基于攻击图的主机安全评估方法

杨宏宇[1,2]，袁海航[2]，张良[3]

（1. 中国民航大学安全科学与工程学院，天津 300300；2. 中国民航大学计算机科学与技术学院，天津 300300；
3. 亚利桑那大学信息学院，图森 AZ 85721）

摘 要：针对目前主机安全评估方法中无法准确计算主机安全值，忽略攻击图中主机关联性等问题，提出一种基于攻击图的主机安全评估方法。首先，生成主机攻击图，从漏洞自身、时间、环境和操作系统可利用性 4 个角度量化原子攻击概率并计算主机攻击概率。然后，根据专家先验评估和相关性定权法计算主机资产重要性，依据攻击图中主机间的关联关系计算主机的拓扑结构重要性。最后，依据主机漏洞影响值、主机重要性和主机攻击概率计算主机安全值。实验结果表明，所提方法得到的主机重要性和安全值符合真实网络情况，能够更全面准确地反映主机的安全状况；所提方法得到的主机安全值标准差为 0.078，大于其他方法得到的安全值标准差，表明所提方法得到的安全值离散程度更大，更易于区分安全等级和后续的风险处置优先级。

关键词：主机安全；攻击图；原子攻击概率；资产重要性；拓扑结构重要性；安全评估

中图分类号：TP393.08

文献标志码：A

DOI: 10.11959/j.issn.1000−436x.2022030

Host security assessment method based on attack graph

YANG Hongyu[1,2], YUAN Haihang[2], ZHANG Liang[3]

1. College of Safety Science and Engineering, Civil Aviation University of China, Tianjin 300300, China
2. College of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300, China
3. College of Information, University of Arizona, Tucson, AZ 85721, USA

Abstract: In order to solve the problems of inaccurate calculation of host security value and ignoring host correlation in attack graph, a host security assessment method based on attack graph was proposed. First, the host attack graph was generated to quantify the atomic attack probability and the attack probability of the host was calculated from four perspectives, such as vulnerability itself, time, environment and operational system availability. Then, the host assets importance was calculated according to expert transcendental evaluation and correlation weighting method, and the topology importance of host was calculated according to the association relationship between hosts in attack graph. Finally, the host security value was calculated according to the impact value of host vulnerability, host importance and host attack probability. The experimental results show that the importance and security value of the proposed method accord with the real network situation and can reflect the security condition of the host more completely and accurately. The standard deviation of host safety value obtained by the proposed method is 0.078, which is larger than that obtained by other methods, indicating that the safety value obtained by the proposed method is more discrete and easier to distinguish the safety level from the subsequent risk disposal priority.

Keywords: host security, attack graph, atomic attack probability, asset importance, topology importance, security assessment

收稿日期：2021−11−08；**修回日期**：2022−01−11

基金项目：国家自然科学基金资助项目（No.U1833107）

Foundation Item: The National Natural Science Foundation of China (No.U1833107)

0 引言

网络主机是网络拓扑的重要组成部分，日益复杂的攻击手段和方式对网络主机造成的威胁日益增加，主机面临的安全问题日趋突出。评估各主机面临的安全情况是掌握网络整体安全性的基础，深入挖掘和分析主机潜在风险能够为网络安全防御提供有效指导，对于保护网络重要主机、保障网络安全平稳运行具有重要意义[1]。

现有常见的网络安全评估方法主要有博弈论[2]、基于攻击图模型[3]和层次分析法[4]等。相比于其他类型评估方法，基于攻击图的评估方法从攻击角度出发，以节点和边描述网络系统各安全要素间的连接关系，通过攻击路径直观有效地展示了所有可能的攻击步骤，为主机安全管理和防御提供了强有力的分析方式和技术支撑。

文献[5]以网络资产间的互联关系为基础，识别威胁场景中的威胁事件，根据威胁事件发生的概率和损失，从攻击路径的角度分析各主机和网络的安全情况，为主机防护提供了一定的理论依据。文献[6]通过分析主机的漏洞利用关系，依据漏洞利用评分构建各主机间的状态转移矩阵，然后根据 Markov 过程评估主机安全。文献[7]提出基于贝叶斯攻击图的网络安全评估方法，该方法根据漏洞可利用概率计算各主机被攻击的概率，依据主机资产价值计算主机和网络被入侵的风险。文献[8]提出一种定量的安全评估模型，该模型依据安全事件和告警数据构建贝叶斯攻击图并对网络中的威胁场景进行预测，根据漏洞评分和主机资产度量网络风险。文献[9]提出一种基于边权攻击图的风险评估方法，根据漏洞间的依赖性构建基于边权的攻击图模型，通过攻击目标的价值和利用概率对各漏洞进行了排序和分析，该方法为网络安全防御策略的选取提供了有效支撑。文献[10]通过分析漏洞在异构网络环境下被利用的可能性和影响性，设计了漏洞风险排名算法，为量化漏洞在特定环境和组件下的风险和扩展模型的解决方案提供了新的思路。文献[11]提出一种面向零日攻击的概率计算方法，将系统实例图转换为贝叶斯网络，依据贝叶斯网络从路径角度分析零日攻击发生的概率，该方法在零日攻击路径识别方面具有一定的有效性。文献[12]利用攻击图对主机和网络进行安全评估，依据原子攻击概率和邻接矩阵求解主机安全状况。

以上研究方法依据攻击图对网络主机和漏洞进行了分析和评估，但均未考虑时间、漏洞所处主机环境和不同操作系统类型对原子攻击概率的影响，且评估主机安全的方法未充分考虑主机资产重要性属性权重的差异性和攻击图中主机间的关联关系，评估结果并不合理。为解决上述研究中的不足，全面合理地分析主机安全性，本文提出一种基于攻击图的主机安全评估方法。

1 主机安全评估方法

基于攻击图的主机安全评估方法分为 2 个阶段：主机攻击图建立阶段和主机安全值计算阶段。

1) 主机攻击图建立阶段。首先分析和探测目标网络拓扑，依据主机中存在的漏洞和防火墙设定的各主机间通信规则生成主机攻击图。然后根据获取到的漏洞信息量化原子攻击概率并计算主机攻击概率和漏洞影响值。

2) 主机安全值计算阶段。首先依据先验评分结果计算各主机资产重要性值。然后根据得到的主机攻击图分析主机间的攻击利用关系并计算主机的拓扑结构重要性，由资产重要性和拓扑结构重要性共同表征主机重要性。最后，由攻击概率、漏洞影响值和主机重要性计算主机安全值，主机安全评估方法总体架构如图 1 所示。

2 主机攻击图建立

根据攻击图中节点类型的不同，攻击图可以划分为属性和状态攻击图；根据攻击图生成层次的不同，攻击图可以划分为主机攻击图和漏洞层攻击图。其中主机攻击图中的节点表示网络系统中的主机，主机攻击图能够直观展示主机间的关联性和攻击利用关系。为合理分析和评估主机安全状况，本文选用主机攻击图从主机层面对主机进行安全评估。

