专题：内生安全

有限异构资源条件下的工业控制拟态调度算法

张汝云，李合元，李顺斌
（之江实验室，浙江 杭州 311121）

摘　要：网络空间拟态防御技术是应对信息系统未知漏洞后门攻击的有效手段，其安全性与执行体的数量、异构化程度以及具体的裁决调度策略紧密相关。然而在工业控制领域，工业应用的生态资源相对封闭，可实现的异构执行体个数受限。针对上述问题，提出一种适用于有限异构资源约束条件下的工业控制拟态调度算法。算法通过引入执行体上线保护寄存器、周期清洗定时器等，能够根据运行环境自适应选择合适的执行体上线，可有效防范 *N*−1 模与 *N* 模攻击。实验结果表明，所提出的三余度工业控制拟态调度算法，可自适应根据环境特性选择合适的执行体上线，即使在高强度攻击环境下，依然能保持 99.24%的高可用概率。

关键词：拟态防御；内生安全；资源受控模型
中图分类号：TP393
文献标识码：A
doi: 10.11959/j.issn.1000−0801.2021047

Mimic security scheduling algorithm for industrial control under limited heterogeneous resource constraints

ZHANG Ruyun, LI Heyuan, LI Shunbin
Zhejiang Lab, Hangzhou 311121, China

Abstract: Cyberspace mimic defense technology is an effective method to deal with backdoor attacks on unknown vulnerabilities in information systems. Its security is closely related to the number and the heterogeneity of the executors and the scheduling strategy. However, in the field of industrial control, the ecological resources of industrial application are relatively closed, and the number of realizable heterogeneous executors is limited. To solve the above problems, a mimic scheduling algorithm for industrial control under the constraints of limited heterogeneous resources was proposed. The experimental results show that the proposed algorithm for triple-redundancy mimic industrial control system was able to select a suitable executor to go online according to environmental characteristics adaptively. Even in a high-intensity attack environment, it can still maintain a high availability probability of 99.24%.

Key words: mimic defense, endogenous safety and security, resource-constrained model

---

收稿日期：2021−02−13；**修回日期**：2021−03−12
通信作者：李顺斌，lishunbin@zhejianglab.com
基金项目：国家重点研发计划项目（No.2020YFB1804800）；之江实验室开放课题（No.2018FD0ZX01）
Foundation Items: The National Key R&D Program of China (No.2020YFB1804800), Opening Foundation of Zhejiang Lab (No.2018FD0ZX01)

1 引言

当前网络空间安全存在 4 个本源性问题：一是受软/硬件构件设计水平的局限，信息系统设计缺陷的漏洞难以避免；二是在“你中有我，我中有你”的开放生态环境中，信息系统软硬件后门的可能性长期存在；三是依托现阶段的科学技术尚无法彻查所有漏洞后门；四是产品和系统的信息安全质量难以得到有效控制。

为了能在“有毒带菌”的环境下构筑网络安全，邬江兴院士基于共识机制提出了拟态防御理论[1]，通过在“动态－异构－冗余”的 DHR（dynamic heterogeneous redundancy）架构上引入多模裁决机制，对攻击者形成测不准防御迷雾，有效地将网络空间的不确定威胁问题归一化为利用鲁棒控制理论能解决的工程技术问题。Ma 等[2]基于马尔可夫模型建立了可描述分析 DHR 架构核心特征的模型，通过蒙特卡罗仿真验证了冗余度、可用异构资源与拟态防御系统安全防御能力之间的关系。在系统冗余度越高、执行体异构度越大，系统防御性能则越强的普遍共识下，针对拟态防御理论的多模裁决机制和拟态调度策略研究，则是进一步增强系统防御效果，提升最大化资源利用效率的关键。为此，学术界展开了大量的研究。

