小 型 微 型 计 算 机 系 统
Journal of Chinese Computer Systems
DOI:10.20009/j.cnki.21-1106/TP.2025-0076
2026 年 4 月 第 4 期
Vol.47 No.4 2026

利用贝叶斯网络改进执行体调度算法的研究

刘太昆[1],李 彧[1],李召召[1],胡晶晶[1,2],张 艺[1,3]

[1](紫金山实验室,南京 211111)
[2](东南大学 网络空间安全学院,南京 211189)
[3](东南大学 信息科学与工程学院,南京 211189)
E-mail:liyu@pmlabs.com.cn

摘 要: 在拟态防御系统中,异构执行体的动态调度机制是实现系统动态防御能力的关键.然而,现有的调度方法存在一定局限性,难以有效应对同步协同攻击,从而被突破防御.为了解决这些问题,本文提出了一种基于贝叶斯网络的异构执行体异构度度量方法,并设计了一种新型执行体调度算法.该算法综合考虑了网络攻击的成功概率及异构执行体之间的共模漏洞,通过贝叶斯网络量化异构体间的异构度,基于所得异构度确定最优的执行体调度集合.为了验证所提方法的有效性,本文设计了仿真碰撞实验,并与现有调度方法进行了对比.实验结果表明,在特定攻击成功概率和随机攻击条件下,本文方法展现出更强的环境适应性和动态防御能力.

关 键 词: 异构度;贝叶斯网络;执行体调度;动态异构冗余;拟态防御
中图分类号: TP309 **文献标识码:** A **文 章 编 号:** 1000-1220(2026)04-0937-07

Research on Improving Executive Dynamic Scheduling Algorithm Using Bayesian Network

LIU Taikun[1],LI Yu[1],LI Zhaozhao[1],HU Jingjing[1,2],ZHANG Yi[1,3]

[1](Purple Mountain Laboratories,Nanjing 211111,China)
[2](School of Cyber Science and Engineering,Southeast University,Nanjing 211189,China)
[3](School of Information Science and Engineering,Southeast University,Nanjing 211189,China)

Abstract: In mimic defense systems,heterogeneous executors with their dynamic scheduling mechanism being crucial for realizing the system's dynamic defense capabilities. However,existing scheduling methods have some limitations that struggle to effectively counter synchronized and coordinated attacks. To address these challenges,this paper proposes a Bayesian network-based method for measuring the heterogeneity of heterogeneous executors and introduces a novel executor scheduling algorithm. The proposed algorithm comprehensively considers both the probability of network attacks and the common-mode vulnerabilities among executors,quantifying their heterogeneity via Bayesian networks. It dynamically ranks the executors and determines the optimal scheduling set. To validate the proposed method,a simulation collision experiment is designed and compared with existing scheduling approaches. The experimental results demonstrate that,under specific attack success probabilities and random attack conditions,the proposed method exhibits superior environmental adaptability and dynamic defense capabilities.

Keywords: heterogeneity;Bayesian network;executive scheduling;dynamic heterogeneous redundancy;mimic defense

0 引 言

目前网络空间安全问题日益严峻,网络攻击事件发生越来越频繁,尤其在金融服务、人工智能等领域带来了极大的风险.为应对网络空间易攻难守的局面,邬江兴院士提出了网络空间拟态防御(CMD,cyber mimic defense)通过异构冗余和动态反馈机制构建防御系统[1,2].其核心是动态异构冗余(DHR,dynamic heterogeneous redundancy)架构,以主动变迁的方式实现优秀的防御效果,进而实现主动防御,提高系统防御能力[3,4].执行体的调度机制是 DHR 系统的核心,优秀的调度算法具有更强的动态性和安全性,使攻击者无法对当前运行防御策略造成严重的攻击效果[5,6].围绕调度算法的优化问题,已有很多学者提出了相应的解决方案.文献[7]和[8]提出了利用反馈动态调度执行体的方法,提高执行体调度的动态性和系统安全性.文献[9]提出了基于异构执行体相似性的高阶异构度计算方法.目前在 DHR 系统中对于执行体的调度方法大都缺少了网络环境和漏洞攻击发生以及成功的概率的相关考虑.以漏洞类型和数量的差异性来衡量表征执行体之间的异构度,面对多个漏洞威胁协同攻击时,目前的调度方法存在不足.此外,执行体中往往存在一些未知的漏洞无法被详细衡量[10].本文主要的研究工作如下.

1)基于网络系统的不确定性,提出了复杂网络环境和协同攻击情况下衡量执行体间异构性的方法.

2)提出了一种考虑网络不确定性和网络攻击成功概率

收稿日期:2025-02-25 收修改稿日期:2025-03-25 基金项目:国家重点研发计划项目(2022YFB3104300)资助. 作者简介:刘太昆,男,1987 年生,硕士,工程师,研究方向为网络空间安全和拟态防御;李 彧(通信作者),男,1979 年生,博士,高级工程师,研究方向为网络空间安全、集成电路设计;李召召,男,1989 年生,博士,工程师,研究方向为网络空间安全、软件定义互连;胡晶晶,女,1992 年生,博士研究生,高级工程师,研究方向为网络安全理论与技术;张 艺,女,1991 年生,博士研究生,高级工程师,研究方向为高效基带算法与实现.

