. 假设 N 代表节点的入度，O 代表节点的出度.

假设节点 i 入度和出度之和与所有节点入度和出度之和的比值作为节点 i 的关联度 g_i，取值为[0,1]，其值越大表示节点 i 与其他节点的关联程度越大，值越小表示节点 i 与其他节点的关联程度越小.

系统关联度矩阵 $\boldsymbol{G}$ 计算步骤如下：

首先，使用式(6)～(8)得到节点 i 的关联度 g_i.

其次，由于节点 i 的关联度只与自身的入度和出度有关，故将得到的 g_i 作为对角线元素放到系统关联度矩阵 $\boldsymbol{G}$ 中，得到系统关联度矩阵 $\boldsymbol{G}$.

$$N_j=\sum_{i=1}^{n}T_{ij};\ j=1,2,\cdots,m \tag{6}$$

$$O_i=\sum_{j=1}^{m}T_{ij};\ i=1,2,\cdots,n \tag{7}$$

$$g_i=\frac{O_i+N_j}{\sum_{i=1}^{n}O_i+\sum_{j=1}^{m}N_j} \tag{8}$$

$$\boldsymbol{G}=\mathbf{diag}\{g_1,g_2,\cdots,g_n\}$$

(4)获取关联评价属性矩阵

由于全业务流程中存在多个业务系统,且各个业务系统之间存在关联关系,不能单独用评价属性矩阵 $\boldsymbol{P}$ 代表全业务流程业务系统的评价结果,因此将评价属性矩阵与系统关联度矩阵结合得出关联评价属性矩阵,用关联评价属性矩阵作为全业务流程业务系统的评价结果.

将关联评价属性矩阵作为 TOPSIS 改进方法的输入,进而识别关键系统.

1.3 关键系统识别与分析

在关键系统识别模块,使用 TOPSIS 改进方法得出系统重要性系数,进而识别关键系统.重要性系数越大代表该业务系统重要程度越高.

在系统分析模块,通过计算系统性能下降值评估系统发生信息安全事件时业务流程的连续性.

信息安全事件是指由于人为、软硬件、自然灾害等情况对系统或者其中的数据造成不可逆的影响,且对社会造成负面影响的网络安全事件.

业务系统在发生信息安全事件时会威胁到业务流程的连续性,从而对业务流程造成一定的影响.示意图如图 5 所示.

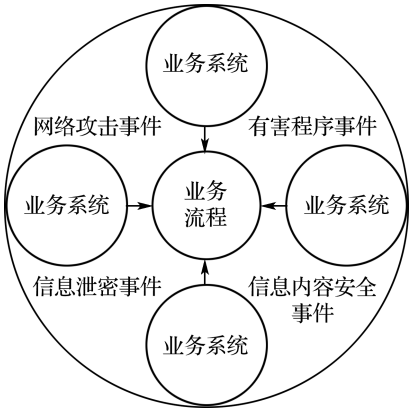

图 5 信息安全事件威胁示意图

Fig. 5 Schematic diagram of information security event threat

设业务系统某一时刻的性能集合由 $H_z(\alpha,\beta,\gamma)$ 表示,性能参数在正常情况下最大值为 $H_{\max}(\alpha_{\max},\beta_{\max},\gamma_{\max})$,其取值为 $H_{\max}(1\ 000,1,1)$.其中 α 代表并发用户数,β 代表资源利用率,γ 代表响应时间.假设业务系统在发生信息安全事件后某 t_1 时刻性能参数为 $H_1(\alpha_1,\beta_1,\gamma_1)$,某 t_2 时刻性能参数为 $H_2(\alpha_2,\beta_2,\gamma_2)$,则利用式(9)、(10)可得这段时间业务系统的性能下降值:

$$P_{H_z}=1-\frac{1}{3}\sum_{z=1}^{2}(H_z/H_{\max}) \tag{9}$$

$$\Delta P_H=P_{H_1}-P_{H_2} \tag{10}$$

若 $\gamma\gg\gamma_{\max}$,则 $P_{H_z}=0$.可知 $0\leqslant P_{H_z}\leqslant 1$.