马海龙等[3]在基于动态异构冗余机制的路由器拟态防御体系结构中提出了基于执行体可信度的随机调度策略和基于执行体性能权重的随机调度策略，该策略将可信度、性能权重应用于执行体上线阶段，以达到可信度高、性能好的执行体优先上线的效果；吴春明等[4]也提出了基于信誉度与相异度相结合的自适应拟态控制器，利用相异度指标衡量各执行体之间的差异，从而得到异构程度最高的执行体；利用信誉度指标衡量执行体的脆弱程度，从而决定执行体在多模裁决中的作用程度；然而，上述算法的决定执行体上线的参考因素相对固定且缺少对运行环境的自适应迭代更新机制，策略可能存在选出的执行体缺乏随机性的缺陷。陈利跃等[5]提出了基于 *K*-means 聚类算法的执行体调度策略，一定程度平衡了执行体上线的针对性与随机性问题，但其算法需要用到特征分解等复杂操作，在工业控制场景的嵌入式设备中较难推广。

伴随理论研究的不断深入，拟态防御技术已经广泛用于路由器、防火墙、数据中心、域名服务器等关键网元设备，赋予设备内生安全的功能。安全设计者的目光焦点从理论研究逐步转移到实际场景中的设备拟态化改造上，更加关注工程可实现性、投入费效比的衡量上。魏帅等[6]认为，在单处理机故障率小于 1%的情况下，四余度拟态处理机与三余度拟态处理机相比整体的错误故障率降低幅度并不明显，三余度拟态处理机明显具有更高的费效比。

此外，在工业控制领域，工业应用的生态资源相对封闭，许多应用场景可能无法在较低的成本、较短的时间内生成多个异构化程度较大的执行体集合。在许多场合，可用的异构资源数量可能只有 6 个，远小于参考文献[2]中假定的最小可用异构资源数量 20。在异构执行体资源受限的条件下，如何设计适用于工业控制系统的拟态裁决算法并进行可量化安全性评估，是值得研究的一个问题。

本文针对当前应用最为广泛的三余度的DHR架构，提出了一种基于置信度和胜任系数的工业控制系统拟态调度方法，将执行体的当前状态与历史表现状态转化为可量化的指标来实施拟态调度。本文的主要贡献有以下 3 点。

（1）本文所提出的拟态调度策略，能够根据运行环境自适应选择合适的执行体上线。在低强度攻击时，每个执行体上线的概率趋于平均，保持了随机性；在高强度攻击时，优先选中可靠性更强（漏洞分布更少）的执行体上线，以提升系

统可用概率。

（2）本文所提出的拟态调度策略，对三余度拟态系统可能存在的所有异常状态做了针对性分类，引入了执行体上线保护寄存器、周期清洗定时器等专用结构分别应对 N−1 模与 N 模攻击。实验结果表明，系统只需要执行 2 次清洗操作即可杜绝 N−1 模攻击逃逸行为，只需要执行 3 次清洗即可杜绝 N 模攻击逃逸行为。

（3）针对应用生态受限的客观条件，本文建立基于攻击强度的仿真模型，验证了在异构执行体数量只有 6 个的极端约束条件下，拟态防御系统在对抗高强度攻击时仍能保持 99.24%的高可用概率。给拟态系统设计的成本规划提供了新思路。

2　资源受限条件下的安全调度模型

2.1　拟态防御理论

根据拟态防御理论：拟态防御系统包含由多个独立的异构执行体；执行体根据时间（或环境）动态切换成上线或清洗备用状态；系统的输入通过输入代理模块分发至在运行的多个执行体中并获得多个输出结果；多模裁决模块通过对比执行体的输出结果，判定各执行体的安全状态，动态调控执行体的状态。由于系统架构采用严格的单向联系机制，攻击者无法直接触碰到由输入代理与输出裁决模块组成的拟态括号。实现攻击逃逸的唯一方式，即对拟态括号内由多个异构执行体实现非配合下的盲协同攻击。可见，基于拟态防御系统的安全性很大程度上依赖于执行体相互间的异构化程度。倘若执行体完全异构，则采用简单的择多判决即可保证系统安全可信。

然而受当前应用生态发展现状的约束，异构执行体之间存在共模漏洞是不可避免的事实。因此，拟态防御理论并不强调绝对的静态安全，而是通过引入多模裁决策略对受到攻击的执行体进行动态清洗切换。即使攻击者耗费巨大精力在非配合条件下成功构造出盲协同攻击，也会被系统识别并清洗。指数量级地提升攻击难度并且使得攻击效果不可持续，是拟态防御的两大显著效果。