的调度算法,解决同时针对多种漏洞协同攻击时,执行体和网络环境之间相互影响的问题.

3)通过进行碰撞实验的仿真,对不同调度算法进行对比评估,验证了基于贝叶斯网络的调度算法所具有的安全优势和动态性.

根据贝叶斯网络的相关理论[11,12],本文从攻击者攻击概率以及攻击成功概率的角度利用贝叶斯网络对 DHR 系统中执行体之间的异构性进行量化,并设计相应的调度算法,进而实现主动防御的动态性.

1 基于贝叶斯网络的异构性量化方法

1.1 基于差异性的异构性量化方法存在的问题

对于动态异构冗余架构中执行体调度算法的研究,使用的异构度指标通常为二阶异构度或者高阶异构度,其通过相互比较执行体之间的差异程度并对其值求和的方法进行计算执行体整体间的差异性和复杂性[13]. 攻击者攻击成功率与执行体漏洞可利用性、漏洞时间可用性以及漏洞来源等维度有关,不同的漏洞其对应的攻击成功率不同,并且攻击往往是同步协同,非简单针对单一漏洞的. 此方法仅考虑执行体漏洞情况,而未考虑执行体所遭受攻击者协同攻击的因素,具有局限性,容易造成系统出现更多的被攻破机会[14,15]. 下面举例进行分析.

在 n 模冗余集合中,执行体相似性由所有不同元素两两之间的相似度之和归一化表征异构度. 假设有 4 个执行体,其编号分别为 1 ~4,存在的漏洞情况如表 1 所示.

表 1 执行体中存在的漏洞情况

Table 1 Vulnerabilities in the executors

执行体编号	漏洞编号
1	1,2,3,4,5
2	3,5,7,8,9
3	1,5,9,10,11
4	1,2,7,8,9

假设当前需要调度执行体的数量是 3,当系统选中执行体 1,2 和 4 时,执行体之间相似度最小,系统整体共模漏洞为 0,按照相似度表征执行体异构性的方法,此时执行体之间异构度最大,此选择为最优解. 当针对漏洞 1 和漏洞 3 的协同攻击成功概率增加时,执行体 1、2 和 4 所组成的系统被攻破的概率就会增加,因此只有当概率最低时此调度选择才是最优解. 由此可知执行体调度选择过程中需要根据不同漏洞同步攻击成功概率进行调度才是最优解. 本文根据贝叶斯网络在信息安全态势中的应用场景[12],通过贝叶斯网络进行评估网络环境中针对不同漏洞类型的攻击成功概率,量化执行体异构性,进而达到动态适应网络环境的目的.

1.2 基于贝叶斯网络的异构性量化方法

当拟态防御系统共有 n 个异构执行体,为了定量化描述 n 个执行体之间的异构度,设置特征测试向量 W,向量中元素包含执行体所处网络环境中的威胁类型、硬件波动以及威胁相关的征兆事件等. 利用测试向量对执行体进行测试,可以获得测试结果,对测试结果进行量化,则可以得到在包含了测试向量 W 的网络环境中 n 个执行体的响应函数,此响应函数反映出不同结构的执行体在网络环境中的综合表现,故函数值中包含了执行体之间的异构性和网络环境之间相互作用等信息.

利用测试向量分别对执行体进行测试,对测试过程进行贝叶斯概率分析综合,将得到的响应函数值进行量化,将其值称为贝叶斯异构度. 根据生成贝叶斯攻击图的原理[16],类似地由测试向量和执行体之间的关系生成贝叶斯网络图,可以表示为 $BAG=(S/U,E,P)$,具体定义如下.

1)S/U 是条件节点集合. 其中 S_0 为初始节点,作为测试向量 W 的发起节点,是网络中的祖节点. 其中二层节点为执行体,对于包含 n 个执行体的动态异构冗余系统,共有 n 个节点,S_0 是网络中二层节点的父节点. 三层节点为测试向量作用于 n 个执行体时,所观察测量的最小作用单元,共有 m 个节点. 对于多数表决一致算法的 DHR 系统,m 和 n 满足 $m=C_n^{(n+1)/2}$,其中 n 为奇数,最小作用单元里包含执行体的数量为$(n+1)/2$,即包含了大多数个执行体. 对于全体一致表决算法的 DHR 系统,则 $m=1$,即最小作用单元中包含了全部的 n 个执行体.

2)E 是贝叶斯网络图的有向边集合. 它表示节点间的因果关系,即每一条有向边的起点是其终点的前置条件,这是条件节点的迁移方式. 当测试向量 W 作用于 n 个执行体,从起始节点 S_0 有 n 条路径可以到达不同的执行体. 随着网络环境的变化,路径的内容跟着变化. 在实际网络环境中,受到网络威胁类型,软硬件布置以及各种因素的影响下,测试向量中的内容将会到达执行体,记 E_n 为系统到达 S_n 节点的有向边.