业务系统在发生信息安全事件后,全业务流程不仅会在短时间内面临较高的安全风险,也会导致业务流程连续性下降,假设业务流程的连续性为 P_s,则

$$P_s=S_e\Delta P_H \tag{11}$$

其中 S_e 代表业务系统重要性系数.S_e 的计算方法将在 2.3 详细阐述.

2 TOPSIS 改进方法

2.1 问题分析

业务流程中具有多个业务系统,而这些业务系统的安全性由许多评价属性决定.秩和比法、综合指数法与 TOPSIS 是多属性决策分析的常用方法.秩和比法在指标转化时会使信息发生改变且无法正确区分优劣指标.综合指数法在使用时必须使用同向指标.TOPSIS 对初始数据没有要求且能准确区分优劣指标,故本文选取 TOPSIS 方法并对其进行改进.不同评价属性的数据类型不同,对于数字型数据,都可以将数字型数据转换成矩阵并利用 TOPSIS 改进方法求解.对于非数字型数据,如文本型数据、字节型数据等,都需要转换成数字型数据才能使用本文模型,其中转换方法并不是本文所研究的内容.由于影响业务系统安全性的评价属性大多属于数字型数据,故本文模型有很好的泛化能力且能够将本文模型应用到业务系统安全性研究.

针对 TOPSIS 中加权方法较主观与相对接近度计算方法不准确的问题,本文对其进行改进.

2.2 加权方法改进

在运用 TOPSIS 时,需要预先设定各评价属性的权值,人为权值设定存在一定的主观性,影响识别结果.本文将熵权法、变异系数法和先验估计法相结合,提出一种综合加权方法.

(1)熵权法步骤如下:

①计算信息熵

计算每个系统中各评价属性占整体的比重:

$$y_{ij}=p_{ij}\Big/\sum_{i=1}^{n}p_{ij} \tag{12}$$

其中 p_{ij} 代表第 i 个系统中第 j 个评价属性的取值.

然后,计算第 j 个评价属性的信息熵:

$$e_j=-\theta\sum_{i=1}^{n}p_{ij}\ln p_{ij} \tag{13}$$

其中 θ 为常量,$\theta=1/\ln m$.

②计算权值

$$w_{1j}=(1-e_j)\Big/\sum_{j=1}^{m}(1-e_j) \tag{14}$$

(2)变异系数法步骤如下:

计算出评价属性的标准差 σ 与平均值 μ,则第 j 个评价属性的变异系数 C_j 可由式(15)求得:

$$C_j=\sigma_j/\mu_j \tag{15}$$

其中 σ_j 代表第 j 个评价属性的标准差,μ_j 代表第 j 个评价属性的平均值.得到评价属性的变异系数后,用式(16)计算权值.

$$w_{2j}=C_j\Big/\sum_{j=1}^{m}C_j \tag{16}$$

(3)先验估计法根据以往加权经验为评价属性加权.

分别用熵权法、变异系数法和先验估计法为评价属性加权,第 j 个评价属性的综合权值为

$$w_j=\frac{1}{3}\sum_{j=1}^{m}(w_{1j}+w_{2j}+w_{3j}) \tag{17}$$

式中:w_{1j} 为熵权法对第 j 个评价属性的加权结果,w_{2j} 为变异系数法对第 j 个评价属性的加权结果,w_{3j} 为先验估计法对第 j 个评价属性的加权结果.

2.3　相对接近度修正

业务系统之间存在关联,但 TOPSIS 计算出的相对接近度仅表示距离上的相对接近,且评价属性之间存在离散性.本文引入离散系数 c 来修正相对接近度.