2.2　安全调度控制模型与假设

区别于拟态防御理论中的一般化描述，本文对工业控制系统的安全调度模型做出如下理论假设。

（1）假设拟态工业控制系统采用费效比最高的三余度 DHR 架构。因为同时在线运行的执行体数量必须大于或等于 3 个，才能对输出结果的进行裁决。

（2）拟态工业控制系统的可用异构执行体的数量最小值设置为 6。6 个执行体是三余度 DHR 架构系统在遭受 N 模攻击后通过裁决清洗操作可恢复到正常状态并实现攻击面转移的最低条件[1]。

（3）每个执行体均存在漏洞，且漏洞分为两大类。第一类漏洞后门依赖于该执行体所独有运行环境，称之为“差模漏洞”，触发该漏洞仅会造成差模攻击效果，触发概率值用 P_{diff} 表示；第二类漏洞后门与执行体所独有运行环境无关，称之为“共模漏洞”，多执行体同时触发该漏洞将造成 N−1 模或 N 模攻击效果，执行体单体触发概率值用 P_{comm} 表示。

（4）在系统执行体启动前为每个执行体分配一个胜任系数值 T_c，$T_c \in (0,1)$。该执行体胜任系数，由用户结合执行体应用生态情况以及执行体相互间异构化程度综合评定。

- 执行体应用生态越好，对安全防护考虑越多，漏洞越少，则胜任系数值越高。
- 执行体与其他异构执行体的差异度越大，则胜任系数值越高；执行体的差异度可借助相似性度量工具评估[7]；拟态调度算法偏向于选择异构化程度大的执行体上线，以达到提升抗盲协同攻击难度的效果。

- 执行体胜任系数 T_c 是一个时变参数，根据执行体在实际工作环境中的表现自适应动态更新。

（5）假设系统内所有执行体均能通过下线清洗的方法消除漏洞或使漏洞不再处于被激活状态。所有漏洞后门都需要经过触发加载恶意指令才能生效。执行体下线后，其存储数据被重置，因而该假设充分且合理。

（6）由于不同执行体输出结果不同步的超时问题已经被参考文献[8]提出的基于回归样条的自适应超时机制解决，故本文仅就执行体输出结果的异同展开讨论，假定异构执行体对相同输入会在给定时间段内“同时”输出各自的结果。

3 基于置信度与胜任系数的拟态调度器

由于系统构造复杂、执行体不完全异构、攻击行为不可预测，有限资源条件下的拟态工业控制系统遭受 N−1 模以及 N 模攻击时必然存在一定的逃逸概率，可能需要多次清洗才能彻底消除攻击带来的影响。因此如何在有限异构资源约束条件下，有效地降低异构冗余构造的逃逸概率和逃逸时间是本文的主要目标。

本节提出一种基于置信度与胜任系数的拟态调度算法，其中置信度 V 是执行体在运行环境中的综合表现评价（包括历史表现行为与当前风险抵御能力），用于判别该执行体是否需要进行清洗；胜任系数 T_c 是执行体原始属性（包括执行体应用生态、清洗成本、执行体间异构化程度等）与历史表现行为的综合评价，用作表征该执行体上线运行的胜任能力。有限异构资源约束条件下的拟态调度器如图 1 所示，包含采集器、比较器、裁决器、清洗器（含周期清洗定时器 C）等。