3)P 为贝叶斯网络图中条件节点可达概率的集合. $P(W)$表示测试向量 W 的概率,即向量中各个元素发生的概率. $P(E)$表示有向边的概率,即在测试向量元素发生的前提下,到达执行体的概率. 二层节点 $P(S)$表示到达执行体节点的概率,即执行体被测试向量占有的概率. 三层节点 $P(U)$表示到达由执行体所组成的最小作用单元的概率,当最小作用单元中所有执行体节点都被占有时,即为最小作用单元被占有. 以 4 个执行体为例,其贝叶斯网络图示例如图 1 所示. 图中 S_0 是起点,表示测试向量对执行体的测试攻击起始点. 示例中有 4 个执行体,S_1,S_2,S_3,S_4 是执行体节点,E_1,E_2,E_3,E_4 是到达执行体的有向边,即测试向量占有 S_0 之后对执行体攻击的路径,$P(E_1)$,$P(E_2)$,$P(E_3)$,$P(E_4)$是测试向量攻击各

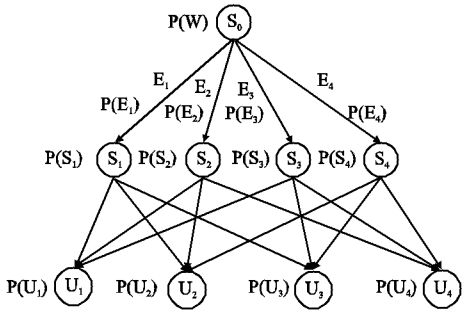

图 1 贝叶斯网络图示例

Fig. 1 Example of a bayesian network diagram

个执行体的概率. $P(S_1)$,$P(S_2)$,$P(S_3)$,$P(S_4)$是测试向量占有执行体节点的概率. U_1,U_2,U_3,U_4 是最小作用单元节点,

有向边代表单元所包含执行体,例如 U_1 包含了 1、2 和 3 这 3 个执行体,故存在 S_1, S_2, S_3 节点到达 U_1 的有向边,且概率为 1.

记 $Par(S_j)$ 表示节点 S_j 的父节点集合,$\{E_{i+1}, E_{i+2}, \cdots, E_{i+m}\}$ 为连接 S_j 和 $Par(S_j)$ 的有向边集合,$P(S_j|Par(S_j))$ 表示节点 S_j 在其父节点集合影响下的条件概率,是其被测试向量占有的概率. 利用贝叶斯网络中各个节点的条件概率和执行体被测试向量占有的概率以及节点之间的逻辑关系,则可以计算出每个节点的可达概率,便可用于量化执行体间的异构性. 三层节点在其父节点集合影响下的条件概率计算公式为:

$$P(U_j=1|Par(U_j)) = \prod_{k=1}^{(n+1)/2} P(U_j|S_k=1) \tag{1}$$

式(1)中包含了节点之间的因果逻辑关系. 二层节点在其父节点集合即测试向量集合影响下的条件概率计算公式为:

$$P(S_i=1|Par(S_i)) = P(S_i|S_0)P(S_0) \tag{2}$$

利用贝叶斯网络图中各个节点的条件概率和执行体在测试向量作用下的响应结果,可以计算出每个三层节点的可达概率. 记最小作用单元里面包含执行体的数量为 k,其满足 $k=(n+1)/2$,可知最小作用单元节点的父节点数量同样为 k,测试向量同时作用于所有执行体,三层节点共有 $k+1$ 个祖节点,记为 $\{S_i, S_{i+1}, \cdots, S_{i+k}\}$,由条件概率计算方法可得三层节点的可达概率计算公式:

$$\begin{aligned} P(U_j) &= P(U_j=1|Par(U_j)) \prod_{x=0}^{k-1} P(S_{i+x}|Par(S_{i+x})) \\ &= P(U_j=1|Par(U_j)) \prod_{x=0}^{k-1} P(S_{i+x}|S_0) \end{aligned} \tag{3}$$

将式(1)和式(2)代入式(3)即可得到三层节点的可达概率:

$$P(U_j) = \prod_{k=1}^{(n+1)/2} P(U_j|S_k=1) \prod_{x=0}^{k-1} P(E_{i+x}) P(W)^k \tag{4}$$

系统中执行体共可以组成 m 个最小作用单元,即贝叶斯网络中有 m 个三层节点,每一个节点的可达概率都包含了执行体在测试向量作用下的响应结果以及测试向量的概率分布等信息. 每个最小作用单元对所要衡量执行体间的异构性影响程度不同,用 r_j 表示权重系数,当所有最小作用单元相互之间没有差异时 $r_j=1$. X 为修正系数,因执行体个数而异,$P_{Par_i}(E_x)$ 表示 i 个执行体的所有最小作用单元在测试向量作用条件下第 x 个执行体被攻破的概率,即有向边 E_x 的概率,归纳可以得到修正系数公式为:

$$X = \sum_{i=k+1}^{n} (i-1) P(W)^i \prod_{x=1}^{i} P_{Par_i}(E_x) \tag{5}$$

其在测试向量 W 作用下的异构性量化公式为:

$$R_W = \sum_{j=1}^{m} r_j P(U_j) - X \tag{6}$$

将修正系数代入式(6)可以得到:

$$R_W = \sum_{j=1}^{m} r_j P(U_j) - \sum_{i=k+1}^{n} (i-1) P(W)^i \prod_{x=1}^{i} P_{Par_i}(E_x) \tag{7}$$