使用式(18)、(19)计算正理想解 y^+ 和负理想解 y^-,再用式(20)～(22)计算业务系统到正、负理想解的相对接近度 L_i.

$$y^+=\{\max_{1\leqslant i\leqslant n}p_{ij}\,|\,j\in J^+,\min_{1\leqslant i\leqslant n}p_{ij}\,|\,j\in J^-\}=\{y_1^+,y_2^+,\cdots,y_m^+\} \tag{18}$$

$$y^-=\{\min_{1\leqslant i\leqslant n}p_{ij}\,|\,j\in J^+,\max_{1\leqslant i\leqslant n}p_{ij}\,|\,j\in J^-\}=\{y_1^-,y_2^-,\cdots,y_m^-\} \tag{19}$$

$$D_i^+=\sqrt{\sum_{j=1}^{m}(p_{ij}-y_j^+)^2} \tag{20}$$

$$D_i^-=\sqrt{\sum_{j=1}^{m}(p_{ij}-y_j^-)^2} \tag{21}$$

$$L_i=\frac{D_i^-}{D_i^-+D_i^+} \tag{22}$$

式中:J^+ 代表效益型指标集,J^- 代表成本型指标集,D_i^+ 代表第 i 个系统到正理想解的距离,D_i^- 代表第 i 个系统到负理想解的距离,L_i 代表第 i 个系统与理想解的相对接近度.

使用式(23)～(25)得到修正相对接近度 S_{ei},并将其作为业务系统的重要性系数.

$$\overline{X}=\frac{1}{mn}\sum_{j=1}^{m}p_{ij} \tag{23}$$

$$c=\frac{\sqrt{\sum_{j=1}^{m}(p_{ij}-\overline{X})^2/(mn-1)}}{\overline{X}} \tag{24}$$

$$S_{ei}=L_i(1-c) \tag{25}$$

其中 $\overline{X}$ 代表评价属性的均值.

3　实验结果与分析

3.1　数据集选取与分析

本文的仿真实验对象为机场离港业务流程,以 FlightAware 中获取的数据集进行仿真实验.FlightAware 是一个开放的飞机数据信息查询网站,其包含大量飞机基本离港数据以及可视化的飞行路径等信息,相比于其他数据集有着很好的及时性和准确性.

离港系统中包含很多数据信息,结合 FlightAware 中的数据,本文选取的数据集信息如表 4 所示.

表 4　数据集信息

Tab.4　Data set information

序号	字段名	描述
1	STN	航站信息
2	FLTYP	航班类型
3	FLIGHT	航班号
4	DEST	到达站
5	BDTIME	登机时间
6	SD	预计离港时间
7	ED	实际离港时间
8	PAX	登机旅客数
9	CLIMB	飞行高度限制
10	PDEST	货物到达时间

3.2　数据获取与关键系统识别

根据《信息安全技术　信息系统安全等级保

护基本要求》(GB/T 22239—2008),信息系统安全面临的威胁主要来自数据安全、物理安全和主机安全.

数据安全主要确保数据在传输过程中的完整性、保密性和可用性.也许某一个系统数据缺失或者丢失对业务系统没有太大影响,但大量看似无关紧要的系统数据收集后,可能会产生严重的后果.因此,在考虑系统安全时数据安全是必不可少的.

物理安全主要指的是环境安全、设备安全和介质安全.设备安全中最主要的一项是考察设备的老化程度,即设备的健壮性.目前,中国大多数企业的设备处于长期运行状态,核心设备很少更换,甚至从未更换,设备老化问题严重.若系统核心设备出现问题,必定带来一系列问题,而这些问题都是未知的.设备老化就如同炸弹一样时刻威胁着人们的财产安全、生命安全甚至国家安全.因此,设备的健壮性是影响系统安全的一项重要因素之一.