2.1 主机攻击图定义

主机攻击图定义为三元组 $H_{AG}=(N, E, P)$。具体概念表示如下。

1) N 表示主机攻击图中的节点集合且 $N=N_{attack}\cup N_{host\_i}$，其中 N_{attack} 表示初始攻击主机，N_{host_i} 表示其他主机。

2) $E=\{E_1, E_2, E_3, \cdots, E_n\}$表示边集合，代表两主机间的关联关系，其中 n 表示攻击图中所有边的数量。

3) $P=\{P_1, P_2, P_3, \cdots, P_n\}$表示原子攻击概率集

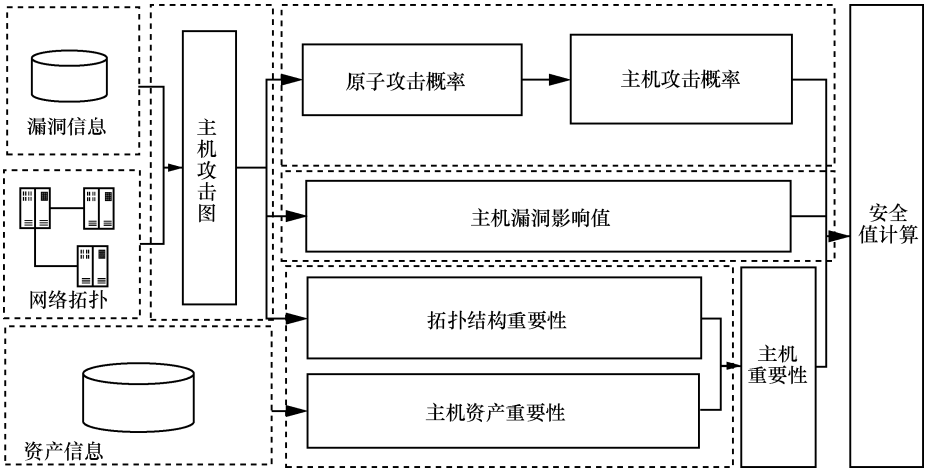

图 1　主机安全评估方法总体架构

合，原子攻击概率表示攻击图中攻击行为迁移的可能性大小，原子攻击概率越大，表示两主机间的攻击行为越容易发生。

2.2　主机攻击图结构建立

根据目标网络采集到的漏洞信息和主机通信访问规则构建主机攻击图[12]，由于真实网络环境下主机的漏洞可能并不唯一，为简化攻击图规模，分析攻击者最可能的攻击意图，当多条边同时指向同一主机时，仅保留原子攻击概率最大漏洞所在的边，主机攻击图示例如图 2 所示。

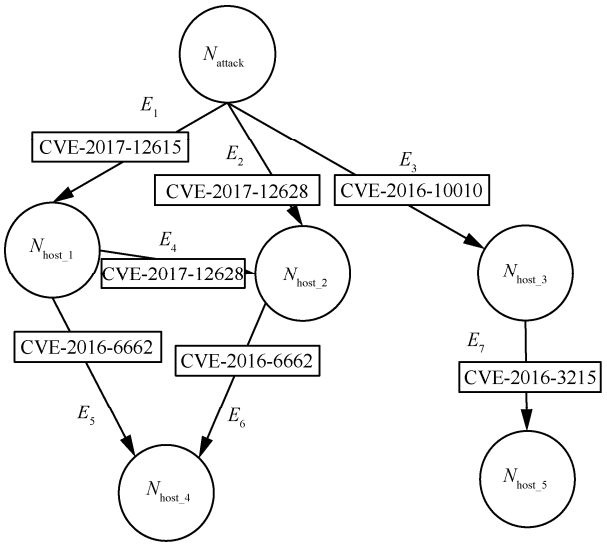

图 2　主机攻击图示例

图 2 中，N_{attack} 表示攻击者所在的攻击主机，N_{host_1}～N_{host_5} 表示网络拓扑中的正常主机，E_1～E_7 表示主机攻击图中的边，边上的漏洞标注了攻击者从前置主机到后置主机利用的漏洞。例如，边 E_1 表示攻击者通过攻击主机 N_{attack} 可以利用主机 N_{host_1} 上的漏洞 CVE-2017-12615 对主机 N_{host_1} 发起攻击并获取权限。

2.3　主机攻击图中概率计算

2.3.1　原子攻击概率计算

漏洞的自身可利用性是影响原子攻击概率取值的重要因素，通常根据通用漏洞评分系统（CVSS, common vulnerability scoring system）[13]进行量化计算。依据 CVSS，漏洞的自身可利用性由攻击途径 V、攻击复杂度 C 及身份认证 U 量化，取值结果为

$$\mathrm{VE}_i = 2V_iC_iU_i \tag{1}$$

其中，VE_i 表示漏洞的自身可利用性；V_i 按本地、邻近拓扑、网络划分为 3 个等级，取值分别为 0.395、0.646、1；C_i 按高、中、低划分为 3 个等级，取值分别为 0.35、0.61、0.71；U_i 按多重、单重和不需要认证划分为 3 个等级，取值分别为 0.45、0.56、0.704。

漏洞的时间可利用性、环境可利用性和所在主机的操作系统类型同样会影响原子攻击概率大小。从时间角度分析，漏洞被发布的时间越长，漏洞被成功利用的可能性则越大。漏洞的时间可利用性（TE, time exploitability）由漏洞代码被利用的可能用性和补丁修复程度共同决定，取值分别满足 Pareto 和 Weibull 分布[14]，即

$$\mathrm{TE}_i = \left(1-\left(\frac{l}{z_i}\right)^r\right)\left(1-\exp\left(-\frac{z_i}{q}\right)^u\right) \tag{2}$$

其中，l 和 r 表示 Pareto 分布系数，取值分别为 0.26 和 0.001 61；q 和 u 表示 Weibull 分布系数，取值分别为 0.209 和 4.04；z_i 表示某一漏洞从公开日期至评估日期的天数。

从漏洞所处环境角度分析，漏洞所处主机的防

御措施完备程度越高，对应原子攻击概率取值越小。本文依据主机防御措施程度划分为高、较高、中、较低和低 5 个等级[15]，漏洞的环境可利用性（EE, environment exploitability）对应取值区间设定为 0～0.2、0.2～0.4、0.4～0.6、0.6～0.8、0.8～1.0。取值越大表示漏洞越容易被利用，范围区间内的具体取值可由评估人员依据各主机实际情况赋值。

从漏洞所在主机的操作系统分析，主机的操作系统安全性越高，则对应原子攻击概率的取值越低。参考文献[16]，本文将主流操作系统划分为 Linux 类系统、苹果主机系统和 Windows 类系统，对应操作系统的可利用性（OSE, operating system exploitability）取值设定为 0.5、0.8、1.0。

