不完全信息下的威胁处置效果模糊评估

李凤华[1,2,3]，李勇俊[1,2]，杨正坤[1,2]，张晗[1,2]，张玲翠[1,2]

（1. 中国科学院信息工程研究所，北京 100093；2. 中国科学院大学网络空间安全学院，北京 100049；
3. 通信网信息传输与分发技术重点实验室，河北 石家庄 050081）

摘 要：为合理选取和调整威胁处置方式，需要对威胁处置效果进行评估。现有的评估方法主要针对风险和威胁态势，很少评估威胁处置效果，且这些方法的前提条件之一是用于评估的所有信息完全，这一条件在实际环境中难以实现。针对该问题，提出了一种不完全信息下的威胁处置效果模糊评估方法。首先，综合考虑攻防双方设计层次化评估指标树；其次，利用模糊层次分析法计算各指标的综合权重；最后，通过模糊综合评价法对威胁处置效果进行评估。特别地，针对层次分析时判断矩阵元素缺失问题，利用指标重要性的传递性关系对缺失元素进行补全；针对综合评价时指标数据缺失问题，通过矩阵分解对缺失元素进行补全。实验结果表明，所提方法可有效处理信息不完全的情况，实现对威胁处置效果的有效评估。

关键词：不完全信息；威胁处置效果；模糊评估；矩阵补全

中图分类号：TP302

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2019078

Fuzzy evaluation for response effectiveness in cases of incomplete information

LI Fenghua[1,2,3], LI Yongjun[1,2], YANG Zhengkun[1,2], ZHANG Han[1,2] , ZHANG Lingcui[1,2]

1. Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
3. Science and Technology on Communication Networks Laboratory, Shijiazhuang 050081, China

Abstract: In order to appropriately select and adjust response countermeasures, it is necessary to evaluate response effectiveness. Although a large amount of effort has been spent on the evaluation of risk and threat situations, the existing schemes are not suitable to evaluate response effectiveness, because the sechems require that all the information used for evaluation is complete, which is difficult to implement in the real environment. To address the problem, a fuzzy scheme was proposed to deal with incomplete information (i.e., missing elements of judgment matrix and missing data of indicators) and the response effectiveness was evaluate. Firstly, a hierarchical indicator tree was design to characterize the effectiveness from the perspectives of both attack and defense. Then, the fuzzy analytic hierarchy process (FAHP) was used to calculate the comprehensive weight of each indicator. Finally, the response effectiveness was calculated using fuzzy comprehensive evaluation. In particular, to deal with the problem of incompleteness of fuzzy judgment matrix in the process of FAHP, the missing elements were completed based on the transitivity of elements. And to deal with the problem of loss data in the comprehensive evaluation, the missing data was completed based on matrix completion. The experimental results show that the proposed scheme can accurately recover the missing data and can effectively evaluate the effectiveness of response.

Key words: incomplete information, response effectiveness, fuzzy evaluation, matrix completion

收稿日期：2018−11−06；**修回日期**：2019−01−22

通信作者：张玲翠，zhanglingcui@iie.ac.cn

基金项目：国家重点研发计划基金资助项目（No.2016YFB0801001）；国家自然科学基金资助项目（No.61672515）

Foundation Items: The National Key Research and Development Program of China (No.2016YFB0801001), The National Natural Science Foundation of China (No.61672515)

1 引言

网络威胁日益严重，攻击手段层出不穷。2017 年 5 月，勒索病毒 WannaCry 爆发，至今已感染全球超过 150 个国家的近 500 万台计算机。为了应对威胁、拦截攻击，研究人员提出了各类威胁处置方案[1]，通过在攻击发生前、发生中或发生后部署各类安全措施，实现对威胁的处置。

然而，由于安全局势瞬息万变，难以确保威胁处置方案可以有效地阻止攻击，所部署安全措施的合理性也无法保证，甚至无法知晓安全措施是否按照预期真实、有效部署，因此，需要在部署安全措施后对其合理性、有效性进行评价，如系统运行状态是否恢复正常、服务质量是否得到改善等，即需要对威胁处置效果进行评估。威胁处置效果评估指对威胁处置前后被保护对象安全状态的变化情况的度量，反映了被保护对象在威胁处置后安全状态的提升或下降情况，是选取、评价和调整威胁处置方案的重要依据。

现有关于威胁处置效果评估的工作主要从受害主机/网络或用户感受的角度选取效果评估指标，或仅从风险变化角度考虑处置的有效性，忽略了不同维度指标对处置效果的综合影响，且未考虑指标数据本身的不准确性和模糊性，造成了评估的片面性和不准确性。

不仅如此，现有处置效果评估方案在评估过程中，要求所选取的指标数据可以真实、准确、有效地被获取，然而对于实际网络环境，处置效果评估数据获取过程中，这样的要求难以实现，具体可能存在以下问题：1) 由于指标获取技术手段的限制，无法获取相应指标数据；2) 由于部分设备可能已遭受攻击，不在受控范围内，无法提供相应指标数据；3) 由于数据获取频率设置不恰当等原因，未获取到所需时刻的指标数据；4) 由于网络传输的不可靠性，导致获取的指标数据在传输过程中丢失；5) 部分用户可能出于自我隐私保护的需要，拒绝提供相关指标数据。以上问题都会导致指标数据的缺失和遗漏，从而影响处置效果评估的准确性。

针对上述问题，本文提出了威胁处置效果模糊评估模型。该模型综合考虑防守方和攻击方 2 个角度，从运行状态、系统行为、服务情况和报警情况 4 个维度综合选取处置效果评估指标，并利用模糊层次分析法确定不同指标的权重，然后通过模糊综合评价法确定威胁处置效果；在此基础上，对模糊层次分析和模糊综合评价过程中的数据缺失情况进行分析，并对缺失数据进行补全。本文的主要贡献如下。

1) 综合考虑攻防双方 2 个角度的运行状态、系统行为、服务情况和报警情况这 4 个维度的各类指标对威胁处置效果评估的影响，以及评估过程中各指标数据的不准确性和模糊性，将模糊评价思想（模糊层次分析法和模糊综合评价法）引入处置效果评估。

2) 在模糊评估过程中利用“元素补全”思想对缺失元素进行填补。具体地，针对层次分析时判断矩阵数据缺失问题，利用指标重要性的传递性关系对缺失元素进行补全；针对综合评价时指标数据缺失问题，通过矩阵分解对缺失元素进行补全，解决了数据不完全的问题，增强了所提效果评估方法在实际网络环境中的实用性和可操作性。

3) 在实验网络环境下，对所提出的方法进行了实验验证。实验结果表明，本文方法可有效处理信息不完全的情况，实现了对威胁处置效果的有效评估。

2 相关工作

目前，针对威胁处置效果的评估方法相对较少，但从安全评估技术本身出发，已有很多研究，且可供处置效果评估借鉴。本节主要从评估技术本身入手，对相关研究进行论述。

2.1 基于层次分析的安全评估

基于层次分析[2]（AHP，analytic hierarchy process）的评估是指通过目标层、准则层、方案层等分层形式构建树状指标评估体系，将定性分析与定量计算相结合的多目标评价方法。