主机安全主要包括系统软件安全、硬件安全、固件安全及一些附加的安全技术与管理措施.系统软件安全则是主要的研究对象.系统软件主要负责管理计算机系统中各种资源,使得它们可以协调工作.在复杂的业务系统中,高并发是一个主要的问题,系统访问量的大小会反映当前系统的运行状态,系统运行状态是否正常又与系统安全密切相关.因此,系统访问量是影响系统安全的一个重要因素之一.

根据上述分析可知,业务系统安全性由多种因素综合决定.本文选取数据、设备和系统访问量3种评价属性来对系统安全性进行研究.

实验对象为机场离港业务流程.其流程如图6所示.

实验步骤设计如下:

(1)离港业务流程中的业务系统包括航班数据控制系统、旅客值机系统和配载平衡系统.根据离港业务流程建立业务流程关联树,本文选取的评价属性为数据、设备和系统访问量.离港业务流程关联树如图7所示.

本文以旅客值机系统为例,介绍如何获取评价属性.

数据评价属性取值方法:根据1.2中数据评价属性取值方法,对旅客值机系统中的数据进行赋值,得到数据安全属性矩阵:

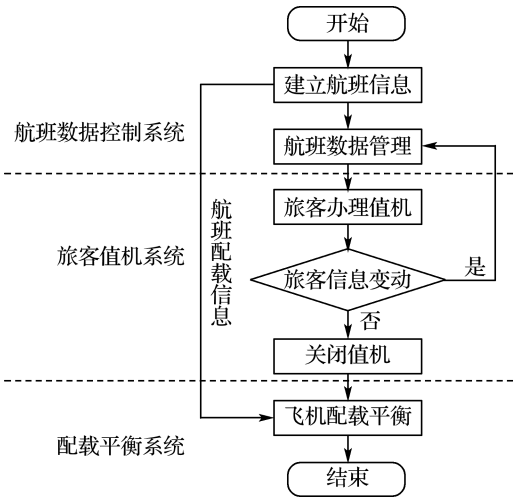

图6 离港业务流程

Fig. 6 Departure business process

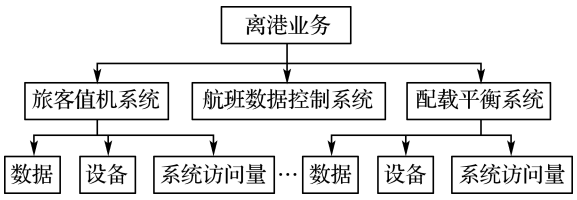

图7 离港业务流程关联树

Fig. 7 Departure business process association tree

$$\boldsymbol{D}=\begin{pmatrix}0.50 & 0.75 & 1.00\\ 0 & 0.50 & 1.00\\ 0.50 & 0.50 & 0.25\end{pmatrix}$$

随后,利用式(1)得到数据评价属性取值 $d=0.56$.

设备评价属性取值方法:由于系统有很多设备,本文选取系统服务器作为目标,根据1.2中设备评价属性取值方法,记录旅客值机系统服务器7 d内的CPU使用率与内存使用率,取它们的均值并根据表2得到系统服务器的CPU负荷系数 $f_l=1.10$,内存系数 $f_e=1.05$,且根据服务器规格说明得到 $t_d=8$.利用式(2)~(4)可得设备评价属性的取值为0.40.旅客值机系统服务器参数如表5所示.

系统访问量取值方法:获取7 d内旅客值机系统访问量的值,以每天平均访问量作为当天的实际访问量,可得 $V_{now}=\{300,280,360,480,500,450,610\}$.系统的最大访问量 $V_{max}=1\ 000$,根据表3中等级对应的二进制取值可得矩阵 $\boldsymbol{C}$、$\boldsymbol{R}$,再根据式(5)得到系统访问量评价属性的取值为0.85.

