基于信誉度与相异度的自适应拟态控制器研究

沈丛麒*[1]，陈双喜[2]，阮伟[3]，吴春明[4]

之江实验室[1]，杭州市 311100

浙江大学工程师学院[2]，杭州市 310027

浙江大学控制学院[3]，杭州市 310027

浙江大学计算机科学与技术学院[4]，杭州市 310027

shencq@zhejianglab.com, abelchen@zju.edu.cn, ruanwei@zju.edu.cn, wuchunming@zju.edu.cn

摘　要：控制层作为各类网络模型的主要层次，对网络安全性及其防御成本有较大影响。现有的拟态控制器防御成本过高，因此，本文研究能够抵抗未知攻击同时防御成本相对较低的拟态控制器。首先，引入信誉度指标表征拟态控制器中各执行体的脆弱程度，定义相异度指标表征各执行体之间的异构程度。执行体选择模块基于相异度与信誉度选择脆弱程度最低且异构程度最大的执行体集。另外，利用信誉度指标优化现有的多模裁决。最后，通过引入负反馈模块动态更新各执行体信誉度，实现执行体集选择策略与多模裁决策略的动态更新。本文所设计的自适应拟态控制器在上述三个模块进行创新。仿真结果表明，该自适应拟态控制器具有良好的抗攻击能力。

关键词：拟态控制器；信誉度；多模裁决；动态异构冗余

An Adaptive Mimic Defensive Controller framework based on Reputation and Dissimilarity

SHEN Congqi*[1], CHEN Shuangxi[2], RUAN Wei[3], WU Chunming[4]

Zhejiang Lab, Hangzhou 311100, China[1]

Polytechnic Institute of Zhejiang University, Hangzhou, 310027, China[2]

College of Control Science and Engineering, Zhejiang University, Hangzhou, 310027, China[3]

College of Computer Science, Zhejiang University, Hangzhou, 310027, China[4]

shencq@zhejianglab.com, wuchunming@zju.edu.cn, ruanwei@zju.edu.cn, abelchen@zju.edu.cn

Abstract: As a key layer of the Internet model, controller has a significant impact on the cyberspace security and its defense cost. Since the defense cost of current mimic controller is relatively high, we research a novel mimic controller with defense cost relatively low and good defensive performance. First, we introduce reputation indicator to describe the vulnerability of performers and a dissimilarity dictator to describe the heterogeneity of the performers.

The performer selection module uses the dissimilarity and reputation to obtain an optimized performer set featuring most reliable and heterogeneous. Second, the ruling module reduce the negative effect of unreliable performers on the ruling result by using the reputation of performers. Besides, by interacting with the performer selection module and the multi-strategic ruling module, the negative feedback controller updates the reputation of performers according to the ruling result and determines the attacked heterogeneous objects need to be cleaned. Simulation results show that the proposed adaptive mimic controller has good robust against malicious attacks.

Key words: mimic controller; reputation; ruling module; dynamic heterogeneous redundancy

1 引言

当前网络空间易攻难守，面临严峻的安全挑战。由于互联网架构日趋开放，无法保证互联网始终是无菌无毒的环境。另外，随着美国退出网络中立原则，我国互联网被攻击的风险将日益加剧。以工业互联网为例，我国工业互联网关键基础设施大量采用了进口设备，软硬件中很可能留有恶意代码。未知漏洞问题、软硬件后门问题以及侧信道攻击层出不穷，工业互联网有菌带毒的现状短期内难以根除。未知威胁是网络安全易攻难守不平衡态势难以逆转的核心因素之一。因此，亟需主动防御体系解决网络空间安全问题[1]。

现有的防御体系是基于威胁特征感知的精确防御，即以攻击来源、攻击途径、攻击行为为先验知识获得攻击特征，从而实施有效的防御手段。因此，这种防御手段能针对已知类型的攻击，不能防御未知攻击，且体系架构透明、处理空间单一，缺乏多样性。

受自然界生物拟态伪装增加存活几率现象的启发，邬江兴院士提出了拟态防御[2]。其中一种重要的机制是动态异构冗余构造(Dynamic Heterogeneous Redundancy, DHR)。DHR 引入动态性、随机性、多样性，使运行环境异构化，增加攻击难度，有效应对未知攻击。冗余构件的动态性和随机性能够提升多方参与、具有一致性或协同性要求的行动的不确定度，多模判决环节又在机理上提升了非配合条件下的协同攻击难度。动态异构冗余构造，理论上要求系统具有结构表征的不确定性，包括非周期地从功能等价的异构冗余体池中随机的抽取若干个元素组成当前执行集，或者重构异构冗余体自身，或者借助虚拟化技术改变冗余执行体内在的资源配置方式以及运行环境，或者对异构冗余体作预防性或修复性的清洗、初始化等操作，使攻击者在时空维度上很难有效的再现成功攻击的场景。

无论网络模型或工业模型，控制层是其中较为关键的层次。提高控制层中控制器的防御能力能有效提升系统安全性。因此，本文将研究重点放在基于拟态理论的控制器上，研究能防御未知攻击且防御成本较低的拟态控制器。

近年来，针对拟态控制器的研究，取得了一定的研究成果。文献[2]简要定义了 DHR 架构以及拟态防御的基本理念。文献[3]利用 petri 网对电网故障点进行推理分析。类似的工作还有文献[4,5]。文献[6]利用