张义荣等[3]基于层次分析法确定吞吐量、时延等指标的权重，并通过网络熵对攻击前后的安全状态进行比较，得到网络熵差从而得到攻击效果的评价结果，但在指标权重确定过程中，忽略了用户评价的模糊性，难以保证评估的准确性。Li 等[4]提出了一种基于灰关联的指标体系以避免指标的任意选择，设计了一种基于区间数互判别矩阵的 AHP 方法，该方法扩展了经典的层次分析法，处理不同领域专家提出的可能的矛盾意见，以及评价中收集独立和不确定数据的标准化问题，并给出了新的灰色层次分析模型的转换和优化方法，最后基于上述方法建立了一种改进的灰色变权重聚类评价模型。Gao 等[5]针对服务质量的层次分析评估过程中，判断矩阵难以获取而导致的排序困难问题，基于不完备判断矩阵提出了一种改进的 AHP 评估方法，该方法通过考虑判断矩阵中元素的传递性对缺失元

素进行补全，从而提高评估方法的实用性，但在评估过程中未考虑判断矩阵元素的模糊性问题。

采用层次分析的好处是表示清晰、易于理解，在使用过程中容易扩展，可根据需要随时增加。但是影响指标因素的选取主观性较强，在实际应用中，判断矩阵中的值无法完全获取。

2.2　基于知识推理的安全评估

基于知识推理的评估方法充分利用历史经验建立评估模型，通过模糊理论、图模型、D-S 证据理论等方法处理不确定性，利用逻辑推理方法实现对目标对象的评估。

Alali 等[6]利用 Mamdani 模糊推理系统设计了一个风险评估模型，模型综合脆弱性、威胁、可能性和影响这 4 个风险因素，生成风险评估结果，以确定可能威胁实体的风险范围。Samantra 等[7]在提出层次化风险结构表示方法的基础上建立了定性风险评估的形式化模型。该模型首先定义了风险的基本参数——异常可能性（likelihood）和严重程度，并利用模糊集理论代替概率评估，通过广义梯形模糊数的质心法的概念来量化风险程度，提高决策可靠性。Rashidi 等[8]提出了基于隐马尔可夫模型（HMM, hidden Markov model）的 Android 应用程序和资源风险评估框架 XDroid，该框架将地图类应用程序的行为作为观察组，得到关于时间戳的观测集，引入在线学习模型来整合用户输入，从而提供自适应的风险评估。Sen 等[9]提出了一种基于攻击图的传感器云中无线传感器网络 WSN（wireless sensor network）的风险评估框架，该框架使用贝叶斯网络来评估和分析不同时间段内攻击对系统安全参数（如机密性、完整性、可用性等）的影响，从而评估风险。

基于知识推理的评估方法将“知识”的运用融合到推理过程中，评估结果可对目标对象进行优劣等级或类型划分，清晰明了。但该方法要求维护大量推理规则，空间开销和推理代价都很高。

2.3　基于模式识别的安全评估

基于模式识别的评估方法指通过机器学习建立目标对象的模板，通过模式匹配的方式，完成对目标对象的划分。

杨豪璞等[10]对网络中的安全事件进行场景聚类以识别攻击者，对每个攻击场景进行因果关联，识别出相应的攻击轨迹与攻击阶段，建立态势量化标准，结合攻击阶段及其威胁指数，实现对网络安全态势的评估。黄亮等[11]针对评估过程需要卸载和重新部署处置措施所带来的高成本问题，提出一种基于神经网络的分布式拒绝服务（DDoS, distributed denial of service）攻击的处置效果评估方案，但该方案仅从用户感受角度进行指标选取，虽然降低了指标数据的获取难度，但无法保证评估的准确性和全面性。黄亮等[12]利用多属性决策理论，综合考虑了合法用户平均等待时间、合法用户请求应答率等指标对 DDoS 攻击处置措施的效果进行评估，但在各指标权重的确定过程中，仅从攻击者和防御者 2 个角度对权重进行计算，未考虑用户评价及偏好对权重的影响，且忽略了指标之间的层次关系。

基于模式识别的评估方法将机器学习引入评估过程，可从历史数据中自动学习目标对象划分知识。但该方法计算量大，在非实时环境中效果较好，在实时环境中难以满足实时性要求。

现有的评估方法的主要思路是，获取所有需要的指标或表征数据，对得到的各类表征数据进行融合处理，从而得到一个评估结果。不同方法之间的差异主要体现在融合信息来源不同、融合方法不同，但这些评估方法的前提条件之一是获取评估所需的所有指标数据，这在现实网络环境中难以实现，从而使得这些方法可行性低。

本文提出不完全信息下的威胁处置效果模糊评估方法，从攻防双方 2 个角度的运行状态指标、系统行为指标、服务情况指标和报警情况 4 个维度选取更为全面的评估指标，考虑数据不完全的情况设计了相应的缺失数据补全算法，通过模糊评估模型计算威胁处置效果。该评估方法不要求获取评估所需要的所有指标数据，提高了方法的实用性，并通过模糊评价一定程度上解决了主观经验造成的评估结果偏差问题，从而提高了评估的准确性。

3　模糊评估树

对于威胁处置效果的评估，涉及攻防双方多个维度、多种类别的不同指标，采用单级评估的方式难以合理评价不同评估指标对处置效果的影响程度，因此借鉴层次分析思想进行指标权重的计算；同时，为降低主观因素对评估过程的影响，基于模糊评价法对处置效果进行评估。

3.1　分层评估指标树

威胁处置效果的评估指标是对被保护对象的安全状况的具体衡量标准，是评估威胁处置有效性的基本依据。由于系统的安全保护涉及诸多方面，

如果仅根据某类或某一指标对威胁处置效果进行评价无疑是片面的、不合理的，难以准确反映出系统的真实安全状况。鉴于威胁处置过程同时涉及防守方和攻击方，系统的安全状况可根据攻防双方的状态或行为进行判断，因此从攻防双方 2 个角度对各类指标进行归类和分析。

从防守方的角度，可将指标分为系统运行状态、系统行为和服务情况这 3 个方面。

1) 运行状态方面。当被保护对象受到攻击时，其系统运行状态会发生改变，例如当系统遭受拒绝服务攻击时，系统的 CPU 占用率会显著高于正常水平。因此，系统的安全状况可通过系统运行状态反映。

2) 系统行为方面。当被保护对象遭遇入侵时，恶意程序需要通过修改系统参数等系统行为实现特定目的，例如为了实现自身的有效隐藏，恶意程序会对系统注册表进行修改。因此，系统行为可在一定程度上反映出系统的安全状况。