表 5　旅客值机系统服务器参数

Tab. 5　Server parameters of passenger check-in system

时间/d	CPU 使用率/%	内存使用率/%
1	63	42
2	54	53
3	76	47
4	53	55
5	80	60
6	77	45
7	56	44

同理，对离港业务流程其余业务系统的评价属性进行取值，如表 6 所示.

表 6　离港业务系统评价属性取值

Tab. 6　Evaluation attribute value of departure business system

系统名称	评价属性取值		
	数据	设备	系统访问量
旅客值机系统	0.56	0.40	0.85
航班数据控制系统	0.39	0.48	0.61
配载平衡系统	0.61	0.38	0.53

(2)将离港业务流程中的旅客值机系统、航班数据控制系统和配载平衡系统抽象为节点，将业务系统之间的关联性用一条有向边表示，得到离港业务流程关联网络(图 8)和系统关联度矩阵 $\boldsymbol{G}=\mathbf{diag}\{0.375,0.375,0.250\}$.

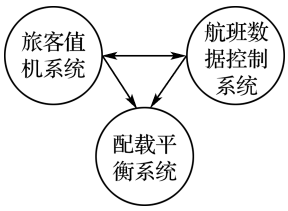

图 8　离港业务流程关联网络

Fig. 8　Departure business process association network

(3)将评价属性矩阵与系统关联度矩阵结合得出关联评价属性矩阵，将其作为 TOPSIS 改进方法中的决策矩阵.

(4)使用熵权法、变异系数法和先验估计法分别为评价属性加权. 然后用式(17)得到本文方法为评价属性的加权结果，并将加权结果与决策矩阵结合得到加权决策矩阵，加权结果如表 7 所示.

表 7　评价属性加权取值

Tab. 7　Weighted value of evaluation attribute

加权方法	评价属性加权结果		
	数据	设备	系统访问量
熵权法	0.234	0.269	0.498
变异系数法	0.280	0.304	0.416
先验估计法	0.370	0.230	0.400
本文方法	0.295	0.268	0.438

(5)计算离港业务中业务系统重要性系数. 利用 TOPSIS 改进方法，计算业务系统重要性系数，分别得到以下结果.

正理想解与负理想解：

$$y^{+}=\{0.059,0.046,0.173\}$$

$$y^{-}=\{0.064,0.051,0.047\}$$

离港业务系统的相对接近度 L 为

$$L=\{0.755,0.654,0.482\}$$

修正相对接近度 S_e 为

$$S_e=\{0.49,0.38,0.27\}$$

将修正相对接近度 S_e 作为业务系统重要性系数.

(6)根据步骤(5)中离港业务流程中业务系统重要性系数的大小为业务系统排序，旅客值机系统＞航班数据控制系统＞配载平衡系统，因此旅客值机系统为离港业务流程中的关键业务系统.

3.3　业务系统的影响分析

本实验目的是分析业务系统发生信息安全事件后业务流程可能面临的安全风险，并评估其对业务流程连续性的影响. 旅客值机系统发生信息安全事件 5 min 内性能参数变化情况如表 8 所示.

表 8　旅客值机系统性能变化参数

Tab. 8　Performance change parameters of passenger check-in system

时间/min	α	β	γ
1	600	0.6	5
2	500	0.8	10
3	200	0.9	60
4	50	1.0	200
5	10	1.0	未响应

利用式(9)～(11)，可得旅客值机系统发生信息安全事件 5 min 内离港业务流程连续性的变化情况，实验结果如图 9 所示.