依据漏洞的自身可利用性、时间可利用性、环境可利用性和操作系统可利用性，原子攻击概率 P_i 的计算式为

$$P_i = \mathrm{VE}_i \times \mathrm{TE}_i \times \mathrm{EE}_i \times \mathrm{OSE}_i \tag{3}$$

2.3.2 主机攻击概率计算

主机攻击图中的攻击路径直观地表示了攻击者可能采取的所有攻击序列，路径攻击概率从整体角度计算从初始攻击主机到其他主机攻击发生的可能性。以初始攻击主机为起点，各主机为终点，通过深度优先查找所有攻击路径并由路径上所有主机中漏洞的原子攻击概率乘积计算攻击概率，选取攻击概率集合中的最大概率作为各主机的攻击概率，即各主机的最大路径攻击概率为

$$\mathrm{Path}_j = \max\left(\prod_{i=1}^{n} P_i\right) \tag{4}$$

2.4 主机漏洞影响值计算

主机上存在的漏洞会对主机产生影响，各主机的漏洞影响值为主机上全部漏洞产生的影响值之和。依据 CVSS[13]，单个漏洞的影响值（VV, vulnerability impact value）为

$$\mathrm{VV}_i = 10.41\left(1-\left(1-\mathrm{VC}_i\right)\left(1-\mathrm{VI}_i\right)\left(1-\mathrm{VA}_i\right)\right) \tag{5}$$

其中，VC_i、VI_i、VA_i 分别为第 i 个漏洞对主机的机密性、完整性和可用性的影响值，VC_i、VI_i、VA_i 均按无、低、高划分为 3 个等级，取值分别为 0、0.275、0.66。

各主机的漏洞影响值（HV, host node vulnerability impact）为

$$\mathrm{HV}(N_{\mathrm{host}\_i}) = \sum_{j=1}^{n} \mathrm{VV}_j \tag{6}$$

其中，n 表示主机的漏洞个数。

3 主机安全值计算

主机的安全值由攻击概率、漏洞影响值和主机重要性共同决定，其中主机重要性由主机的资产重要性和拓扑结构重要性共同表征。

3.1 主机资产重要性计算

主机的资产重要性通过主机的机密性、完整性和可用性量化，主机资产重要性计算过程设计如下。

步骤 1 依据不同主机的安全需求，根据国家标准《信息安全风险评估规范》[17]，将各主机的资产重要性属性划分为 L_1、L_2、L_3、L_4、L_5 共 5 个等级，更细粒度的划分会增加先验评分难度，导致资产重要性属性等级难以界定，因此资产重要性属性等级不再进一步划分。资产重要性属性取值评价如表 1 所示。

表 1 资产重要性属性取值评价

属性	等级标识	重要性赋值
机密性 C	高（L_1）	5
	较高（L_2）	4
	一般（L_3）	3
	较低（L_4）	2
	低（L_5）	1
完整性 I	高（L_1）	5
	较高（L_2）	4
	一般（L_3）	3
	较低（L_4）	2
	低（L_5）	1
可用性 A	高（L_1）	5
	较高（L_2）	4
	一般（L_3）	3
	较低（L_4）	2
	低（L_5）	1

步骤 2 由 n 位专家依据表 1 对各主机资产重要性的属性进行先验赋值，由赋值结果构造第 j 个主机的资产重要性属性评价矩阵 $\boldsymbol{M}_j$

$$\boldsymbol{M}_j = \begin{pmatrix} m_{1\mathrm{C}} & m_{1\mathrm{I}} & m_{1\mathrm{A}} \\ m_{2\mathrm{C}} & m_{2\mathrm{I}} & m_{2\mathrm{A}} \\ \vdots & \vdots & \vdots \\ m_{n\mathrm{C}} & m_{n\mathrm{I}} & m_{n\mathrm{A}} \end{pmatrix} \tag{7}$$

步骤 3 对属性评价矩阵中的各列元素归一化处理，记处理后评价矩阵各元素为 d_{ik}。由于相关性

定权法[18]能够综合考虑属性间的差异性和相关性，从相对客观角度计算各属性权重，因此本文采用相关性定权法求解资产重要性各属性权重。

1) 第 k 列属性 d 的平均值为

$$\overline{d_k}=\frac{1}{n}\sum_{i=1}^{n}d_{ik} \tag{8}$$

其中，n 为矩阵行数。

2) 第 k 列资产重要性属性的标准差为

$$\eta_k=\sqrt{\frac{1}{n\sum_{i=1}^{n}(d_{ik}-\overline{d_k})^2}} \tag{9}$$

3) 任意两指标间的相关系数为

$$v_{XY}=\frac{\sum_{i=1}^{n}(X_i-\overline{X})(Y_i-\overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i-\overline{X})^2\sum_{i=1}^{n}(Y_i-\overline{Y})^2}} \tag{10}$$

4) 第 k 列属性所含的信息量为

$$\mu_k=\eta_k\sum_{i=1}^{n}(1-v_{ik}) \tag{11}$$

5) 第 j 个主机的第 k 列资产重要性属性的权重为

$$w_{jk}=\frac{\mu_k}{\sum_{k=1}^{3}\mu_k} \tag{12}$$

步骤 4　依据评价矩阵 $\boldsymbol{M}_j$，计算第 j 个主机资产重要性的第 k 个属性的先验评分取值 ATT_{jk}

$$\mathrm{ATT}_{jk}=\frac{1}{n}\sum_{i=1}^{n}m_{ik} \tag{13}$$

步骤 5　计算第j个主机的资产重要性 $\mathrm{AI}(N_{\mathrm{host\_}j})$，如式(14)所示。

$$\mathrm{AI}(N_{\mathrm{host\_}j})=\log\left(\frac{1}{3}\sum_{k=1}^{3}w_{jk}2^{\mathrm{ATT}_{jk}}\right) \tag{14}$$

3.2　主机拓扑结构重要性计算

拓扑结构重要性从主机所在主机攻击图的结构角度分析主机的重要程度。其中拓扑结构重要性由主机的加权中介中心性和局部重要性组成。

加权中介中心性从主机攻击图的整体角度考虑主机的重要程度，在计算时需要计算任意两节点间的最短路径，而原子攻击概率取值越大则表示两节点间越容易到达，因此本文通过原子攻击概率的倒数对主机攻击图加权，然后由式(15)计算各主机 $N_{\mathrm{host\_}i}$ 的加权中介中心性 $\mathrm{FI}(N_{\mathrm{host\_}i})$

$$\mathrm{FI}(N_{\mathrm{host\_}i})=\frac{\sum_{a\neq N_{\mathrm{host\_}i}\neq t}^{n}\sigma(N_{\mathrm{host\_}i})_{at}}{\sigma_{at}} \tag{15}$$