3) 服务情况方面。服务类被保护对象遭受攻击时，不仅自身会受影响，还会波及接受其服务的用户。例如，当 Web 服务遭受拒绝服务攻击时，合法用户访问 Web 页面时会出现明显时延。因此，系统的安全状况还可以通过系统对外提供服务的情况反映。

从攻击方的角度，可以从攻击成功所需资源（即系统状态）、攻击强度、攻击频度、攻击成功率等维度对威胁处置效果进行评估。但是，由于攻击方一般不在受控范围内，难以获取其系统状态参数等信息，在实际环境中甚至无法知晓攻击者的身份和位置，无法直接获取其相关指标。因此，考虑获取攻击方的系统状态等信息对威胁处置效果进行评估是不现实的。但是，入侵检测类系统/设备可以以报警信息的形式，间接提供威胁相关信息。例如，当攻击者对系统进行拒绝服务攻击时，安全监测类设备会根据攻击的行为特征对流量进行分析，从而向用户发出可能遭受攻击的报警。因此，可将报警情况作为攻击方相关状态和行为的反映指标，从而对威胁处置效果进行评估。基于以上分析，本文从系统状态、系统行为、服务情况、报警情况 4 个维度对处置效果进行评估。

上述 4 个维度仅将各类指标进行了分类，在实际评估过程中需要将其进一步细分为不同的指标。其中，系统状态可以细分为 CPU 占用率、内存占用率、带宽占用率、磁盘占用率等；系统行为可以细分为对系统关键文件的读取/修改/删除的频度、时间等；服务情况可以细分为服务响应时延、分组丢失率、网络传输时延、响应成功率、服务时间抖动等；报警情况包括报警数量、报警频率、报警种类、报警确信度、报警指示的攻击严重程度等。

由于不同类型的攻击针对的攻击对象存在差异，对被攻击对象的影响也不尽相同，因此针对不同类型的攻击/威胁的处置，需要根据攻击特征和受攻击后对象受影响情况选取不同的指标进行威胁处置效果评估。整体上可依据如图 1 所示的分层指标树进行评价。

3.2 模糊层次分析

由于层次分析法无法解决评估数据本身的不准确性问题（例如，报警准确度指标是入侵检测类系统/设备根据网络流量特征等产生的一个非精确指标，其本身就存在误差甚至错误），模糊层次分

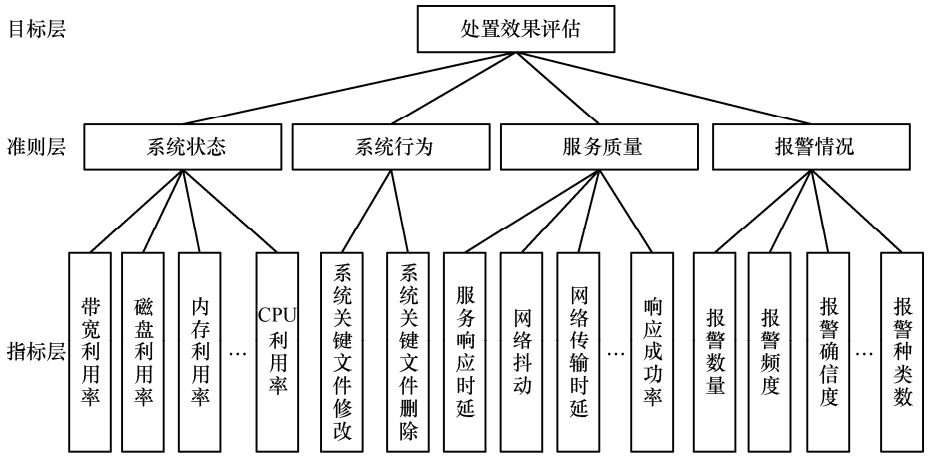


图 1 分层评估指标树

析方法[13]被提出，将三角模糊数等引入层次分析过程，以解决数据的不准确性问题。

3.2.1 确定指标重要性标度

为便于后续分析，首先对指标的重要性标度进行说明。按照层次分析法的划分方式，各指标之间的重要性比较结果包括以下 5 种重要性标度：同等重要、稍微重要、重要、明显重要、非常重要。在模糊层次分析中，分别用 0.5、0.6、0.7、0.8 和 0.9 表示，并用 0.1、0.2、0.3 和 0.4 表示反比较。

3.2.2 构造模糊判断矩阵

在构造指标重要性比较的模糊判断矩阵之前，需要先对各指标重要性比较结果对重要性标度的隶属度进行计算。现有常用的隶属函数包括三角函数型、梯形分布型、正态分布型等。根据指标重要性比较的特点，采用三角函数型隶属函数作为重要性标度的隶属度度量方式，具体定义为

$$\mu_M(x)=\begin{cases}\dfrac{1}{m-x}x-\dfrac{l}{m-l}, x\in[l,m)\\ \dfrac{1}{m-u}x-\dfrac{u}{m-u}, x\in[m,u]\\ 0, \quad\quad 其他\end{cases}$$

其中，模糊集合 M 由 m 标识并确定，m 代表 x 属于 M 的最可能值，其取值为指标重要性标度值，例如当 m 为 0.7 时，表示 M 为“指标 a_i 比指标 a_j 明显重要”；l 代表下界，即 x 属于 M 的最小可能值；u 代表上界，即 x 属于 M 的最大可能值。三角函数型模糊函数的表示为(l, m, u)。

基于 3.1 节所述的评估指标树中各层次因素，以及本节所述指标重要性标度和隶属度函数，得到指标间重要性比较的模糊判断矩阵，矩阵的形式如下

$$\boldsymbol{A}=\begin{pmatrix}a_{1,1} & a_{1,2} & \cdots & a_{1,n}\\ a_{2,1} & a_{2,2} & \cdots & a_{2,n}\\ \vdots & \vdots & \ddots & \vdots\\ a_{n,1} & a_{n,2} & \cdots & a_{n,n}\end{pmatrix}$$

其中，$a_{i,j}$ 表示指标 a_i 相对于指标 a_j 的重要性。需注意的是 $a_{i,j}$ 是一个三角模糊数，即 $a_{i,j}=\left(l_{i,j},m_{i,j},u_{i,j}\right)$。

3.2.3 单层次排序

为计算某一指标在当前维度的模糊综合度，首先对三角模糊数的运算进行介绍。三角模糊数的运算主要包括：求和⊕、求差⊖、求积⊙、倒数−1。对于 2 个模糊数 $b_1=(l_1, m_1, u_1)$，$b_2=(l_2, m_2, u_2)$，各运算定义为

$$b_1\oplus b_2=(l_1+l_2, m_1+m_2, u_1+u_2)$$
$$b_1\ominus b_2=(l_1-l_2, m_1-m_2, u_1-u_2)$$
$$b_1\odot b_2=(l_1l_2, m_1m_2, u_1u_2)$$
$$b_1^{-1}=(u_1^{-1}, m_1^{-1}, l_1^{-1})$$