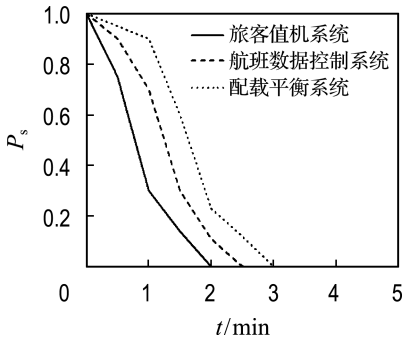

图 9 业务流程连续性走势

Fig. 9 Business process continuity trend

由图 9 可知，业务流程连续性初始值为 1，代表业务流程连续性很好，业务系统发生信息安全事件后，业务流程连续性在短时间内急剧下降，如旅客值机系统，在 1 min 时业务流程连续性下降至 0.3 左右，2 min 业务连续性下降至 0，面临业务流程业务中断的风险. 相比于旅客值机系统，其余两个系统在 2.5、3 min 时面临业务流程中断的风险. 旅客值机系统一旦发生信息安全事件，会在 2 min 内造成离港业务流程中断，导致离港系统无法为后续乘客服务，造成数据堵塞，大量旅客滞留等现象，甚至引起更为严重的社会影响. 无论从系统角度还是从社会影响方面，都体现出旅客值机系统为离港业务流程中的关键业务系统.

3.4 加权方法分析

为了研究加权方法对本文结果的影响，选取不同的加权方法，对相同的数据样本进行对比实验.

具体步骤如下：

(1)将评价属性数量设为 3，业务系统数量设为 5，分别编号为 1～5，用 n_s 表示. 用 Matlab 生成 10 个决策矩阵作为初始数据，分别编号为 1～10，用 d_s 表示.

(2)分别用本文方法、熵权法、变异系数法和先验估计法为初始数据加权，并得到相应的 10 个加权决策矩阵.

(3)将加权决策矩阵作为输入，利用式(18)～(25)计算出修正相对接近度，并识别出关键系统. 识别结果如图 10 所示.

由图 10 可知，4 种加权方法只在编号为 5 和 9 的决策矩阵作为初始数据的情况下，都识别出编号为 2 和 4 的系统为关键系统. 熵权法在编号为 2 和 6 的决策矩阵作为初始数据的情况下，出现了识别结果不准确的情况. 同理，变异系数法与先验估计法都出现了识别结果不准确的情况. 而本文方法在 10 次对比实验中，识别结果均准确，这也证明了本文方法的优越性.

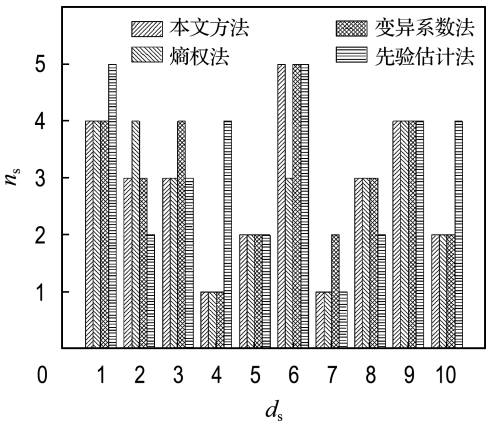

图 10 不同加权方法识别结果

Fig. 10 Recognition results of different weighting methods

3.5 模型识别效果分析

为了分析本文方法的识别效果，将系统抽象为节点，选取不同的关键节点识别方法，使用相同的数据样本进行节点重要度识别对比实验. 文献[9]通过改进 TOPSIS 中加权方法来识别关键节点；文献[10]提出 Bi-TOPSIS，将双极容度理论与 TOPSIS 结合；文献[11]利用灰色关联度识别关键节点. 将本文方法，文献[9]、[10]和[11]中的方法对比，实验设计步骤如下：

(1)用 Matlab 生成 10 个节点数量为 10 的评价属性矩阵，且都将节点 1 设置为关键节点.

(2)为分析本文方法与其他方法的识别准确率，分别用本文方法，文献[9]、[10]和[11]中的方法对步骤(1)中的评价属性矩阵进行识别.

(3)假设上述 4 种方法关键节点识别结果不为节点 1 的数目为 E_r.

(4)用式(26)计算上述 4 种方法的准确率.

$$A_c = 1 - E_r/100 \tag{26}$$

上述 4 种方法准确率如表 9 所示.