基于置信度和胜任系数的工业控制系统拟态调度算法如图 2 所示，具体工作流程描述如下。

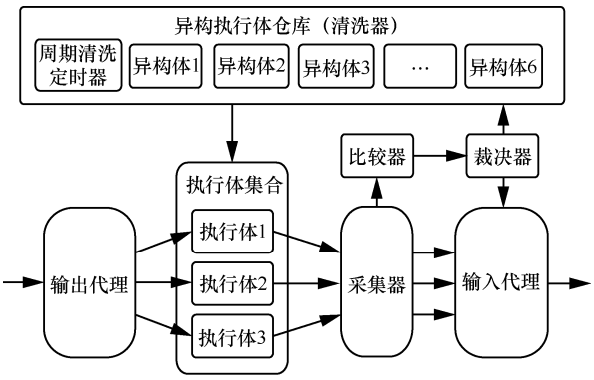


图 1 有限异构资源约束条件下的工业控制系统拟态调度器

（1）系统启动复位。从执行体仓库中选择 3 个胜任系数最高的执行体上线，并将所有刚上线执行体的初始置信度均为最大值 $V_{\max}$。周期清洗定时器 C 复位为零。

（2）执行体输出结果采集。执行体采集器采集 3 个在线执行体的输出结果分别为 $R1$、$R2$、$R3$。

（3）执行体裁决。3 个执行体输出结果两两比较（共 3 次）：

- 当执行体输出结果一致时，两个执行体的置信度都增加 D。
- 当输出结果不一致时，两个执行体的置信度都减少 D。
- 比较结束后，若单个执行的置信度大于 $V_{\max}$，则令其等于 $V_{\max}$。

（4）执行体清洗。选择判断需要下线的执行体并选择置信度最高的执行体作为系统的输出。

- 遍历所有在线执行体当前的置信度 V，选择置信度小于或等于 0 的执行体作为备选清洗对象。
- 如果有多个执行体置信度≤0，选择则置信度最小的执行体作为清洗对象。
- 如果有多个执行体置信度相等且≤0，选择胜任系数较小的作为清洗对象。
- 如果有多个执行体置信度相等且≤0，胜任系数亦相同，随机选择其一作为清洗对象。
- 检查执行体上线保护寄存器 C_{reg}（保护刚上线执行体，对抗 N−1 模攻击）。清洗对象与