如 3.2.2 节所述，$a_{i,j}$ 表示指标 a_i 相对于指标 a_j 的重要性，则可得指标 a_i 在当前维度的模糊综合度 S_i 为

$$S_i=\sum_{j=1}^{n}a_{i,j}\exp\left(\sum_{i=1}^{n}\sum_{j=1}^{n}a_{i,j}\right)^{-1}$$

其中，n 表示当前维度下指标的数量。

模糊综合度计算完成后，对各指标大小比较情况的可能度进行计算。设 $S_1=(l_1, m_1, u_1)$，$S_2=(l_2, m_2, u_2)$是 2 个指标的模糊综合度，则 $S_1\geqslant S_2$ 的可能度 $V(S_1\geqslant S_2)$定义为

$$V\left(S_1\geqslant S_2\right)=\begin{cases}1, m_1\geqslant m_2\\ \dfrac{l_2-u_1}{\left(m_1-u_1\right)-\left(m_2-l_2\right)}, m_1<m_2, l_2>u_1\\ 0, 其他\end{cases}$$

可能度计算完成后，计算各指标的权重分量，当前层第 i 个指标 a_i 的权重计算为

$$w_i^{'}=\min\left\{V\left(S_i\geqslant S_k\right):k=1,2,\cdots,n\right\}$$

然后对各权重分量进行归一化处理，得到当前层次的权重向量 $\boldsymbol{W}=(w_1, w_2, \cdots, w_i,\cdots, w_n)$，其中，

$$w_i=\frac{w_i^{'}}{\sum_{j=1}^{n}w_j^{'}},\quad i=1,2,\cdots,n$$

3.2.4 综合权重计算

假设对于第 k 个维度的各个指标，其权重向量为 $\boldsymbol{W}_k=\left(w_{k_1},w_{k_2},\cdots,w_{k_t}\right)$，则在层次化结构中，维度 i 下指标 j 的综合权重为 $w_{(i,j)}=w_i\ w_{i_j}$。最终，得到最底层所有指标的综合权重向量为

$$\boldsymbol{W}''=(w_{(1,1)},w_{(1,2)},\cdots,w_{(1,m_1)},\cdots,w_{(n,1)},w_{(n,2)},\cdots,w_{(n,m_n)})=(w_1'',w_2'',\cdots,w_p'')$$

其中，n 为维度的数量；$m_1,\cdots,m_n$ 分别为维度 1 到维度 n 下的指标数量；p 为各维度下所有指标数量的总和，即 $p=m_1+m_2+\cdots+m_n$。

由上述运算可知，所有综合权重求和结果为 1，即

$$\sum_{i=1}^{n}\sum_{j=1}^{m_n}w_{i,j}=1$$

3.3 模糊综合评价

3.3.1 确定指标集与评价集

模糊综合评价的指标集由评估树的最底层的各指标构成。

评价集指对各指标值的优良程度的评价。针对效果评估的评价集，选取优、良、中、差这 4 个模糊等级，分别表示威胁处置效果好、较好、一般、差这 4 种情况。由于处置效果的好坏取决于系统处于正常运行下各类相关指标与处置后各类相关指标的对比情况，因此根据对比情况设定相应评价等级。具体如下。

对于系统状态和系统行为这 2 个维度的各类指标数据而言，其在一般情况下符合正态分布，即

$$f(x)=\frac{1}{\sqrt{2\pi}\sigma}\exp\left(-\frac{(x-\mu)^2}{\sigma^2}\right)$$

其中，$x\geqslant 0$，表示各类指标的取值。本文认为各指标值离平均值 μ 偏差越小，效果评价等级越高。评价等级与偏离值的映射关系如表 1 所示。

表 1 系统状态、系统行为各类指标评价等级

评价等级	偏离值
优	0~a
良	a~b
中	b~c
差	$>c$

其中，a、b、c 的取值原则为，当 $x\in[\mu,\ \mu+a]$ 时，$\int_{\mu}^{\mu+a}f(x)\mathrm{d}x=a'$，$\int_{\mu+a}^{\mu+b}f(x)\mathrm{d}x=b'$，$\int_{\mu+b}^{\mu+c}f(x)\mathrm{d}x=c'$，$a'$、$a'-b'$、$c'-b'$ 分别表示评价等级为优、良、中这 3 个等级的指标值占所有指标值的比例。

对于服务情况和报警情况这 2 个维度的各类指标数据而言，本文认为各指标值的大小与处置效果存在正相关或负相关的关系。效果评价等级与指标值之间的映射关系如表 2 所示。

表 2 服务情况、报警情况各类指标评价等级

评价等级	负相关类指标的值	正相关类指标的值
优	0~p_1	$>r_2$
良	p_1~q_1	q_2~r_2
中	q_1~r_1	p_2~q_2
差	$>r_1$	0~p_2

3.3.2 确定隶属函数及模糊矩阵

为了保证评估结果的完备性与相容性，结合处置效果评估数据的分布规律，采用正态分布型隶属函数作为评价等级隶属度的度量方式，具体定义为

$$N_A(x)=\exp\left(-\frac{(x-\mu)^2}{\sigma^2}\right)$$

其中，模糊集合 A 由 μ 标识并确定，例如当 μ 为 $\frac{b+c}{2}$ 时，表示模糊集合 A“效果属于一般”，μ、σ 为集合 A 的隶属函数的分布参数。正态分布型模糊函数表示为(μ,σ^2)。

基于隶属函数，可得到指标 a_i 到评价等级 v_j 的隶属度 $r_{i,j}$，然后得到综合评判矩阵 $\boldsymbol{R}=(r_{i,j})_{pq}$，其中，$p$ 为指标数，q 为评价等级数。

3.3.3 模糊综合算法

根据模糊层次分析求出的各指标的综合权重和评价等级的隶属函数，求得各指标的模糊综合评判矩阵为

$$\boldsymbol{B}=\boldsymbol{W}''*\boldsymbol{R}=(b_1,b_2,\cdots,b_q)$$

其中，*指模糊合成运算。一般而言，常见的算子包括：取大取小算子（$\wedge,\vee$）、最大乘积算子（$\cdot,\vee$）、加权平均型算子（$\cdot,+$）等。本文选取加权平均型算子进行模糊运算，即

$$b_j=\sum_{i=1}^{p}\left(w_i''r_{i,j}\right),j=1,2,\cdots,q$$

所有 b_j 计算完成后，得到评价结果集 $\boldsymbol{B}$。最后，根据加权平均原则处理评价结果集得到处置效果评分值。

4 缺失数据补全算法

如前所述，各类指标数据可能由于各种原因而无法获取，从而导致后续评价无法开展，因此需要对缺失的指标数据进行补全。不仅如此，由于层次分析过程中涉及各类指标的权重计算，而该权重的计算过程依赖于专家对于不同指标重要性比较的先验知识，不同专家经验等的差异也可能导致指标重要性比较的打分值的缺失，从而导致层次分析过程中判断矩阵的不完整，因此需要对判断矩阵中的元素进行补全。