其中，$\sigma(N_{\mathrm{host\_}i})_{at}$ 表示从主机 $N_{\mathrm{host\_}a}$ 到 $N_{\mathrm{host\_}t}$ 的最短路径中经过主机 $N_{\mathrm{host\_}i}$ 的最短路径数，σ_{at} 表示所有从主机 $N_{\mathrm{host\_}a}$ 到 $N_{\mathrm{host\_}t}$ 的最短路径数。

主机的局部重要性从局部角度分析主机的重要程度，根据主机攻击图中各主机和其他主机间的关联关系，由式(16)计算主机 $N_{\mathrm{host\_}i}$ 的局部重要性 $\mathrm{LI}(N_{\mathrm{host\_}i})$

$$\mathrm{LI}(N_{\mathrm{host\_}i})=\frac{g_i+\sum_{j=1}^{b}g_j}{\sum_{i=1}^{n}\left(g_i+\sum_{j=1}^{b}g_j\right)} \tag{16}$$

其中，g_i 表示攻击图中与主机 $N_{\mathrm{host\_}i}$ 相连的边数，g_j 表示与主机 $N_{\mathrm{host\_}i}$ 直接相连的主机所连的边数，b 表示与主机 $N_{\mathrm{host\_}i}$ 直接相连的主机数，n 表示主机攻击图主机数。

根据计算得到的主机的加权中介中心性和局部重要性，由式(17)计算主机拓扑结构重要性 $\mathrm{TI}(N_{\mathrm{host\_}i})$

$$\mathrm{TI}(N_{\mathrm{host\_}i})=\frac{(\mathrm{FI}(N_{\mathrm{host\_}i})+\mathrm{LI}(N_{\mathrm{host\_}i}))}{2} \tag{17}$$

3.3　主机重要性和主机安全值计算

主机重要性由主机资产重要性和主机拓扑结构重要性表征，计算出主机资产重要性和主机拓扑结构重要性后，由式(18)计算各主机的主机重要性 $\mathrm{NI}(N_{\mathrm{host\_}i})$

$$\mathrm{NI}(N_{\mathrm{host\_}i})=\mathrm{TI}(N_{\mathrm{host\_}i})+\mathrm{AI}(N_{\mathrm{host\_}i}) \tag{18}$$

依据计算出的主机攻击概率、漏洞影响值和主机重要性，由式(19)计算各主机的安全值 $\mathrm{NR}(N_{\mathrm{host\_}i})$

$$\mathrm{NR}(N_{\mathrm{host\_}i})=1-\frac{\mathrm{Path}_i(\mathrm{HV}(N_{\mathrm{host\_}i})+\mathrm{NI}(N_{\mathrm{host\_}i}))}{\sum_{i=1}^{n}(\mathrm{Path}_i(\mathrm{HV}(N_{\mathrm{host\_}i})+\mathrm{NI}(N_{\mathrm{host\_}i})))} \tag{19}$$

其中，n 表示主机攻击图中的主机个数。

4　实验与结果分析

4.1　实验环境

为验证本文方法的有效性，在民航机场某业务仿真系统的网络环境中进行验证实验。该仿真系

统由民航某研究所研发，其原型系统已在国内数十家民航机场应用。该仿真系统的硬件平台、网络拓扑和核心功能与国内数十家民航机场实际运行的真实业务系统完全一致。由于该仿真系统是针对目前民航机场广泛运行的典型业务系统的模拟仿真，尚未涉及云计算、虚拟化和 SDN 等应用场景。

该仿真系统的总体抽象层次结构分为数据层、业务逻辑层、消息中间层和业务应用层，各层间相互协作以保障系统正常运行，总体抽象层次结构如图 3 所示。其中，数据层对应系统数据存储区的数据库服务器，负责数据库管理和业务数据支持；业务逻辑层对应系统业务调度区的业务主机等，负责航班业务逻辑抽象、实现和管理；消息中间层对应系统网络布线和系统交互区中提供信息交互的应用服务器等，负责信息内容过滤、系统数据共享和报文收发等；业务应用层对应系统业务调度区、系统监控区和系统交互区中各主机的具体应用和服务等。

该仿真系统的网络拓扑结构如图 4 所示，分为系统交互区、系统业务调度区、数据存储区和系统监控区。

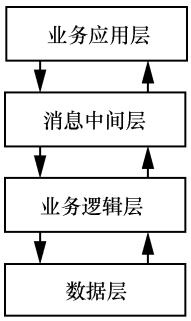

图 3 仿真系统的总体抽象层次结构

各区域提供的功能及服务如下。

1) 系统交互区的主要功能为提供该业务系统与其他业务系统的数据交互服务。其中，管理控制主机 $N_{\text{host\_1}}$ 提供基于 Web 的异常处理和内容过滤服务，应用服务器 $N_{\text{host\_2}}$ 提供多业务单位和部门间的信息交互与数据共享服务，应用服务器 $N_{\text{host\_3}}$ 提供航班运行动态业务信息（如 SITA 报、AFTN 报等）的发送与接收解析等服务。

2) 系统业务调度区的主要功能为处理航班运行业务并进行航班信息管理。其中，业务主机 $N_{\text{host\_4}}$ 提供航班运行业务的基础数据和动态航班等信息