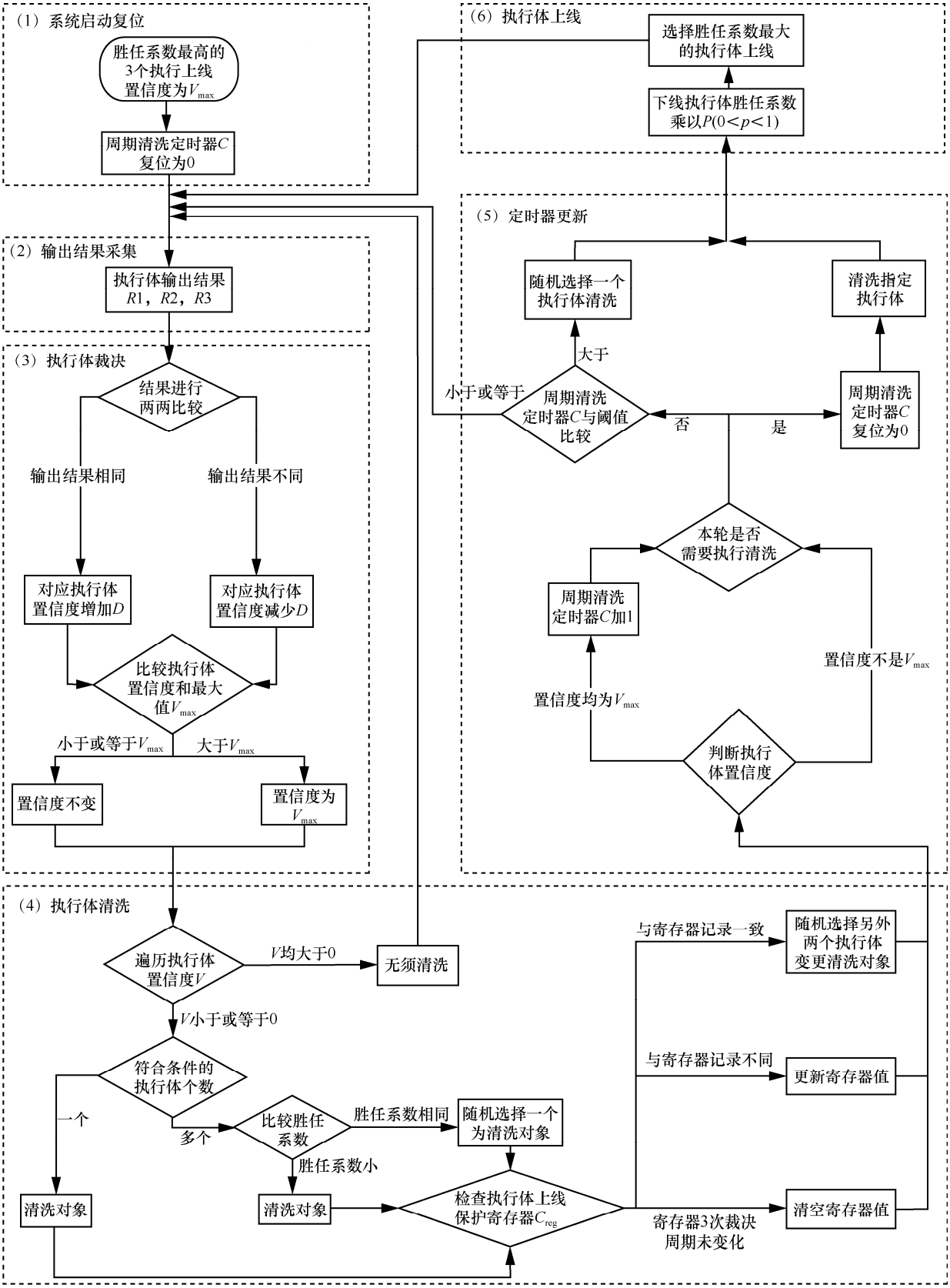


图 2　基于置信度和胜任系数的工业控制系统拟态调度算法

上线保护寄存器 C_{reg} 记录一致，随机清洗选择另外两个执行体中的一个；清洗对象与上线保护寄存器 C_{reg} 记录不一致，更新执行体上线保护寄存器的值；若执行体上线保护寄存器经过 3 次裁决周期未发生变化，清空该寄存器的值。

（5）定时器更新（引入扰动，对抗基于 0-day 漏洞的共模攻击）。

- 如果所有执行体的置信度均为 V_{max}，周期清洗定时器加 1。
- 如果执行体发生过清洗行为，周期清洗定时器 C 复位为零。
- 当周期清洗定时器 C 的值大于指定阈值，随机选择其中一个执行体进行清洗。

（6）执行体上线。选择仓库内胜任系数最高的执行体上线运行，同时将下线清洗的执行体胜任系数乘以系数 $P(0<P<1)$。

4 安全性仿真评估与分析

4.1 随机性故障模型表征

要对拟态防御系统的安全性进行有效评估，必须准确刻画系统裁决切换的流程。其中，异构执行体的随机性故障模型表征是核心。在缺乏攻击者先验信息的前提条件下（这也是拟态防御理论所直面的问题），拟态防御系统中执行体发生故障的时间点呈现随机性，执行体两两之间发生故障的表现形式的差异也呈现随机性。本文首先需要为执行体建立随机性故障模型，然后采用数值仿真的方法，对所提出的基于置信度与胜任系数的拟态调度算法安全性能进行分析。随机性故障模型建立如下。

（1）模型采用 P_{diff} 表征执行体运行过程中差模漏洞的触发概率。

（2）模型采用 P_{comm} 表征执行体运行过程中共模漏洞的触发概率。

（3）模型采用“0/1/2”3 个值，分别表征单个执行体处于正常/差模漏洞生效/共模漏洞生效 3 种状态。仿真过程中的每次迭代，若执行体状态值为“0”，则概率进入状态“1”或者“2”；若执行体状态值已经为“1”或者“2”，则保持原值，直至被清洗。