表 9 不同方法识别准确率

Tab. 9 Recognition accuracy of different methods

方法	评价矩阵数量	节点总数量	准确率/%
本文方法	10	100	96
文献[9]方法	10	100	94
文献[10]方法	10	100	90
文献[11]方法	10	100	92

从表 9 可知，本文方法的识别准确率为 96%，相比于文献[9]、[10]和[11]中的方法，分别提高了 2%、6%和 4%，表明本文方法在准确性方面具有一定优势.

3.6　模型通用性分析

为了分析本文方法的普适性与有效性，将本文方法应用到某高校学生管理业务流程.

学生管理业务流程主要包括学生课程系统、考试系统、教务评价系统、住宿系统、校园卡系统和图书馆系统.

本文模型选取的评价属性为数据、设备和系统访问量. 其中，系统访问量与在校学生的数量有关，且与不同时间段内学校是否有活动安排有关，以 1～10 周为例，学生管理业务流程中关键业务系统识别结果如图 11 所示.

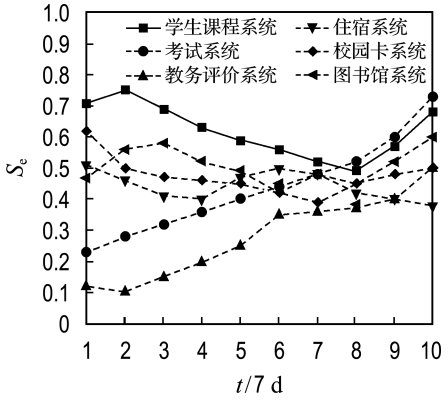

图 11　学生管理业务流程关键系统识别结果

Fig. 11　Key system identification results of student management business process

从图 11 可知，第 1～7 周，学生课程系统是关键业务系统，随着时间的变化，其系统重要性系数逐渐降低. 第 8～10 周，考试系统为关键业务系统，因为此时学生面临考试，随着考试的临近，考试系统重要性系数也随着增大. 其余 4 个系统在不同时期的重要程度与学生需求呈不断变化趋势. 本文模型能够识别出不同时间段内学生管理业务流程的关键业务系统，因此本文模型具有普适性与有效性.

4　结　语

本文结合 TOPSIS 提出面向风险评估的全业务流程关键业务系统识别方法. 由于业务系统之间存在关联关系，逐一识别评估会导致结果不准确. 本文提出的关键业务系统识别方法通过引入关联树与关联网络，并改进加权方法与相对接近度计算方法，从而提高识别准确性. 同时，评估业务系统发生信息安全事件时系统性能下降值，能够进一步分析对业务流程连续性的影响.

参考文献：

[1] 饶志宏，方恩博. 软件与系统漏洞分析与发现技术研究构想和成果展望[J]. 工程科学与技术，2018，**50**(1)：9-21.
RAO Zhihong，FANG Enbo. Prospects for the analysis and discovery technology of vulnerabilities in software and system [J]. **Advanced Engineering Sciences**，2018，**50**(1)：9-21. (in Chinese)

[2] 杨宏宇，王峰岩. 基于无监督多源数据特征解析的网络威胁态势评估[J]. 通信学报，2020，**41**(2)：143-154.
YANG Hongyu，WANG Fengyan. Network threat situation assessment based on unsupervised multi-source data feature analysis [J]. **Journal on Communications**，2020，**41**(2)：143-154. (in Chinese)

[3] 杨宏宇，王在明. Android 共谋攻击检测模型[J]. 通信学报，2018，**39**(6)：27-36.
YANG Hongyu，WANG Zaiming. Android collusion attack detection model [J]. **Journal on Communications**，2018，**39**(6)：27-36. (in Chinese)

[4] 杨宏宇，韩　越. 基于动态信誉的无线 Mesh 网络安全路由机制[J]. 通信学报，2019，**40**(4)：195-201.
YANG Hongyu，HAN Yue. Wireless Mesh network secure routing mechanism based on dynamic reputation [J]. **Journal on Communications**，2019，**40**(4)：195-201. (in Chinese)

[5] BELOV V M，PESTUNOV A I，PESTUNOVA T M. On the issue of information security risks assessment of business processes [C] // **2018 14th International Scientific - Technical Conference on Actual Problems of Electronic Instrument Engineering，APEIE 2018 - Proceedings**. Piscataway：IEEE，2018：136-139.