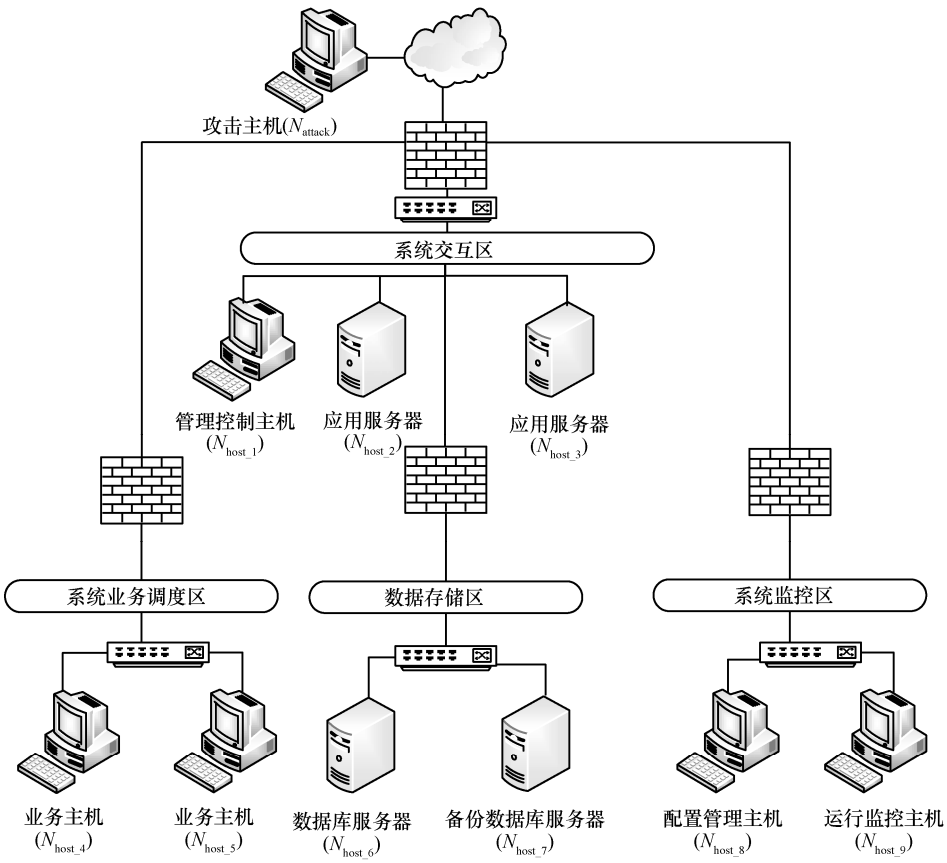

图 4 仿真系统的网络拓扑结构

的发布服务，业务主机 N_{host_5} 提供系统信息管理功能，对航班状态、航班计划和系统资源等信息进行更新和管理。

3) 数据存储区的主要功能为存储机场运行过程中的各类业务数据。其中，数据库服务器 N_{host_6} 存储航班信息的基础数据和动态航班信息及各类业务信息，备份数据库服务器 N_{host_7} 对机场各类业务数据和信息进行备份存储和管理。

4) 系统监控区的主要功能为监控系统运行状态。其中，配置管理主机 N_{host_8} 对系统进行配置管理和航班信息维护，运行监控主机 N_{host_9} 通过运行监控软件监控系统运行状态以保障系统安全平稳运行。

4.2　攻击图生成

首先，利用 Nmap 工具探测上述网络拓扑，获取各主机间的连通关系和漏洞信息。其中各主机间的网络连通关系如表 2 所示。

表 2　　各主机间的网络连通关系

主机	N_{attack}	N_{host_1}	N_{host_2}	N_{host_3}	N_{host_4}	N_{host_5}	N_{host_6}	N_{host_7}	N_{host_8}	N_{host_9}
N_{attack}	—	连通	连通	连通	—	—	—	—	—	—
N_{host_1}	—	—	连通	—	—	—	连通	—	—	—
N_{host_2}	—	—	—	—	—	—	连通	—	—	—
N_{host_3}	—	—	连通	—	连通	连通	—	—	—	—
N_{host_4}	—	—	—	—	—	—	—	—	连通	—
N_{host_5}	—	—	—	—	—	—	连通	—	—	—
N_{host_6}	—	—	—	—	—	—	—	连通	—	—
N_{host_7}	—	—	—	—	—	—	—	—	—	—
N_{host_8}	—	—	—	—	—	连通	—	—	—	连通
N_{host_9}	—	—	—	—	—	连通	—	—	—	—

注：—表示未连通。

然后，依据各主机的漏洞信息，由式(1)计算漏洞自身可利用性 VE，主机漏洞信息如表 3 所示。

最后，依据表 2 和表 3 生成主机攻击图，结果如图 5 所示。从图 5 可知，主机攻击图共包含 10 个节点和 15 条边，分别表示网络拓扑中的主机、主机间的关联关系。

4.3　主机攻击概率和漏洞影响值计算

首先，计算各漏洞原子攻击概率。依据漏洞公开时间，由式(2)计算漏洞时间可利用性。将漏洞自身可利用性、漏洞时间可利用性、漏洞环境可利用性和操作系统可利用性取值代入式(3)，计算得到各漏洞原子攻击概率，结果如图 6 所示。

表 3　　主机漏洞信息

主机	主机名称	漏洞 CVE 标识	VE
N_{host_1}	管理控制主机	CVE-2014-0226(f_1)	0.859
N_{host_2}	应用服务器	CVE-2015-1635(f_2)	1
N_{host_3}	应用服务器	CVE-2015-2578(f_3)	0.859
		CVE-2016-3125(f_4)	1
N_{host_4}	业务主机	CVE-2015-0014(f_5)	1
N_{host_5}	业务主机	CVE-2007-0038(f_6)	0.859
N_{host_6}	数据库服务器	CVE-2016-0639(f_7)	1
		CVE-2016-3471(f_8)	0.392
		CVE-2016-3477(f_9)	0.314
N_{host_7}	备份数据库服务器	CVE-2016-3461(f_{10})	0.315
N_{host_8}	配置管理主机	CVE-2006-2370(f_{11})	1
N_{host_9}	运行监控主机	CVE-2003-0252(f_{12})	1