拟态工业控制系统的安全状态与编码见表 1。

4.2 实验设置

本文的实验仿真平台为 MATLAB 2017b。根据参考文献[9]基于美国国家脆弱性数据库（national vulnerability database, NVD）对 11 种操作系统的漏洞分析，来自于相同家族操作系统（如 Windows 2003 与 Windows 2008）之间的共模漏洞数量会比较多，而来自于不同家族操作系统（如 BSD-Windows）之间的共模漏洞数量很少，对于一般攻击而言，其异常输出矢量一致的比例可以设置为一个合理的较小值 10^{-4}，在具体产品开发时，采用与开发飞行控制系统类似的工程管理方法，能够保证该参数的实际取值远远小于 10^{-4}[10]。根据第 2 节所述的有限异构资源条件，为 6 个执行体的脆弱性仿真模型赋予高/中/低 3 档的仿真参数，见表 2。

表 1 拟态工业控制系统的安全状态与编码

情况	表现形式	安全状态	期望的预期操作
1	“0-0-0”	正常	定时器加 1，若定时器超出阈值则随机清洗
2	“1-0-0”“2-0-0”等	差模攻击，可定位故障执行体	清洗输出结果不一致的执行体，恢复到正常状态
3	“1-1-0”“1-1-1”“1-1-2”“0-1-2”等	差模攻击，未能定位故障执行体	清洗输出置信度低于 0 的执行体，逐次清洗其他受攻击的执行体
4	“0-2-2”“1-2-2”	$N-1$ 模攻击	清洗输出结果不一致的执行体，进入“清洗后仍未恢复状态”；然后清洗输出结果一致的其中一个执行体，退化到差模攻击状态
5	“2-2-2”	共模攻击	定时器加 1，若定时器超出阈值则随机清洗

表 2　执行体脆弱性仿真模型（高/中/低强度攻击）

对象	差模漏洞触发概率 P_{diff}	共模漏洞触发概率 P_{comm}	执行体初始胜任系数
执行体 1	0.001/0.002/0.004	$1\times10^{-5}/2\times10^{-5}/1\times10^{-4}$	0.9
执行体 2	0.001/0.002/0.004	$5\times10^{-5}/1\times10^{-4}/5\times10^{-4}$	0.85
执行体 3	0.002/0.004/0.008	$5\times10^{-5}/1\times10^{-4}/5\times10^{-4}$	0.8
执行体 4	0.002/0.004/0.008	$1\times10^{-4}/2\times10^{-4}/1\times10^{-3}$	0.75
执行体 5	0.004/0.008/0.016	$1\times10^{-4}/2\times10^{-4}/1\times10^{-3}$	0.7
执行体 6	0.004/0.008/0.016	$5\times10^{-3}/1\times10^{-2}/5\times10^{-2}$	0.95

注：该实验参数值仅为评估所提出有限异构资源条件下拟态调度策略安全程度的一组具体系数，读者可以根据实际情况对漏洞概率值进行调整。

在不同的攻击强度下，设置初始置信度 4，检测到异常时置信度扣分差值 D 设置为 1。随机模拟仿真 1 000 次，每次模拟仿真包含 100 000 次迭代。统计不同仿真参数条件下，拟态调度器干预下的运行结果。

4.3　实验结果分析

（1）最多只需要 3 次清洗，即可将系统恢复到正常状态

高强度攻击下的系统安全状态转移如图 3 所示。在第 5 到第 6 个时钟周期间，执行体 2 被触发了 1 次漏洞。系统经过积分累计在 2 个时钟周期内将其置信度降低到 0 并清洗，系统输出正常，攻击无感移除；在第 56 个时钟周期，执行体 2 与执行体 3 同时被触发了共模漏洞，系统进入 N−1 模攻击状态。系统首先判定执行体 1 出现问题，经 56、57 两个时钟周期进行积分累计将执行体 1 清洗下线并更换另一个执行体；58、59 两个时钟周期积分累计发现清洗后状态仍未恢复，做出执行体 3 下线的决策，使得系统在第 60 个时钟周期退化到差模攻击状态。在时钟周期 80~110 则呈现了受定时机制保护下的 N 模攻击恢复状态转移。由于引入了执行体上线保护寄存器 C_{reg}，即使遭受 N 模攻击，系统仅需要 3 次清洗操作即可恢复正常。