4.1 模糊判断矩阵补全

在模糊判断矩阵中，矩阵元素代表不同指标的重要性比较结果。具体而言，元素 $a_{i,j}$ 为指标 a_i 和指标 a_j 的重要性比较结果，即

$$a_{i,j}=a_i\ominus a_j\oplus m \tag{1}$$

其中，m 表示 a_i 与 a_j 具有同等重要性时的取值。

易知，矩阵中各元素的值满足重要性的传递性，即，若 a 比 b 重要，b 比 c 重要，则 a 比 c 重要。因此，可对式(1)进行变换得到式(2)。

$$a_{i,j}=(a_i\ominus a_k)\ominus(a_j\ominus a_k)\oplus m=(a_i\ominus a_k\oplus m)\ominus (a_j\ominus a_k\oplus m)\oplus m=a_{i,k}\oplus a_{j,k}\oplus m \tag{2}$$

其中，$a_{i,j}=\left(l_{i,j},m_{i,j},u_{i,j}\right)$，$m=\left(0.5,0.5,0.5\right)$。需要注意的是，$a_{i,j}$ 为三角模糊数，式(1)和式(2)的 $\oplus$、$\ominus$ 为 3.2.3 节所述的相应的三角模糊运算。

4.2　综合评判矩阵补全

在综合评判矩阵中，矩阵元素代表某一指标属于某一评价结果的隶属度。具体而言，元素 $r_{i,j}$ 表示指标 a_i 到评价结果 v_j 的隶属度。由于每一指标到评价集中各评价值都有一个隶属度，为了简化运算，并考虑综合评判矩阵元素缺失的本质原因，可将综合评判矩阵中缺失元素的填补问题转化为原始指标值缺失元素的填补问题。

在模糊综合评判过程中，涉及通过多个不同指标进行评价，且需要获取威胁处置前后多个时刻的数据，因此可将原始指标数据表示为一个原始指标值矩阵（不完整矩阵）$\boldsymbol{D}_{mn}$，其中，m 表示指标的数量，n 表示数据获取的时刻数。

如前所述，在原始指标值矩阵中，部分元素可能由于各种原因无法获取或丢失，但在评估过程中又需要这些指标值，因此需要对这些缺失元素进行合理、准确地填补。按照上述分析，可将原始指标值缺失元素的填补问题转化为标准矩阵补全[14]问题。考虑到原始指标值矩阵为小规模矩阵、求解精度等原因，基于矩阵分解进行矩阵补全，因此，矩阵补全问题可形式化为

$$\begin{aligned}&\min\nolimits_{\boldsymbol{U}\in\mathrm{R}^{m\times k},\boldsymbol{V}\in\mathrm{R}^{k\times n},\boldsymbol{Z}\in\mathrm{R}^{m\times n}}\left(\boldsymbol{UV}-\boldsymbol{Z}\right)^2\\&\text{s.t. }P_{\boldsymbol{\Omega}}\left(\boldsymbol{Z}\right)=P_{\boldsymbol{\Omega}}\left(\boldsymbol{M}\right)\end{aligned} \tag{3}$$

其中，k 为预测的矩阵秩界；$\boldsymbol{Z}$ 为不完整矩阵，$\boldsymbol{M}$ 为未知指标值矩阵（补全后的矩阵）；$\boldsymbol{\Omega}\subseteq[m]\times[n],[m]=\{1,2,\cdots,m\},[n]=\{1,2,\cdots,n\}$ 为矩阵下标的索引集合；$P_{\boldsymbol{\Omega}}(\cdot)$是正交投影算子，表示当$(i,j)\in\boldsymbol{\Omega}$时，$D_{ij}$为采样元素。

利用交替最小化算法对式(3)进行求解，得到矩阵 $\boldsymbol{U}$ 和 $\boldsymbol{V}$，从而得到矩阵 $\boldsymbol{D}'=\boldsymbol{UV}$，最终得到缺失指标值。

5　实验

5.1　实验设计

实验环境如图 2 所示，包括一台 Web 服务器、防火墙、一台攻击机、入侵检测系统、合法用户。其中，Web 服务器上除了安装 Web 服务外，还安装了 Tsar 系统监控工具、Nagios 系统/网络监控工具，用于获取各类指标数据；防火墙用于在攻击时部署安全措施，实现威胁处置；攻击机上部署了 LOIC（low orbit ion cannon）工具，用于模拟发起拒绝服务攻击；入侵检测系统用于威胁检测并发出报警信息。

实验采用 SYN Flood 攻击作为攻击方式，通过与服务器建立大量不完整的 TCP 连接，使其无法响应合法的用户服务，从而实现拒绝服务；在攻击过程中，通过部署处置措施，实现威胁处置。通过获取攻击前、攻击中和处置后等过程中各个时间段的相关指标数据，基于所获取的指标数据对威胁处置效果进行评估。

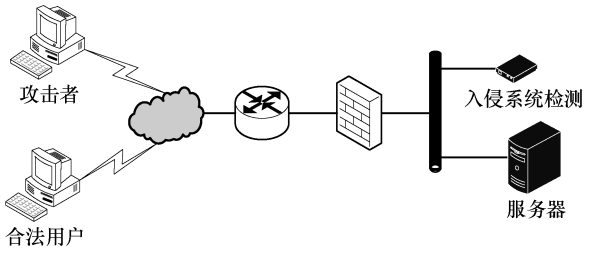


图 2　实验环境

按照 3.1 节所述，根据 SYN Flood 攻击的特点，可知在攻击过程中系统行为维度的指标数据不受 Flood 攻击所影响，因此实验只从系统状态、服务情况、报警情况这 3 个维度获取评估所需的指标。其中系统状态维度下的指标为：CPU 占用率、内存占用率、带宽占用率。服务情况维度下的指标为：服务响应时延、分组丢失率、网络传输时延、响应成功率。报警情况维度下的指标为：报警数量、报警频度。

具体而言，首先开启运行 Web 服务 5 min；在接下来的 5 min 内由合法用户向其发起正常访问；然后由攻击机发起 SYN Flood 攻击，并以 5 min 为单位逐渐增加攻击强度；攻击发生 15 min 后，在防火墙上部署处置措施 1（限制 SYN 分组的最大突发数为 100）；5 min 后删除该措施，并在防火墙上部署处置措施 2（添加过滤攻击源的过滤规则）。以