当测试向量 W 中有 t 个元素进行测试时,计算在每一个元素作用下的异构度量化值 R_W,则执行体之间的异构度量化值为:

$$R = \sum_{W=1}^{t} R_W \tag{8}$$

执行体异构性与量化值 R 之间为反比例关系,故执行体贝叶斯异构度为:

$$R = 1/\sum_{W=1}^{t} R_W \tag{9}$$

量化值越小表示执行体组成的系统被攻破的概率越小,异构度越大. 当 $R=0$ 时表示在当前测试向量条件下执行体不可能被攻破,贝叶斯异构度达到理论无限大.

相较于现有执行体异构性的量化方法,贝叶斯网络可以将不同异构执行体中的漏洞连接在一起,直观展示不同攻击步骤的因果关系,更符合当今多步协同攻击为主的现状.

对于不同的网络环境,测试向量的设计会有差异,从贝叶斯异构度量化公式可以看到,执行体在不同网络环境中的异构性将会不同,随着网络环境中测试向量而差异,这反映了贝叶斯异构度的动态性. 测试向量的完备性越高,经其量化的异构度将越准确,当设计出完备的测试向量时,贝叶斯异构度将无限准确地量化执行体之间的异构性. 根据式(8)和式(9)量化的执行体异构性是动态的,可以更准确地体现出执行体在不同运行环境中的特点和差异,在主动防御的拟态调度领域,将会更有利于增加系统的安全性.

1.3　基于网络威胁后验概率的异构度分析

贝叶斯理论利用样本和未知参数的先验信息得出后验信息,再根据获得的样本信息推导未知参数. 贝叶斯定理本质是在无法确定知晓某个事件的实质性质之前,能够结合与事件特定本质有关的事件发生的概率确定其本质属性的概率. 假设实际网络威胁为 θ,其先验概率为 $P(\theta)$,$X=(X_1, X_2, \cdots, X_n)$ 是威胁 θ 的特征向量,其各个分量从各自的策略描述威胁 θ,假设得到一个事件样本 $x=(x_1, x_2, \cdots, x_n)$,那么由贝叶斯概率公式可以得到威胁发生的后验概率 $P(\theta|x)$ 为:

$$P(\theta|x) = (P(x|\theta) \times P(\theta) / \sum_{i=1}^{n} P(x_i|\theta) P(\theta) \tag{10}$$

稍微更改一下,变为:

$$P(\theta|x) = (P(x|\theta) / \sum_{i=1}^{n} P(x_i|\theta) P(\theta)) P(\theta) = \lambda P(\theta) \tag{11}$$

其中 $P(\theta)$ 是先验概率,$P(\theta|x)$ 是后验概率,调整因子 λ 随着特征向量而变化. 可得到威胁未发生之前,因实际发生的征兆或者事件而更新成功概率. 假设系统所处的网络环境中共有 r 个不同类型的网络威胁,将计算威胁攻击成功概率的贝叶斯公式(11)带入异构度计算式(8)和式(9)可以得到在当前网络环境中执行体贝叶斯异构度公式为:

$$\begin{aligned} H = 1/\sum_{W=1}^{r} \Bigg(& \sum_{j=1}^{m} \Big(r_j \prod_{x=0}^{k-1} P(E_{i+x}) \cdot (\lambda P(\theta_W))^k \cdot \prod_{k=1}^{\frac{(n+1)}{2}} P(U_j|S_k=1) \Big) \\ & - \sum_{i=k+1}^{n} (i-1) (\lambda P(\theta_W))^i \prod_{x=1}^{i} P_{Par_i}(E_x) \Bigg) \end{aligned} \tag{12}$$

从式(12)可以看出,当执行体所处环境中攻击者特征向量中的元素发生时,实际攻击发生的概率也会变化,攻击成功率随着变化,最终执行体异构度将发生变化,从而体现出执行体和环境的相互影响. 动态贝叶斯网络以概率网络为基础,将事件信息与贝叶斯网络结合. 利用这一特性得到的贝叶斯异构度将随着网络环境中的事件信息而变化,其具有的动态性将包含丰富的环境信息. 如果仅分析执行体自身无法得到所有的漏洞信息,特别是未知漏洞. 但将分析漏洞信息转换为使用测试向量的样本数据对执行体进行测试来分析作用过程和

结果,可以得到执行体在不同测试向量条件下的异构度.

2 基于贝叶斯异构度的拟态调度分析

假设执行体存在的漏洞情况如表 1 所示,共有 4 个执行体,若需要调度的执行体数量为 3,那么共有 4 种调度组合,分别为组合 1 即执行体 1,2,3,组合 2 即执行体 1,2,4,组合 3 即执行体 1,3,4,组合 4 即执行体 2,3,4.