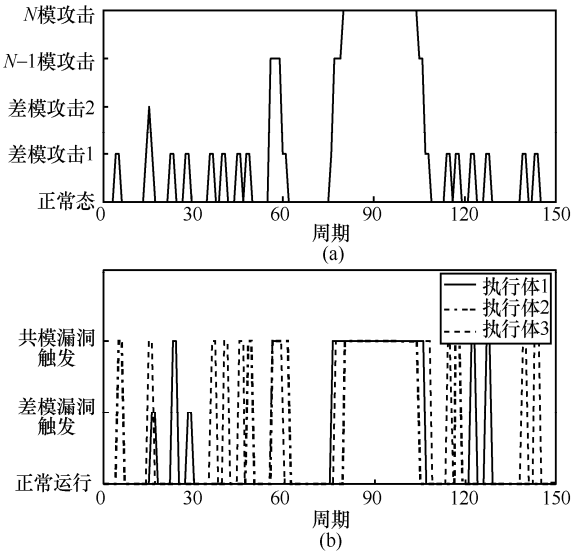


图 3　高强度攻击下的系统安全状态转移

（2）具备环境自适应特性的执行体上线替换机制

不同攻击强度下执行体上线概率情况见表 3。本文假设可用的执行体只有 6 个，且不同执行体在抗攻击性能上具有差异。在高攻击强度下，系统更倾向于根据执行体的实际表现情况选择对系统环境适应性更强（表现为漏洞分布更少、更难被触发）的执行体上线。如表 3 所示，在高强度攻击模型下，执行体 1 上线的概率要比执行体 6 高 69.71%。在低强度攻击仿真条件下，由于各执行体表现差异不大，所以上线概率呈现平均分布

表 3　不同部攻击强度下执行体上线概率

攻击强度	执行体 1	执行体 2	执行体 3	执行体 4	执行体 5	执行体 6
高强度攻击	77.91%	76.52%	55.51%	52.72%	29.11%	8.20%
中强度攻击	74.71%	73.62%	55.74%	52.78%	28.35%	14.77%
低强度攻击	72.99%	71.07%	56.68%	52.87%	29.05%	17.31%

的现象。值得注意的是，执行体的初始胜任系数凭人工经验设置，可以让执行体在系统的初始阶段获得更高的上线优先级，但该值会在系统调度的迭代过程中不断更新。尽管在实验参数中将执行体 6 的初始胜任系数设置为 0.95，但在高强度攻击模型下，该执行体的上线概率依然与执行体实际漏洞后门的分布情况紧密相关。综上分析表明，所提出的基于置信度与胜任系数的拟态调度方法，其执行体上线替换机制具备环境的自适应特性。

（3）在高强度攻击下，系统仍可保持 99.24% 的高可用概率

不同攻击强度下系统的平均清洗概率与平均可用概率见表 4。其中，平均清洗概率由执行体清洗下线次数除以总迭代次数得出；平均可用概率为系统处于正常状态（case1）与可定位故障执行体的差模攻击状态（case2），两种状态在系统运行过程中所有状态的比重。可见在高强度攻击下，尽管系统只有有限的 6 个可用执行体，系统平均可用概率依然可以达到 99.24%；而在低强度攻击下，系统可用概率高达 99.87%。实验数据表明，所提出的基于置信度与胜任系数的拟态调度方法，能为有限异构资源条件下的拟态系统构造提供高效的解决方案。

表 4　不同攻击强度下系统的平均清洗概率与平均可用概率

攻击强度	平均清洗概率	平均可用概率
高强度攻击	1.52%	99.24%
中强度攻击	0.64%	99.77%
低强度攻击	0.31%	99.87%

5　结束语

针对当前工业控制应用生态局限性的约束条件，本文提出了有限异构资源条件下的拟态调度算法，并且基于数值仿真的方案建立了安全评估仿真模型。实验结果表明，所提出的工业控制系统拟态调度算法，最多只需要 3 次清洗，即可将拟态系统从 $N-1$ 模攻击状态、N 模攻击状态恢复到正常状态；执行体上线替换机制具备环境的自适应特性；即使在高强度攻击下，系统仍可保持 99.24%的高可用概率。