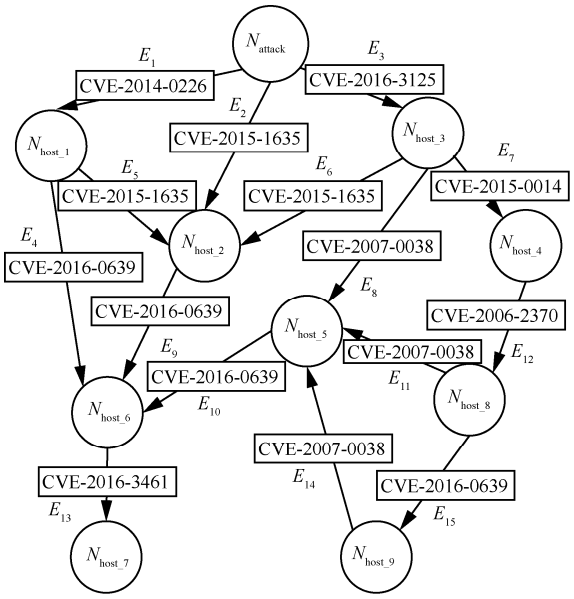

图 5　主机攻击图生成

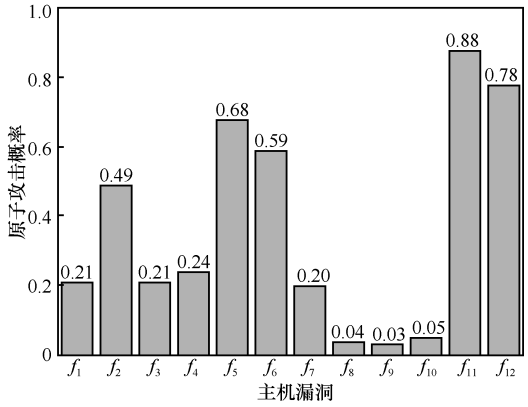

图 6　原子攻击概率

然后，由图 5 查找所有攻击路径，依据图 5 中的原子攻击概率，由式(4)计算得到各主机的最大攻击概率，结果如表 4 所示。

表 4 主机攻击概率

主机	攻击路径	最大攻击概率
N_{host_1}	N_{attack}-N_{host_1}	0.21
N_{host_2}	N_{attack}-N_{host_2} N_{attack}-N_{host_1}-N_{host_2} N_{attack}-N_{host_3}-N_{host_2}	0.49
N_{host_3}	N_{attack}-N_{host_3}	0.24
N_{host_4}	N_{attack}-N_{host_3}-N_{host_4}	0.16
N_{host_5}	N_{attack}-N_{host_3}-N_{host_5} N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_5} N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_9}-N_{host_5}	0.14
N_{host_6}	N_{attack}-N_{host_1}-N_{host_6} N_{attack}-N_{host_2}-N_{host_6} N_{attack}-N_{host_1}-N_{host_2}-N_{host_6} N_{attack}-N_{host_3}-N_{host_2}-N_{host_6} N_{attack}-N_{host_3}-N_{host_5}-N_{host_6} N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_5}-N_{host_6} N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_9}-N_{host_5}-N_{host_6}	0.1
N_{host_7}	N_{attack}-N_{host_1}-N_{host_6}-N_{host_7} N_{attack}-N_{host_2}-N_{host_6}-N_{host_7} N_{attack}-N_{host_1}-N_{host_2}-N_{host_6}-N_{host_7} N_{attack}-N_{host_3}-N_{host_2}-N_{host_6}-N_{host_7} N_{attack}-N_{host_3}-N_{host_5}-N_{host_6}-N_{host_7} N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_5}-N_{host_6}-N_{host_7} N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_9}-N_{host_5}-N_{host_6}-N_{host_7}	0.005
N_{host_8}	N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}	0.14
N_{host_9}	N_{attack}-N_{host_3}-N_{host_4}-N_{host_8}-N_{host_9}	0.11

最后，依据表 3 各主机漏洞信息，由式(5)和式(6)计算得到各主机的漏洞影响值，结果如表 5 所示。

4.4 主机重要性和安全值计算

首先，计算各主机的资产重要性和拓扑结构重要性。以主机 N_{host_1} 为例说明主机资产重要性的计算流程。由 5 位专家依据表 1 对主机 N_{host_1} 的资产重要性属性进行先验评分赋值，由先验赋值结果构建主机 N_{host_1} 的资产重要性属性矩阵 $\boldsymbol{M}_1$

$$\boldsymbol{M}_1=\begin{pmatrix}2&2&4\\2&2&4\\3&3&4\\2&2&3\\2&3&4\end{pmatrix}$$

将矩阵 $\boldsymbol{M}_1$ 各列元素归一化处理后，依据式(8)～式(12)计算主机 N_{host_1} 的资产重要性属性权重，分别为(0.309 2, 0.326 0, 0.364 7)。由式(13)计算得到主机 N_{host_1} 的各资产重要性属性评分取值分别为(2.2, 2.4, 3.8)，将计算得到的属性权重和属性评分取值代入式(14)计算得到主机 N_{host_1} 的资产重要性为 3.04。同理计算其余 8 个主机的资产重要性属性权重和资产重要性，得到 9 个主机的资产重要性属性权重和资产重要性如表 6 所示。

表 5 主机漏洞影响值

主机	漏洞影响值
N_{host_1}	6.4
N_{host_2}	10
N_{host_3}	9.8
N_{host_4}	10
N_{host_5}	10
N_{host_6}	26.4
N_{host_7}	6.4
N_{host_8}	6.4
N_{host_9}	10

表 6 主机资产重要性属性权重和资产重要性

主机	C	I	A	资产重要性
N_{host_1}	0.309 2	0.326 0	0.364 7	3.04
N_{host_2}	0.297 2	0.338 7	0.346 1	3.03
N_{host_3}	0.274 3	0.360 6	0.365 1	3.22
N_{host_4}	0.377 7	0.344 2	0.278 1	1.85
N_{host_5}	0.287 6	0.366 1	0.346 4	2.33
N_{host_6}	0.178 2	0.517 9	0.303 9	4.06
N_{host_7}	0.386 6	0.364 6	0.248 8	4.61
N_{host_8}	0.189 1	0.408 9	0.402 1	2.5
N_{host_9}	0.308 7	0.380 6	0.310 7	1.67

然后，依据 3.2 节中的方法得到加权后的主机攻击图，由式(15)和式(16)计算出各主机的加权中介中心性和局部重要性，代入式(17)得到各主机的拓扑结构重要性，结果如表 7 所示。

表 7 主机拓扑结构重要性

主机	加权中介中心性	局部重要性	拓扑结构重要性
N_{host_1}	0	0.11	0.05
N_{host_2}	2	0.14	1.07
N_{host_3}	4	0.13	2.06
N_{host_4}	8	0.07	4.03
N_{host_5}	4	0.13	2.06
N_{host_6}	8	0.12	4.06
N_{host_7}	6	0.04	3.02
N_{host_8}	0	0.08	0.04
N_{host_9}	0	0.07	0.03

将表 6 和表 7 中的主机资产重要性和拓扑结构重要性代入式(18)，计算得到主机重要性，将表 4 中各主机攻击概率和计算出的主机重要性代入式(19)，计算得到各主机的安全值，结果如图 7 所示。

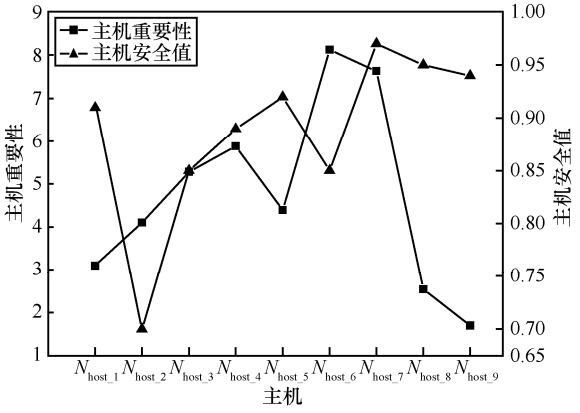

图 7　主机重要性和主机安全值

由图 7 可知，1) 9 个主机的主机重要性排序结果为 NI(N_{host_6})> NI(N_{host_7})>NI(N_{host_4})> NI(N_{host3})> NI(N_{host_5})> NI(N_{host_2})> NI(N_{host_1})> NI(N_{host_8})> NI(N_{host_9})，表明在综合考虑主机资产重要性和拓扑结构重要性后，主机 N_{host_6} 相比于其他主机更重要；2) 9 个主机的安全值排序结果为 NR(N_{host_2})< NR(N_{host_3}) <NR(N_{host_6}) <NR(N_{host_4}) <NR(N_{host_1})< NR(N_{host_5})< NR(N_{host_9})<NR(N_{host_8})<NR(N_{host_7})，表明在综合考虑主机的主机重要性、漏洞影响值和攻击概率后，主机 N_{host_2} 的安全值最低。

上述结果与实验所用仿真系统对应的机场某真实业务系统的网络真实情况一致，且与真实系统的多次安全评估结果一致。因此本文方法能够有效分析不同主机的重要性并对各主机的安全状况进行量化评估。