1 min 为单位获取上述过程中的各类指标数据。

5.2 威胁处置效果评估

本节对实验得到的数据进行分析，并利用模糊评估模型对处置效果进行评估。

利用 3.2 节所提出的模糊层次分析方法计算指标层各指标的综合权重。首先，要求专家对不同维度之间、同一维度下不同指标之间的重要性比较按照三角模糊数进行打分。打分过程中，由于经验等因素的限制，不同专家的打分存在差异，且可能出现部分比较数据缺失的情况，此时采取以下原则确定整合后的比较值：判定对同样 2 个维度或指标打分的专家数量，若该数量小于专家总数的$\frac{2}{3}$，则认为模糊判断矩阵中该比较值不存在；反之按照式(4)求取该比较值。

$$a_{i,j}=\frac{\sum_{a_{i,j}^k\in U_{i,j}} a_{i,j}^k}{m} \tag{4}$$

其中，$U_{i,j}$ 表示对指标 a_i 和指标 a_j 的重要性比较的打分构成的集合，m 表示集合中元素的个数。

表 1~表 4 为专家对各维度及不同维度下各指标的重要性打分表。其中，表 1 为对不同维度比较值的打分，表 2 为对系统状态维度下各指标比较值的打分，表 3 为对服务情况维度下各指标值的打分，表 4 为对报警情况维度下各指标值的打分。在表 1 中，$d_{0,1}$ 表示系统状态/服务情况，$d_{0,2}$ 表示系统状态/报警情况，$d_{0,3}$ 表示服务情况/报警情况。在表 2 中，$d_{1,1}$ 表示 CPU 占用率/内存占用率，$d_{1,2}$ 表示 CPU 占用率/带宽占用率，$d_{1,3}$ 表示内存占用率/带宽占用率。在表 3 中，$d_{2,1}$ 表示服务处理时延/网络带宽，$d_{2,2}$ 表示服务处理时延/网络传输时延，$d_{2,3}$ 表示服务处理时延/分组丢失率，$d_{2,4}$ 表示表示网络带宽/网络传输时延，$d_{2,5}$ 表示网络带宽/分组丢失率，$d_{2,6}$ 表示网络传输时延/分组丢失率。在表 4 中，$d_{3,1}$ 表示报警数量/报警种类，$d_{3,2}$ 表示报警种类/报警数量。

基于表 1~表 4，根据式(3)，可得不完全模糊判断矩阵为

表 1 不同维度重要性比较

	1	2	3	4	5	6	7	8	9	10
$d_{0,1}$	—	0.1,0.3,0.4	0.2,0.3,0.5	—	0.1,0.2,0.3	0.1,0.3,0.5	—	0.1,0.2,0.3	—	—
$d_{0,2}$	—	0.5,0.7,0.8	0.6,0.7,0.9	0.5,0.6,0.7	0.5,0.6,0.7	—	0.7,0.8,0.9	0.5,0.6,0.7	—	0.6,0.8,0.9
$d_{0,3}$	0.7,0.8,0.9	0.6,0.8,0.9	—	0.6,0.7,0.8	0.6,0.7,0.8	0.6,0.8,0.9	0.7,0.8,0.9	—	0.7,0.8,0.9	0.7,0.8,0.9

表 2 系统状态维度下不同指标重要性比较

	1	2	3	4	5	6	7	8	9	10
$d_{1,1}$	—	0.1,0.3, 0.4	0.2,0.3, 0.5	0.2,0.4, 0.5	0.1,0.2, 0.3	—	0.3,0.4, 0.5	0.1,0.2, 0.3	0.2,0.3, 0.4	0.2,0.3, 0.4
$d_{1,2}$	0.6,0.7,0.8	—	0.6,0.7,0.9	—	0.5,0.6,0.7	0.6,0.7,0.8	0.7,0.8,0.9	—	0.6,0.7,0.8	0.6,0.8,0.9
$d_{1,3}$	0.7,0.8,0.9	0.6,0.8,0.9	—	0.6,0.7,0.8	0.6,0.7,0.8	0.6,0.8,0.9	0.7,0.8,0.9	0.6,0.8,0.9	0.7,0.8,0.9	—

表 3 服务情况维度下不同指标重要性比较

	1	2	3	4	5	6	7	8	9	10
$d_{2,1}$	0.2,0.3, 0.4	—	0.2,0.3, 0.5	0.2,0.4, 0.5	0.1,0.2, 0.3	0.1,0.3, 0.5	—	0.1,0.2, 0.3	0.2,0.3, 0.4	0.2,0.3, 0.4
$d_{2,2}$	—	0.5,0.7,0.8	—	0.5,0.6,0.7	—	0.6,0.7,0.8	0.7,0.8,0.9	—	0.6,0.7,0.8	0.6,0.8,0.9
$d_{2,3}$	0.7,0.8,0.9	0.6,0.8,0.9	0.7,0.8,0.9	—	0.6,0.7,0.8	0.6,0.8,0.9	0.7,0.8,0.9	0.6,0.8,0.9	0.7,0.8,0.9	0.7,0.8,0.9
$d_{2,4}$	0.2,0.3, 0.4	0.1,0.3, 0.4	0.2,0.3, 0.5	0.2,0.4, 0.5	0.1,0.2, 0.3	0.1,0.3, 0.5	0.3,0.4, 0.5	0.1,0.2, 0.3	0.2,0.3, 0.4	—
$d_{2,5}$	0.6,0.7,0.8	0.5,0.7,0.8	0.6,0.7,0.9	0.5,0.6,0.7	0.5,0.6,0.7	0.6,0.7,0.8	0.7,0.8,0.9	0.5,0.6,0.7	0.6,0.7,0.8	0.6,0.8,0.9
$d_{2,6}$	0.7,0.8,0.9	—	0.7,0.8,0.9	—	0.6,0.7,0.8	—	0.7,0.8,0.9	0.6,0.8,0.9	—	0.7,0.8,0.9

表 4 报警情况维度下不同指标重要性比较

	1	2	3	4	5	6	7	8	9	10
$d_{3,1}$	0.7,0.8,0.9	0.6,0.8,0.9	0.7,0.8,0.9	0.6,0.7,0.8	0.6,0.7,0.8	0.6,0.8,0.9	0.7,0.8,0.9	0.6,0.8,0.9	0.7,0.8,0.9	0.7,0.8,0.9
$d_{3,2}$	0.2,0.3, 0.4	0.1,0.3, 0.4	0.2,0.3, 0.5	0.2,0.4, 0.5	0.1,0.2, 0.3	0.1,0.3, 0.5	0.3,0.4, 0.5	0.1,0.2, 0.3	0.2,0.3, 0.4	0.2,0.3, 0.4

$$\boldsymbol{A}_1=\begin{pmatrix}(0.5,0.5,0.5) & (-1,-1,-1) & (0.46,0.69,0.80)\\ (-1,-1,-1) & (0.5,0.5,0.5) & (0.56,0.78,0.88)\\ (0.2,0.31,0.54) & (0.12,0.22,0.44) & (0.5,0.5,0.5)\end{pmatrix}$$

$$\boldsymbol{A}_{2,1}=\begin{pmatrix}(0.5,0.5,0.5) & (0.18,0.30,0.36) & (0.6,0.62,0.83)\\ (0.64,0.7,0.82) & (0.5,0.5,0.5) & (0.64,0.78,0.88)\\ (0.17,0.38,0.4) & (0.12,0.22,0.36) & (0.5,0.5,0.5)\end{pmatrix}$$

$$\boldsymbol{A}_{2,2}=\begin{pmatrix}(0.5,0.5,0.5) & (0.16,0.29,0.41) & (-1,-1,-1) & (0.66,0.79,0.89)\\ (0.59,0.71,0.84) & (0.5,0.5,0.5) & (0.17,0.30,0.37) & (0.57,0.63,0.8)\\ (-1,-1,-1) & (0.63,0.7,0.83) & (0.5,0.5,0.5) & (-1,-1,-1)\\ (0.11,0.21,0.34) & (0.2,0.37,0.43) & (-1,-1,-1) & (0.5,0.5,0.5)\end{pmatrix}$$

$$\boldsymbol{A}_{2,3}=\begin{pmatrix}(0.5,0.5,0.5) & (0.65,0.79,0.89)\\ (0.17,0.30,0.42) & (0.5,0.5,0.5)\end{pmatrix}$$