[6] FATHI M，NOURMOHAMMADI A，NG A H C，*et al*. An optimization model for balancing assembly lines with stochastic task times and zoning constraints [J]. **IEEE Access**，2019，**7**：32537-32550.

[7] GU Hui，SONG Bifeng. Study on effectiveness evaluation of weapon systems based on grey

relational analysis and TOPSIS [J]. **Journal of Systems Engineering and Electronics**, 2009, **20**(1): 106-111.

[8] YAAKOB A M, SERGUIEVA A, GEGOV A. FN-TOPSIS: Fuzzy networks for ranking traded equities [J]. **IEEE Transactions on Fuzzy Systems**, 2017, **25**(2): 315-332.

[9] WANG Dongqing, LU Yueming, GAN Jiefu. An information security evaluation method based on entropy theory and improved TOPSIS [C] // **Proceedings - 2017 IEEE 2nd International Conference on Data Science in Cyberspace, DSC 2017**. Piscataway: IEEE, 2017: 595-600.

[10] ZHANG Ling, XU Yan, YEH C H, *et al*. Bi-TOPSIS: A new multicriteria decision making method for interrelated criteria with bipola measurement [J]. **IEEE Transactions on Systems, Man, and Cybernetics: Systems**, 2017, **47**(12): 3272-3283.

[11] LI Xiaolong, HAN Yiliang, WU Xuguang, *et al*. Evaluating node importance in complex networks based on TOPSIS and gray correlation [C] // **Proceedings of the 30th Chinese Control and Decision Conference, CCDC 2018**. Shenyang: IEEE, 2018: 750-754.

[12] YANG L A, CHANG Y J, CHEN S H, *et al*. SQUAT: a sequencing quality assessment tool for data quality assessments of genome assemblies [J]. **BMC Genomics**, 2019, **19**(9): 238-249.

[13] KARUPPASAMY P, KAMALESH T, SENTHIL PANDIAN M, *et al*. Growth of high-quality organic single crystal of 2-aminopyridinium 4-nitrophenolate 4-nitrophenol (2AP4N) by a novel Rotational Sankaranarayanan - Ramasamy (RSR) method [J]. **Journal of Crystal Growth**, 2019, **518**: 59-72.

[14] HAMAMREH J M, FURQAN H M, ARSLAN H. Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey [J]. **IEEE Communications Surveys and Tutorials**, 2019, **21**(2): 1773-1828.

Key system identification for risk assessment

YANG Hongyu*, QIN Geng

(School of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China)

Abstract: In order to effectively identify the key business system and assess the security risk and impact of business systems on the entire business process security, a key business system identification model for the entire business process is proposed. Firstly, the business process association tree and the business process association network are established, and the evaluation attribute matrix and the system association degree matrix are obtained. Secondly, the association evaluation attribute matrix is built by the evaluation attribute matrix and the system association degree matrix. And the weighting and relative proximity calculation methods of the technique for order preference by similarity to an ideal solution (TOPSIS) are improved. Then, the important coefficient of business system is calculated based on the improved TOPSIS method and the key business system is identified. Finally, the effect on the continuity of the entire business process is evaluated when information security incidents occur in the business system. Experimental results show that the method can identify the key business system accurately, and it can help to evaluate the impact of the business system on the entire business process effectively.

Key words: business process; risk assessment; business system; TOPSIS; system identification