4.5　原子攻击概率对比

原子攻击概率表示攻击图中攻击行为迁移的可能性大小，为证明本文方法计算原子攻击概率的合理性，将本文方法、CVSS 方法和文献[7]方法中依照时间划分得到的原子攻击概率进行对比，如表 8 所示。

由表 8 可知，CVSS 方法和文献[7]方法仅从单一角度考虑漏洞被利用的可能性，忽略了漏洞所处主机环境因素和主机操作系统类型对原子攻击概率的影响，导致计算结果并不准确。例如，由 CVSS 方法计算得到的漏洞 f_2、f_4、f_5、f_7、f_{11} 和 f_{12} 的漏洞原子攻击概率均为 1，由文献[7]方法计算得到的漏洞 f_1～f_7、f_{11} 和 f_{12} 的漏洞原子攻击概率均为 0.9。而在实际系统的网络环境中，上述漏洞发布时间不同，且漏洞分别位于不同主机中，原子攻击概率均相同，显然不合理。本文方法综合考虑漏洞自身可利用性、时间可利用性、环境可利用性和操作系统类型，计算出的漏洞原子攻击概率值更符合真实网络中漏洞被利用的情况。

表 8　　原子攻击概率对比

漏洞	本文方法	CVSS 方法	文献[7]方法
f_1	0.21	0.859	0.9
f_2	0.49	1	0.9
f_3	0.21	0.859	0.9
f_4	0.24	1	0.9
f_5	0.68	1	0.9
f_6	0.59	0.859	0.9
f_7	0.20	1	0.9
f_8	0.003 8	0.392	0.5
f_9	0.003 1	0.314	0.5
f_{10}	0.05	0.315	0.5
f_{11}	0.88	1	0.9
f_{12}	0.78	1	0.9

4.6　主机资产重要性评估对比

为验证本文方法计算主机资产重要性的合理性，在图 4 所示的网络拓扑结构下，分别采用本文方法、层次分析法[4]和先验评分法计算各主机资产重要性，结果如图 8 所示。

由图 8 可知，本文方法计算出的主机资产重要性值更合理，因为本文方法充分考虑主机资产重要性不同属性所占权重，在先验评分赋值的基础上采用相关性定权法为各主机资产重要性的不同属性权重赋值；层次分析法和先验评分法为所有主机资产重要性的所有属性采用相同权重计算，计算结果并不合理。

4.7　主机安全评估对比

主机安全值能够反映主机当前的安全状况，取值越小表明主机的安全状况越差。为证明本文方法的优越性，在相同实验环境下，采用资产连通图方法[5]、Markov 攻击图方法[6]和邻接矩阵法[12]3 种主机安全评估方法计算主机安全值，4 种方法归一化后的安全值如图 9 所示。

由图 9 可知，本文方法得到的各主机安全值更准确合理。原因分析如下。

1) Markov 攻击图方法仅以迭代后的攻击可能

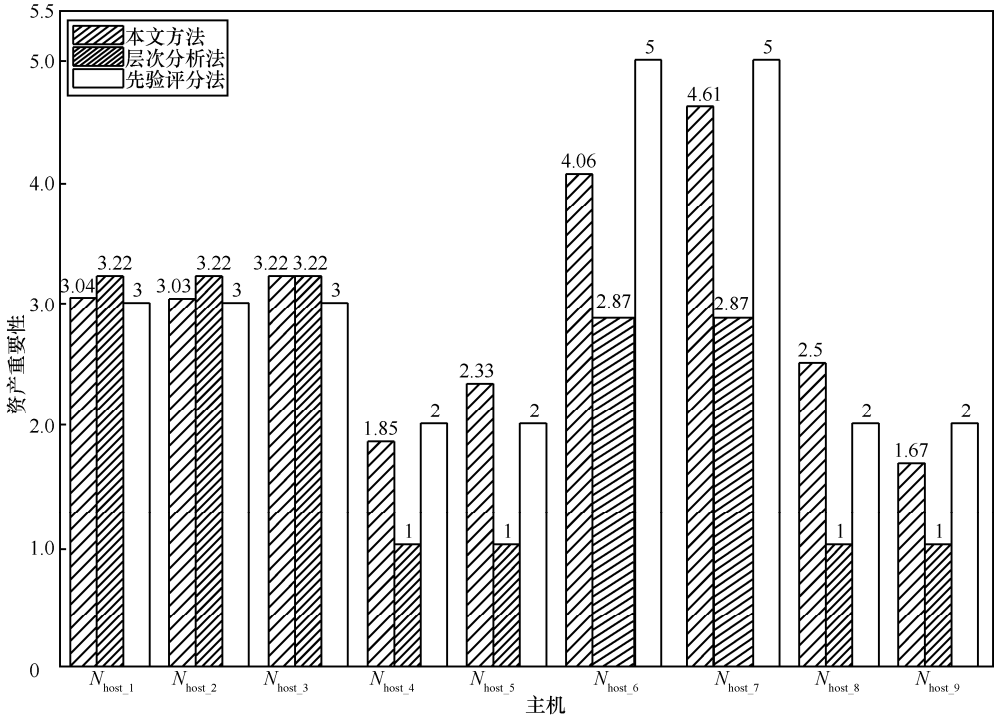

图 8　主机资产重要性对比

性作为评估各主机安全性的指标，无法准确区分各主机的安全和风险状况。

2) 邻接矩阵法和资产连通图方法依据主机的攻击概率和资产重要性计算主机安全值，但均未考虑主机资产重要性属性的权重差异性和攻击图中各主机间的关系，安全值计算不够准确。

3) 本文方法从主机攻击概率、漏洞影响值、资产重要性和拓扑结构重要性方面对主机进行安全评估，能够更全面、更准确地反映各主机的安全状况。

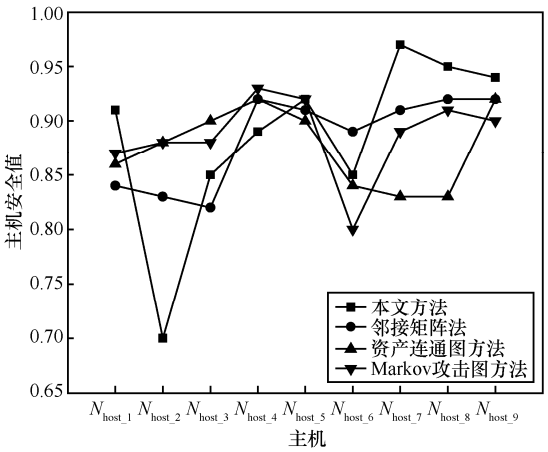

图 9　不同方法的主机安全值对比

标准差的大小反映了数据间的离散程度，安全值的标准差越大，表明数据离散程度越大，其益处是对安全等级的区分度越明显，越易于区分并划分主机的安全和风险等级。

为进一步证明本文方法的优势，在得到主机安全值的基础上，分别计算 4 种方法的主机安全值的标准差，结果如表 9 所示。

表 9　　主机安全值的标准差

方法	标准差
本文方法	0.078
邻接矩阵法	0.042
资产连通图方法	0.036
Markov 攻击图方法	0.037

由表 9 可知，本文方法得到的主机安全值的标准差比其他 3 种方法得到的安全值标准差分别增加了 85.7%、116.7%和 110.8%，说明本文方法得到的主机安全值离散程度更大、区间分布也更大，可以更显著地表征不同主机安全值的差异性，更便于划分主机的安全等级，从而有利于高效处置主机风险和网络风险。