2.1 一次攻击仅利用一个漏洞

根据执行体漏洞情况生成贝叶斯网络,最小作用单元包含 3 个执行体,3 个执行体都被攻破时,最小作用单元失去安全性能. 有向边表示执行体被漏洞威胁进行攻击. 当到达 T_1 时,表示执行体被相应类型的威胁攻破,只有调度组合中的 3 个执行体都被攻破时,调度组合才被攻破. 根据节点之间的因果逻辑关系即可生成贝叶斯网络图如图 2 所示. 执行体 1、3 和 4 因为存在漏洞 A_1 即漏洞 1,所以都会被攻破,其路径概率为 1,攻击会到达 3 个执行体,到达路径可以用有向边表示,有向边概率为 1. 执行体 2 不存在漏洞 A_1,条件概率为 0,所以不存在到达路径,攻击不会到达执行体 2.

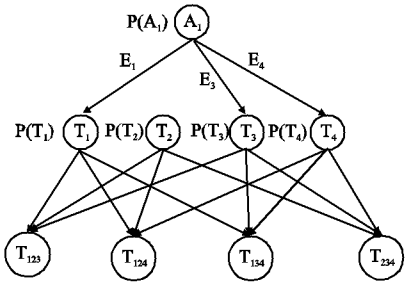

图 2 3 个执行体异构度贝叶斯网络图

Fig. 2 Bayesian network diagram of the heterogeneity of three executors

同理可以得到其他漏洞攻击威胁下相应的节点到达概率. $Par(A)$表示漏洞集合,综合可以得到,当这 10 种漏洞威胁分别进行攻击时,可以得到调度组合中执行体间异构性量化值.

组合 1 的量化值 $P(T_{123}|Par(A)) = P(A_5)$;即攻击者针对漏洞 5 攻击成功概率.

组合 2 的量化值 $P(T_{124}|Par(A)) = 0$;即攻击者针对 10 种漏洞分别进行攻击,均无法攻破.

组合 3 的量化值 $P(T_{134}|Par(A)) = P(A_1)$;即攻击者针对漏洞 1 攻击成功的概率.

组合 4 的量化值 $P(T_{234}|Par(A)) = P(A_9)$;即攻击者针对漏洞 9 攻击成功概率.

由组合中执行体之间的异构性量化值可以看到组合 2 的值最小,其值为 0,即执行体 1,2 和 4 在攻击者漏洞威胁 $Par(A)$的条件下,贝叶斯异构度最大. 这与根据执行体相似性进行计算量化异构度得到的结论相一致,但是可以得到更多的细节. 比如其他组合中执行体之间的异构度与攻击者针对漏洞 1、5 和 9 攻击成功概率有关,当处于针对漏洞 5 的攻击成功的概率比较高的运行环境中时,调度组合 1 异构度比较小,在调度策略中应该被避免选择,最优的无法被调度时,可以优先选择概率低的其他组合. 通过全数一致表决情况下调度组合中执行体之间的异构度可以看到,在选择调度策略时所要考虑的影响因素,以及各个因素对成功概率所产生的影响,仅使用相似度进行分析计算共模漏洞以及高阶异构度无法提供更符合现实情况的调度策略.

2.2 两个漏洞协同攻击

当攻击者针对漏洞 2 和 3 协同攻击时,根据贝叶斯攻击网络图,可以计算得到异构性量化值. $P(T_{124}|A_2,A_3) = P(A_2)P(A_3)$,$P(T_{123}|A_2,A_3) = 0$,$P(T_{134}|A_2,A_3) = 0$,$P(T_{234}|A_2,A_3) = 0$.

由此可知组合 1,2 和 4 在针对漏洞 2 和 3 协同攻击时的作用节点可达概率为 $P(A_2)P(A_3)$,其异构度将随概率而变化,不再是一成不变. 但以执行体相似性进行量化表征异构度可以发现,此异构度仍然为最大. 所以基于此进行的拟态调度防御已经无法适应协同攻击的应用场景. 执行体 1,2 和 4 异构度与针对漏洞 2 和 3 的攻击成功概率有关,如果系统所处的网络环境中攻击者针对漏洞 2 和 3 协同攻击成功概率比较大,而针对漏洞 1、5 和 9 分别独立攻击成功的概率较小,那么虽然执行体 1、2 和 4 在利用相似性进行计算分析时异构度是最大的,但是考虑到环境条件发生改变了,执行体 1、2 和 4 组成的调度组合不能被选为最优调度组合. 因此当遇到针对多个漏洞进行的协同攻击时,使用相似度进行表征的异构度将无法获得最佳的调度类型,而使用贝叶斯网络推算得到的概率进行表征的异构度可以选中最佳的调度类型组合.

2.3 分 析

可以看到利用贝叶斯网络进行量化计算得到的执行体异构度随着执行体所处的环境而变化,将能更准确地反映出 DHR 防御系统实际运行时所应采取的防御策略. 当执行体之间没有共模漏洞时,相似度表征的异构度最大,但是如果协同攻击不同执行体的不同漏洞,那么执行体将会被同时攻破. 贝叶斯异构度与网络威胁发生的概率有关,更准确地表征拟态防御调度过程. 在现实网络环境中,漏洞往往不是线性的,也不是相互之间完全独立的,相较于基于相似度的方法,贝叶斯网络更容易处理复杂的网络攻击环境,可以反映出环境和执行体之间的相互影响,并且更有利于防御针对不同执行体漏洞的协同攻击. 利用贝叶斯网络进行量化计算得到的执行体异构度随着执行体所处的环境而变化,将能更准确地反映出系统实际运行情况.