其中，矩阵元素为(−1,−1,−1)代表该元素缺失。

根据式 1)，需对不完全模糊判断矩阵 $\boldsymbol{A}_1$ 和 $\boldsymbol{A}_{2,2}$ 进行补全，得到补全后的 2 个矩阵为

$$\boldsymbol{A}_1=\begin{pmatrix}(0.5,0.5,0.5) & (0.26,0.59,0.92) & (0.46,0.69,0.80)\\ (0.18,0.41,0.74) & (0.5,0.5,0.5) & (0.56,0.78,0.88)\\ (0.2,0.31,0.54) & (0.12,0.22,0.44) & (0.5,0.5,0.5)\end{pmatrix}$$

$$\boldsymbol{A}_{2,2}=\begin{pmatrix}(0.5,0.5,0.5) & (0.16,0.29,0.41) & (0.03,0.09,0.08) & (0.66,0.79,0.89)\\ (0.59,0.71,0.84) & (0.5,0.5,0.5) & (0.17,0.30,0.37) & (0.57,0.63,0.8)\\ (0.92,0.91,0.97) & (0.63,0.7,0.83) & (0.5,0.5,0.5) & (0.83,0.73,0.8)\\ (0.11,0.21,0.34) & (0.2,0.37,0.43) & (0.2,0.27,0.17) & (0.5,0.5,0.5)\end{pmatrix}$$

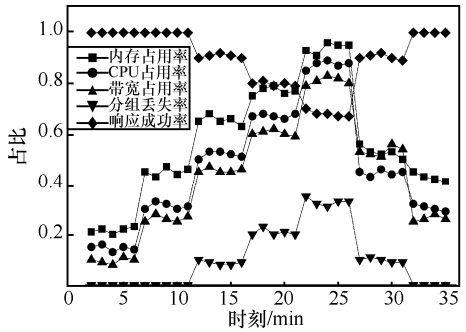
计算得到各维度之间的可能度矩阵为

$$\begin{bmatrix}1 & 1 & 1\\ 0.956\,2 & 1 & 1\\ 0.591\,8 & 0.618\,9 & 1\end{bmatrix}$$

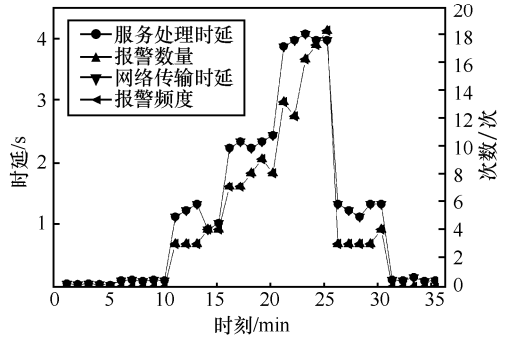
对该矩阵进行归一化后得到本层的权重向量为(0.392 5, 0.375 3, 0.232 2)。同理，根据前述判断矩阵 $\boldsymbol{A}_{2,1}$、$\boldsymbol{A}_{2,2}$、$\boldsymbol{A}_{2,3}$，可计算得到在相应评价维度下各指标的权重向量分别为(0.30, 0.70, 0)、(0, 0.213 1, 0.786 8, 0)、(0.969 3, 0.030 7)。从而得各指标的综合权重向量为(0.117 7, 0.274 7, 0, 0, 0.08, 0.295 3, 0, 0.225 1, 0.007 1)。

各类指标数据在获取过程中可能缺失，因此按照 4.2 节所述方法对缺失数据进行补全。在实验环境下各类指标数据可以完整获取，所以得到指标数据后，采用随机的方式去除部分数据，从而得到不完整指标数据集。

图 3 为内存占用率、CPU 占用率等各类指标的原始数据。



(a) 5类指标的原始数据



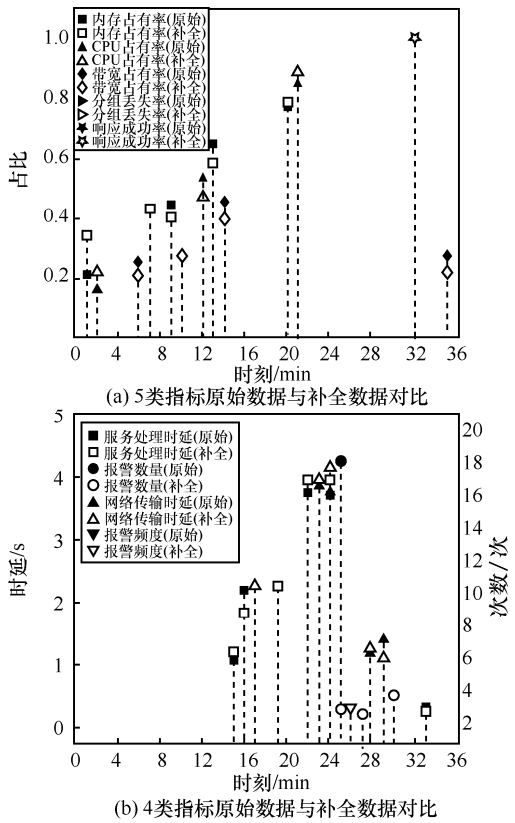
(b) 4类指标的原始数据

图 3　各类指标的原始数据

在图 3(a)中，前 10 min 为 Web 正常运行或正常向合法用户提供服务，CPU 占用率、内存占用率等处于相对平稳状态，从第 11 min 开始发起攻击，可以看出 CPU 占用率等 4 类指标不断增加，响应成功率不断降低，Web 服务受到攻击所影响。