5　结束语

为合理有效地评估网络中主机的安全状况，本文提出一种基于攻击图的主机安全评估方法。在构建主机攻击图的基础上，依据漏洞的多个属性值计算原子攻击概率，依据攻击图、相关性定权法得到

主机的攻击概率、漏洞影响值、主机资产重要性和拓扑结构重要性，进而计算得到主机的安全值。

通过民航机场某业务仿真系统环境下的验证实验，验证了本文方法在真实系统网络环境下的可行性和有效性。与其他方法相比，本文方法能够合理计算主机攻击概率、漏洞影响值、资产重要性和拓扑结构重要性，可以全面、准确地反映主机的安全状况。

未来，将进一步细化主机资产重要性评价指标，从主机安全管理角度进一步完善主机安全评估的针对性，提高该方法在复杂网络环境中的适用性。此外，将针对云计算和虚拟化环境的特点，重点研究云计算和虚拟化应用场景下的网络安全评估模型和基于 SDN 环境的网络主机安全评估方法，提出适用于云计算和SDN环境的安全评估解决方案。

参考文献：

[1] 吴晨思, 谢卫强, 姬逸潇, 等. 网络系统安全度量综述[J]. 通信学报, 2019, 40(6): 14-31.
WU C S, XIE W Q, JI Y X, et al. Survey on network system security metrics[J]. Journal on Communications, 2019, 40(6): 14-31.

[2] 丁绍虎, 齐宁, 郭义伟. 基于 M-FlipIt 博弈模型的拟态防御策略评估[J]. 通信学报, 2020, 41(7): 186-194.
DING S H, QI N, GUO Y W. Evaluation of mimic defense strategy based on M-FlipIt game model[J]. Journal on Communications, 2020, 41(7): 186-194.

[3] 罗智勇, 杨旭, 刘嘉辉, 等. 基于贝叶斯攻击图的网络入侵意图分析模型[J]. 通信学报, 2020, 41(9): 160-169.
LUO Z Y, YANG X, LIU J H, et al. Network intrusion intention analysis model based on Bayesian attack graph[J]. Journal on Communications, 2020, 41(9): 160-169.

[4] 席荣荣, 云晓春, 张永铮. 基于环境属性的网络威胁态势量化评估方法[J]. 软件学报, 2015, 26(7): 1638-1649.
XI R R, YUN X C, ZHANG Y Z. Quantitative threat situational assessment based on contextual information[J]. Journal of Software, 2015, 26(7): 1638-1649.

[5] SHAN C, GAO J, HU C Z, et al. Network risk assessment method based on asset correlation graph[C]//Trusted Computing and Information Security. Berlin: Springer, 2019: 65-83.

[6] POKHREL N R, TSOKOS C P. Cybersecurity: a stochastic predictive model to determine overall network security risk using Markovian process[J]. Journal of Information Security, 2017, 8(2): 91-105.

[7] 李欢. 基于贝叶斯网络攻击图的动态风险评估方法研究[D]. 秦皇岛: 燕山大学, 2019.
LI H. Research on dynamic risk assessment method based on Bayesian network attack diagram[D]. Qinhuangdao: Yanshan University, 2019.

[8] HU H, ZHANG H Q, YANG Y J. Security risk situation quantification method based on threat prediction for multimedia communication network[J]. Multimedia Tools and Applications, 2018, 77(16): 21693-21723.

[9] HU W H, ZHANG L, LIU X Y, et al. Research on automatic generation and analysis technology of network attack graph[C]//Proceedings of 2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security. Piscataway: IEEE Press, 2020: 133-139.

[10] WANG W R, SHI F, ZHANG M, et al. A vulnerability risk assessment method based on heterogeneous information network[J]. IEEE Access, 2020, 8: 148315-148330.

[11] SUN X Y, DAI J, LIU P, et al. Using Bayesian networks for probabilistic identification of zero-day attack paths[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(10): 2506-2521.

[12] 李鑫. 基于攻击图的网络安全评估技术研究与实现[D]. 北京: 北京邮电大学, 2017.
LI X. Research and implementation of network security assessment technology based on attack graph[D]. Beijing: Beijing University of Posts and Telecommunications, 2017.

[13] RUOHONEN J. A look at the time delays in CVSS vulnerability scoring[J]. Applied Computing and Informatics, 2019, 15(2): 129-135.

[14] FREI S, MAY M, FIEDLER U, et al. Large-scale vulnerability analysis[C]//Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense - LSAD'06. New York: ACM Press, 2006: 131-138.

[15] 葛海慧. 信息安全风险多维动态管理模型及相关评估方法研究[D]. 北京: 北京邮电大学, 2015.
GE H H. Research on the multidimensional and dynamic information security risk management model and the related assessment algorithms[D]. Beijing: Beijing University of Posts and Telecommunications, 2015.

[16] WANG R Y, GAO L, SUN Q, et al. An improved CVSS-based vulnerability scoring mechanism[C]//Proceedings of 2011 Third International Conference on Multimedia Information Networking and Security. Piscataway: IEEE Press, 2011: 352-355.

[17] 国家质量监督检验检疫总局, 中国国家标准化管理委员会. 信息安全技术信息安全风险评估规范: GB/T 20984−2007[S]. 北京: 中国标准出版社, 2007.
General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China, Standardization Administration of the People's Republic of China. Information security technology-risk assessment specification for information security: GB/T 20984−2007[S]. Beijing: Standards Press of China, 2007.

[18] 周爱民, 周彩霞, 欧阳晋焱, 等. 基于指标适度标准化的界面风格美综合评价模型[J]. 浙江大学学报(工学版), 2020, 54(12): 2273-2285.
ZHOU A M, ZHOU C X, OUYANG J Y, et al. Model of synthetic evaluation on interface stylistic beauty based on moderately standardized of index[J]. Journal of Zhejiang University (Engineering Science), 2020, 54(12): 2273-2285.

[作者简介]

杨宏宇（1969− ），男，吉林长春人，博士，中国民航大学教授，主要研究方向为网络与系统安全。

袁海航（1997− ），男，山东济宁人，中国民航大学硕士生，主要研究方向为网络与系统安全。

张良（1987− ），男，天津人，博士，亚利桑那大学博士后研究员，主要研究方向为强化学习和基于深度学习的信号处理。