3 基于贝叶斯异构度的动态调度算法

基于贝叶斯概率思想和异构度量化表征方法,本文设计了一种执行体动态调度算法. 下面对调度算法进行形式化描述,异构执行体池由多个功能等价的异构执行体组成,异构执行体池分为等待池 Ω_W 和运行池 Ω_R,可以表示为 $\Omega = \{T_1, T_2, \cdots, T_n\}$,各执行体间相互独立. 基于贝叶斯异构度的动态调度算法如下所示.

算法 1. 基于贝叶斯异构度的执行体动态调度算法.

输入: 等待池 Ω_W,运行池执行体容量 N_R,贝叶斯异构度矩阵 M,初始默认值为全 0,大小与 Ω_R 相同,初始状态为空.

输出: 运行池 Ω_R

1. 分析系统运行环境和异构执行体漏洞情况,构造测试向量
2. 计算分析测试向量各元素的概率分布 P_m
3. 计算在测试向量作用下各个执行体被攻破的概率
4. for i in N,N 为调度组合的数量
5. 　　生成执行体异构性量化的贝叶斯网络
6. 　　计算得到异构度 H_i
7. end for
8. 选中 H_i 中最大值所对应的编号,获得相应的执行体信息
9. 输出相应的执行体到运行池
10. 跟踪网络环境威胁实际发生情况,更新测试向量及概率分布
11. 更新测试向量,重复 2 ~ 8.

流程如图 3 所示. 算法为一次动态调度的实现,其中的概率分布 P_m 随着威胁信息发生概率以及攻击成功概率的实际情况而改变,从而影响下次调度结果. 与现有仅研究执行体或者仅依据已发现的漏洞进行执行体调度相比,基于贝叶斯异

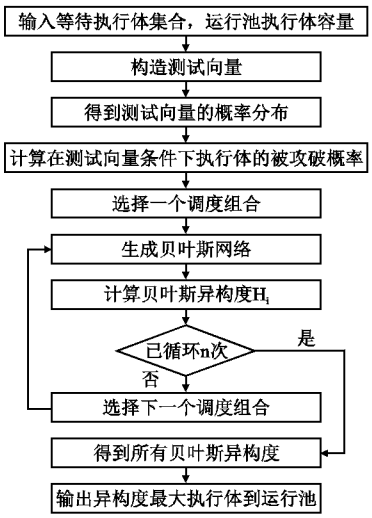

图 3　拟态调度流程

Fig. 3　Mimic scheduling process

构度进行动态调度,可以避免执行体的未知漏洞带来的威胁影响,即使无法提前获得未知漏洞的详细信息,经过训练之后得到的贝叶斯异构度可以在一定程度上反映出执行体所有漏洞的全貌,包含已知漏洞和未知漏洞的所有细节.

4　实验验证

为了验证本文算法的有效性,将其与其他 2 种调度算法(FAWA,Random)进行对比. 其中 FAWA 为基于执行体的常规异构度对执行体进行拟态调度,其焦点在于分析执行体的相似性进行量化表征异构度. 碰撞实验进行仿真验证的核心思想是通过对攻击原子和防御原子的碰撞率来衡量系统的安全性,碰撞率越高系统越安全. 模拟现实情况,即不是所有威胁攻击都能攻破执行体,所以攻击原子载荷即使碰撞到了执行体,也未必百分百能攻破防御执行体,而是具有一定的概率. 构造威胁的方式将不再是随机的,而是对不同的威胁,根据历史经验赋予一定的发生概率. 用系统攻破率表示系统被威胁攻破的概率,系统攻破率越低,代表系统越安全.

实验步骤:

Step 1. 等待池和运行池初始化.

Step 2. 基于一定的概率分布进行构造威胁输入.

Step 3. 利用贝叶斯网络攻击图进行计算,得到最大的贝叶斯异构度,从等待池中选取执行体到运行池.

Step 4. 进行碰撞检测和计数.

Step 5. 返回 Step 2,重复进行多次实验.

Step 6. 计算平均碰撞概率,碰撞率等于产生碰撞的攻击原子策略除以所有攻击原子策略.

Step 7. 改变威胁数目,返回 Step 1.

4.1　碰撞仿真实验

本文对碰撞实验进行了改进,模拟现实情况,对漏洞威胁设置一定的概率分布,近似呈现正态分布的特点. 威胁攻击方式为针对执行体存在漏洞情况采用协同攻击. 实验程序用 Python 语言编写,实验中用系统攻破率表示系统被威胁攻破的概率,系统攻破率越低,代表系统越安全. 构造威胁的方式将不再是随机的,而是对不同的威胁,赋予漏洞威胁一定的概率.