通过式(2)对缺失的指标数据进行补全，各指标数据补全后的结果和指标数据的实际值的比较如图 4 所示。

由图 4 可以看出，补全后的数据与获取到的原始数据之间的差值都较小，在可接受范围内，因此可以认为补全是比较准确的。



(a) 5类指标原始数据与补全数据对比

(b) 4类指标原始数据与补全数据对比

图 4 原始指标数据与补全数据对比

基于补全后的指标数据，利用模糊综合评价法，得到处置效果如图 5 所示。根据折线的变化情况可知，在 1~5 min，评分值在 3 分上下波动；在 6~10 min，评分值上升到 4 分左右。这是因为在 1~5 min 时，Web 服务器并未向用户提供服务，尽管服务器处于安全状态，但作为服务提供方其资源处于闲置状态，因此评分值低于 6~10 min 向用户提供正常服务时的评分。在 11~15 min、16~20 min、21~25 min，评分值不断降低，这是因为攻击强度不断加强。在 26~30 min，部署处置措施 1 后，评分值基本提高到正常程度，但存在波动。可能的原因是处置措施虽然阻断了攻击，但对用户正常服务也造成了影响，因此评分存在波动。在 31~35 min，在部署处置措施 2 后，评分基本恢复正常，与 6~10 min 时的情况基本一致，说明处置措施 2 有效地发挥了威胁处置的作用。

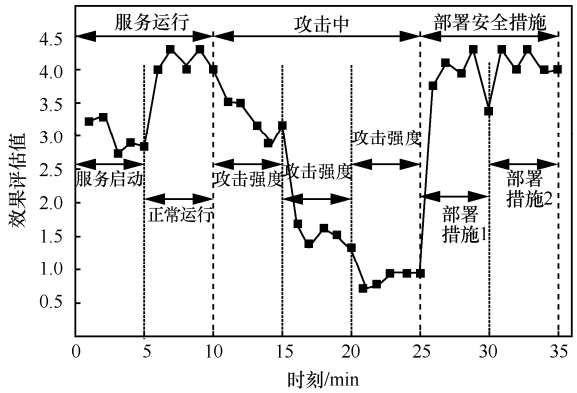


图 5 威胁处置效果评估结果

6 结束语

本文重点研究了不完全信息下的威胁处置效果评估方法，针对现有威胁处置效果评估方法的不足，提出了威胁处置效果的模糊评估模型。从攻防双方 2 个角度的运行状态、系统行为、服务情况和报警情况 4 个维度出发构建分层评估指标树，在此基础上综合考虑指标数据的不准确性，利用模糊层次分析和模糊综合评价对威胁处置效果进行评估。特定地，考虑到评估过程中指标重要性比较数据缺失和指标数据缺失的情况，利用指标重要性的传递性关系和矩阵分解对缺失元素进行补全，从而有效解决信息缺失的问题，提高了评估方法的实用性和可操作性。本文在实验网络环境下构建了攻防场景，对本文提出的评估方法的有效性与合理性进行了分析。

后续的研究主要包括：在数据补全过程中，加入指标数据间的关联关系的考虑，提高数据补全的精度；增加对判断矩阵的一致性校验，进一步提高评估方法的实用性。

参考文献：

[1] SHAMELI-SENDI A, CHERIET M, HAMOU-LHADJ A. Taxonomy of intrusion risk assessment and response system[J]. Elsevier Computers & Security, 2014, 45(3):1-16.

[2] TSAI H, HUANG Y. An analytic hierarchy process-based risk assess-

ment method for wireless networks[J]. IEEE Transactions on Reliability, 2011, 60(4):801-816.

[3] 张义荣, 鲜明, 王国玉. 一种基于网络熵的计算机网络攻击效果定量评估方法[J]. 通信学报, 2004, 25(11):158-165.
ZHANG Y R, XIAN M, WANG G Y. A quantitative evaluation technique of computer network based on network entropy[J]. Journal on Communications, 2004, 25(11):158-165.

[4] LI C, CHEN K, XIANG X. An integrated framework for effective safety management evaluation: application of an improved grey clustering measurement[J]. Elsevier Expert Systems with Applications, 2015, 42(13):5541-5553.

[5] GAO C, MA J, LIU Z, et al. An approach to quality assessment for Web service selection based on the analytic hierarchy process for cases of incomplete information[J]. Springer Science China Information Sciences, 2015, 58(12):122102.

[6] ALALI M, ALMOGREN A, HASSAN M, et al. Improving risk assessment model of cyber security using fuzzy logic inference system[J]. Elsevier Computers & Security, 2018, 74: 323-339.

[7] SAMANTRA C, DATTA S, MAHAPATRA S. Risk assessment in IT outsourcing using fuzzy decision-making approach: an Indian perspective[J]. Elsevier Expert Systems with Applications, 2014, 41(8): 4010-4022.

[8] RASHIDI B, FUNG C, BERTINO E. Android resource usage risk assessment using hidden markov model and online learning[J]. Elsevier Computers & Security, 2017, 65:90-107.

[9] SEN A, MADRIA S. Risk assessment in a sensor cloud framework using attack graphs[J]. IEEE Transactions on Services Computing, 2017, PP(99):1.

[10] 杨豪璞, 邱辉, 王坤. 面向多步攻击的网络安全态势评估方法[J]. 通信学报, 2017, 38(1):187-198.
YANG H P, QIU H, WANG K. Network security situation evaluation method for multi-step attack[J]. Journal on Communications, 2017, 38(1):187-198.

[11] 黄亮, 冯登国, 连一峰,等. 基于神经网络的 DDoS 防护绩效评估[J]. 计算机研究与发展, 2013, 50(10):2100-2108.
HUANG L, FEGN D G, LIANG Y F, et al. Artificial-neural - network-based DDoS defense effectiveness evaluation[J]. Journal of Computer Research and Development, 2013, 50(10): 2100-2108.

[12] 黄亮, 冯登国, 连一峰,等. 一种基于多属性决策的 DDoS 防护措施遴选方法[J]. 软件学报, 2015, 26(7):1742-1756.
HUANG L, FEGN D G, LIANG Y F, et al. Method of DDoS countermeasure selection based on multi-attribute decision making[J]. Journal of Software, 2015, 26(7):1742-1756.

[13] KUBLER S, ROBERT J, DERIGENT W, et al. A state-of the-art survey & testbed of fuzzy AHP (FAHP) applications[J]. Elsevier Expert Systems with Applications, 2016, 65: 398-422.

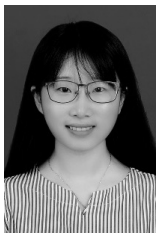
[14] XIE K, NING X, WANG X, et al. Recover corrupted data in sensor networks: a matrix completion solution[J]. IEEE Transactions on Mobile Computing, 2017, PP(99):1.

[作者简介]

李凤华（1966− ），男，湖北浠水人，博士，中国科学院研究员、博士生导师，主要研究方向为网络与系统安全、信息保护、隐私计算。

李勇俊（1992− ），男，浙江丽水人，中国科学院博士生，主要研究方向为入侵响应、访问控制。

杨正坤（1994− ），男，重庆人，中国科学院硕士生，主要研究方向为入侵响应。



张晗（1996− ），女，安徽淮北人，中国科学院硕士生，主要研究方向为入侵检测与响应、访问控制。

张玲翠（1986− ），女，河北固城人，中国科学院工程师、博士生，主要研究方向为网络安全、信息保护。