拟态防御是基于内生性安全机制的一种创新网络防御，其安全效果可量化设计，可验证度量。本文从适应应用、节约成本、简化拟态调度策略的角度出发，评估了当前应用最广泛的三余度 DHR 架构在有限异构资源条件下系统可用概率，给拟态系统设计的成本规划提供了新思路。

参考文献：

[1] HU H, WU J, WANG Z, et al. Mimic defense: a designed-in cybersecurity defense framework[J]. IET Information Security, 2017, 12(3): 226-237.

[2] MA B L, ZHANG Z. Security research of redundancy in mimic defense system[C]//Proceedings of 3rd IEEE International Conference on Computer and Communications (ICCC). Piscataway: IEEE Press, 2017: 2910-2914.

[3] 马海龙, 伊鹏, 江逸茗, 等. 基于动态异构冗余机制的路由器拟态防御体系结构[J]. 信息安全学报，2017, 2(1): 29-42.
MA H L, YI P, JIANG Y M, et al. Dynamic heterogeneous redundancy based router architecture with Mimic defenses[J]. 2017, 2(1): 29.

[4] 沈丛麒, 陈双喜, 吴春明. 基于信誉度与相异度的自适应拟态控制器研究[J]. 通信学报, 2018, 39(Z2): 173-180.
SHEN C Q, CHEN S X, WU C M. Adaptive mimic defensive

controller framework based on reputation and dissimilarity[J]. Journal on Communications, 2018, 39(Z2): 173-180.

[5] 陈利跃, 孙歆, 吴春明, 等. 一种基于异构度的拟态执行体调度模型研究[C]//第一届“先进计算与防御技术”会议. 北京: 人民邮电出版社, 2018: 494-500.
CHEN L Y, SUN X, WU C M, et al. A heterogeneous-based mimic execution scheduling model[C]//Proceedings of the first national conference on advanced computing and defense. Beijing: People’s Posts and Telecom Press, 2018: 494-500

[6] 魏帅, 于洪, 顾泽宇, 等. 面向工控领域的拟态安全处理机架构[J]. 信息安全学报, 2017, 2(1): 54-73.
WEI S, YU H, GU Z Y, et al. Architecture of mimic security processor for industry control system[J]. Journal of Cyber Security, 2017, 2(1): 54-73.

[7] 赵长海, 晏海华, 金茂忠. 基于编译优化和反汇编的程序相似性检测方法[J]. 北京航空航天大学学报, 2008(6): 711-715.
ZHAO C H, YAN H H, JIN M Z. Approach based on compiling optimization and disassembling to detect program similarity[J]. Journal of Beijing University of Aeronautics and Astronautics, 2008(6): 711-715.

[8] LIN S, LIU Q, WU Y, et al. A self-adaptive timeout mechanism in Mimic Defense System[C]//Proceedings of 2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS). Piscataway: IEEE Press, 2017: 588-591.

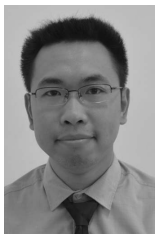
[9] GARCIA M, BESSANI A, GASHI I, et al. Analysis of OS diversity for intrusion tolerance[J]. Software: Practice and Experience (accepted for publication), 2013.

[10] 邬江兴. 网络空间内生安全——拟态防御与广义鲁棒控制[M]. 北京: 科学出版社, 2020.
WU J X. Cyberspace endogenous security: Mimic defense and generalized robust control[M]. Beijing: Science Press, 2020.

[作者简介]

张汝云（1973− ），男，博士，之江实验室工业互联网研究中心研究员，主要研究方向为工业互联网内生安全、新型网络架构、工业网络计算等。

李合元（1986− ），男，之江实验室工业互联网研究中心工程师，主要研究方向为工业互联网内生安全、时间敏感网络等。



李顺斌（1990− ），男，博士，之江实验室工业互联网研究中心助理研究员，主要研究方向为异构计算、可重构计算与工业互联网内生安全等。