1. 等待池共有 20 个执行体;

2. 执行体调度为 3 模异构执行体集,即每次从等待池中调度 3 个执行体到运行池中;

3. 设置执行体漏洞,威胁攻击集根据概率分布生成或者随机生成;

4. 使用威胁集攻击执行体,得到贝叶斯攻击图;

5. 计算调度组合节点的攻破概率,得到贝叶斯异构度,选取执行体调度组合;

6. 对选取的调度组合实验测试 10000 次,实验结果取平均值.

7. 执行体调度为 5 模异构执行体集,每次从等待池中调度 5 个执行体到运行池;

8. 威胁攻击集根据概率分布生成,进行重复实验;

9. 设置等待池中执行体数量为变量,威胁漏洞数量保持不变;

10. 每次从等待池中调度 3 个执行体到运行池,进行重复实验.

4.2　攻击方按照概率分布进行协同攻击

攻击方的威胁装载机制为大多数威胁原子以高概率出现,少数威胁原子出现概率低. 在该方法下,概率越大,越容易被选中,表示相应的威胁攻击越容易发生. 攻击方协同 2 种威胁原子进行攻击. 得到的实验结果如图 4 所示,系统攻破率为对数坐标系.

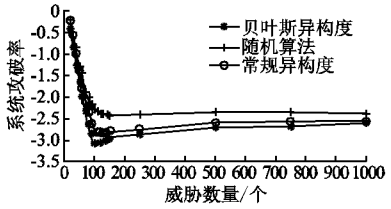

图 4　3 模时按概率分布协同攻击实验结果

Fig. 4　Results of cooperative attack according to the probability distribution at 3 modes

从图 4 中的实验结果可以看到,基于贝叶斯异构度进行调度异构执行体,在面对针对两个漏洞协同攻击时,始终能选

择被攻破概率最低的执行体组合,获得最大的安全增益.通过对比发现在威胁数量较少时,基于贝叶斯异构度的调度选择策略所产生的优势更为明显.

当系统扩展到5模时,改变所要调度执行体数量,每次从等待池中调度5个执行体到运行池中,实验结果如图5所示.

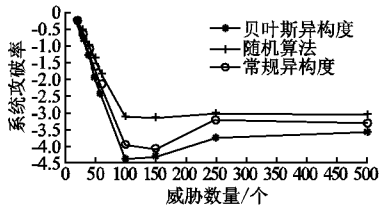

图5 5模时按概率分布协同攻击实验结果

Fig. 5 Results of the cooperative attack according to random at 5 modes

当扩展到调度5个执行体时,基于贝叶斯异构度进行调度系统攻破率低,获得了较高的安全增益.与3模时相比,具有相似的优势.改变等待池中执行体数量,同时保持威胁数量不变,进行仿真实验,实验结果如图6所示.

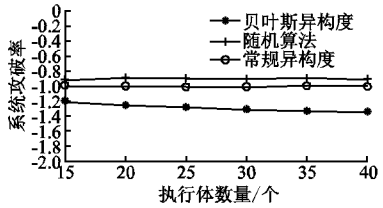

图6 改变等待池数量实验结果

Fig. 6 Results of the experiment when the number of executors changed

当执行体数量逐渐变化时,基于贝叶斯异构度的调度算法仍然具有优势,系统攻破率低于基于现有常规异构度的调度算法.在调度不同数量的执行体时,本文算法均有优势,体现了系统动态变化下的安全性.

4.3 攻击方随机装载

攻击方按照随机的方式发生攻击,测试向量呈现随机分布,其实验结果如图7所示.可以看到在威胁数量较低时,基

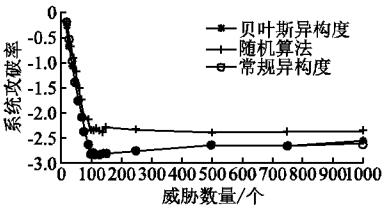

图7 3模时随机装载实验结果

Fig. 7 Experimental results of random at 3 modes

于贝叶斯异构度的调度算法具有一定的优势,随着威胁数量增加,系统攻破率和基于相似度表征异构度的调度算法保持一致.

4.4 实验结论

从仿真实验数据中可以看到,当攻击方的威胁具有一定概率时,基于贝叶斯异构度进行拟态调度所选执行体组合被攻破的概率更低,当攻击方随机装载时,当网络威胁攻击数量较低时,基于贝叶斯异构度所调度的执行体组合保持优势,随着数量的增多,优势将不再存在.实验结果也符合贝叶斯相关理论即利用贝叶斯网络可以推理威胁实际发生的概率以及攻击成功率,进而采取更贴合实际网络环境的防御手段.从概率论的视角,现实网络环境中威胁攻击可以用相应的概率分布进行描述,利用贝叶斯网络工具学习到网络威胁攻击的样本数据,推理模拟网络威胁发生的概率分布模型和攻击模型,然后基于贝叶斯网络量化执行体异构性进行调度将具有更大的安全增益.

5 结束语

针对目前DHR系统对异构度的分析仅限于执行体自身相似性,造成系统安全性不足且缺乏对系统运行环境的适应性问题.本文提出了基于贝叶斯网络的执行体异构性量化概念,给出了计算不同执行体之间异构度的计算公式和方法,以及贝叶斯异构度在拟态调度方面的应用.仿真实验验证了基于贝叶斯异构度进行调度执行体具有良好的防御能力.贝叶斯异构度算法在未知网络环境中面对未知威胁协同攻击时,将具有更大的最优调度选择策略潜力,后续将基于本文所做工作,继续优化贝叶斯理论在DHR系统中的应用方法,进一步提高系统的安全性.

References:

[1] WU J X. Cyberspace's endogenous safety and security problems and the counter measures[J]. Scientia Sinica Informationis, 2022, 52(10): 1929-1937.

[2] WU J X, JI X S, HE L, et al. Development status, trends, and prospects of cybersecurity strategies and methods[J]. Strategic Study of CAE, 2025, 27(1): 14-27.

[3] Sepczuk M. Dynamic web application firewall detection supported by cyber mimic defense approach[J]. Journal of Network and Computer Applications, 2023, 213: 103596, doi: 10.1016/j.jnca.2023.103596.

[4] Tan J L, Jin H, Zhang H Q. A survey: when moving target defense meets game theory[J]. Computer Science Review, 2023, 48: 100544, doi: 10.1016/j.cosrev.2023.100544.

[5] Hu J J, Li Y, Li Z Z, et al. Unveiling the strategic defense mechanisms in dynamic heterogeneous redundancy architecture[J]. IEEE Transactions on Network and Service Management, 2024, 21(4): 4912-4926.

[6] Zheng Y, Li Z, Xu X L, et al. Dynamic defenses in cyber security: techniques, methods and challenges[J]. Digital Communications and Networks, 2022, 8(4): 422-435.

[7] CHEN N N, JIANG Y, HU A Q, et al. An attack feedback dynamic scheduling strategy based on endogenous security[J]. Journal of Information Security Research, 2023, 9(1): 2-12.

[8] YANG L, WANG Y J, ZHANG J. FAWA: a negative feedback dynamic scheduling algorithm for heterogeneous executor[J]. Computer Science, 2021, 48(8): 284-290.

[9] JIA H Y, PAN Y F, LIU W H, et al. Executive dynamic scheduling algorithm based on high-order heterogeneity[J]. Journal on Communication, 2022, 43(3): 233-245.

[10] GAO Y,ZI C C,FENG S F,et al. Security scheduling algorithm for web gateways based on mimicry defense theory[J]. Journal of Chinese Computer Systems,2021,42(9):1913-1919.
[11] ZHANG L W,GUO H P. Introduction to Bayesian networks[M]. Beijing:Science Press,2006.
[12] ZENG K L,ZHANG N,LI W H,et al. Network asset security assessment model based on Bayesian attack graph[J]. Computer Science,2023,50(12):349-358.
[13] WANG M,FU W H,WANG B T,et al. Defense strategy optimization of cyber mimic defense based on evolutionary game theory [J]. Application Research of Copuers,2024,41(2):576-581.
[14] LIU D Q,HU H C,HUO S M. Research on persistent storage – oriented mimic defense technology in container clouds[J]. Computer Engineering,2024,50(2):165-179.
[15] YANG W J,LIU X Y,ZHANG Y,et al. A method for arbitration and scheduling of mimicry industrial controllers[J]. Journal of Information Security Research,2022,8(6):534-544.
[16] Xue S,Li X,Wang X. Fault diagnosis of multi-state gas monitoring network based on fuzzy Bayesian net[J]. Personal and Ubiquitous Computing,2019,23(3-4):573-581.

附中文参考文献:

[1] 邬江兴. 论网络空间内生安全问题及对策[J]. 中国科学:信息科学,2022,52(10):1929-1937.
[2] 邬江兴,季新生,贺　磊,等. 网络安全战略与方法发展现状、趋势及展望[J]. 中国工程科学,2025,27(1):14-27.
[7] 陈楠楠,姜　禹,胡爱群,等. 一种基于内生安全的攻击反馈动态调度策略[J]. 信息安全研究,2023,9(1):2-12.
[8] 杨　林,王永杰,张　俊. FAWA:一种异构执行体的负反馈动态调度算法[J]. 计算机科学,2021,48(8):284-290.
[9] 贾洪勇,潘云飞,刘文贺,等. 基于高阶异构度的执行体动态调度算法[J]. 通信学报,2022,43(3):233-245.
[10] 高　岩,资郴琛,冯四风,等. 面向拟态防御理论构造 Web 网关的安全调度算法[J]. 小型微型计算机系统,2021,42(9):1913-1919.
[11] 张连文,郭海鹏. 贝叶斯网引论[M]. 北京:科学出版社,2006.
[12] 曾昆仑,张　尼,李维皓,等. 基于贝叶斯攻击图的网络资产安全评估模型[J]. 计算机科学,2023,50(12):349-358.
[13] 王　敏,付文昊,王宝通,等. 基于演化博弈的拟态防御策略优化[J]. 计算机应用研究,2024,41(2):576-581.
[14] 刘道清,扈红超,霍树民. 容器云中面向持久化存储的拟态防御技术研究[J]. 计算机工程,2024,50(2):165-179.
[15] 杨汶佼,刘星宇,张　奕,等. 一种针对拟态工业控制器的裁决及调度方法[J]. 信息安全研究,2022,8(6):534-544.