马尔可夫链分析不同控制系统的抗攻击性能。文献[7]结合拜占庭容错协议介绍了一种安全的软件定义网络(Softeware Defined Network, SDN)控制层架构。文献[8]结合 paxos 协议研究多控制器达到一致的方法。文献[9,10]从测试评估的角度，介绍了拟态防御的测试方法。文献[11]以 SDN 为应用环境，根据网络流量及计算能力实现交换机的动态选择，但选调机制本身没有考虑执行体的异构化问题，即所选择的异构体可能存在随机性，没有完全做到运行环境的最大异构化。文献[12]仍以 SDN 为背景，定义控制器的异构视图，得到最大异构度的候选控制器集合，但没有考虑控制器的抗攻击性。综上，在已有研究工作中，选择模块和表决器是孤立的两个模块，无法获知执行体集的运行状态，也无法动态调整裁决策略或选择策略，且研究成果大多集中于 SDN，尚无普适性的研究结果。

因此，本文引入相异度与信誉度，设计一种自适应的拟态控制器。本文工作的贡献可概括为 3 个层次：首先，定义信誉度指标表征执行体的脆弱程度，并定义相异度表征各执行体之间的异构程度。基于前述指标，提出了一种基于信誉度与相异度联合优化的执行体选择算法，使得执行体集脆弱程度最低且异构程度最高。其次，引入负反馈模块与执行体选择模块、多模裁决模块进行交互，实现选择策略与裁决策略基于信誉度的自适应调整。第三，改进了多模裁决算法，降低脆弱的执行体对多模裁决结果的影响，提高拟态控制器对未知攻击的防御能力。

本文的余下部分安排如下：第二部分介绍本文的系统模型。第三部分通过引入信誉度与相异度，介绍所提出的自适应的拟态控制器，包括基于信誉度与相异度的执行体选择算法、多模裁决算法、负反馈模块工作机理。第四部分给出仿真结果，分析所提出的拟态控制器的性能。第五部分总结全文。

2 自适应的拟态控制器系统模型

通用的拟态控制器抽象模型如图 1 所示。用集合 $\mathcal{I}$ 表示异构体集合中各异构体构成的集合，$\mathcal{I}=\{E_1,E_2,...,E_N\}$，$|\mathcal{I}|=N$。用集合 $\mathcal{S}(t)$ 表示 t 时刻执行体选择模块选择得到的执行体集合，$\mathcal{S}(t)=\{E_1,E_2,...,E_M\}$，$|\mathcal{S}(t)|=M$。$M$ 个执行体进行多模裁决得到最终的输出结果。异构体集合中可能存在受恶意攻击的异构体。由于异构体之间只有功能相同，结构完全不同，因此，可以假设各异构体被攻击的概率完全互相独立。

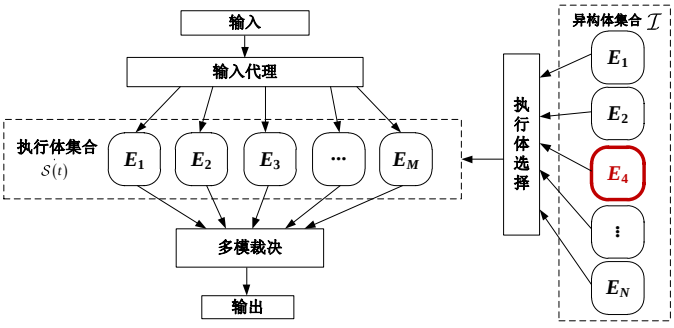

图 1 拟态控制器抽象模型.

本文所用的自适应拟态控制器系统模型如图 2 所示。自适应的拟态控制器包括异构体集合、执行体选择模块、负反馈模块、多模裁决模块。我们在控制系统中引入负反馈模块，用于连接多模裁决器与执行体选择模块，通过互相交换信息实现多模裁决的裁决策略与执行体选择模块的选择策略的自适应动态调整。执行体选择模块根据负反馈控制器所反馈的信息从异构体集合中选择 M 个执行体，输入代理将输入信息分发给 M 个执行体。M 个执行体根据输入信息进行本地处理得到本地裁决结果。多模裁决器结合负反馈控制器提供的信息，收集 M 个执行体的本地裁决结果，根据多模裁决算法输出全局裁决结果。

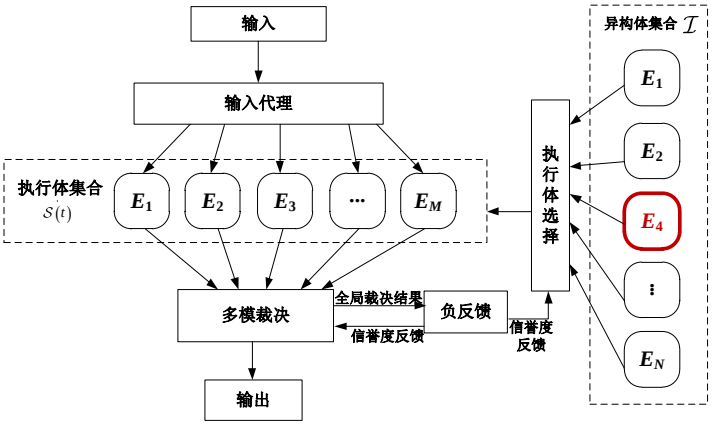

图 2 自适应的拟态控制器系统模型.

由于现有的执行体选择与多模裁决模块之间没有交互，控制器系统无法根据网络变化及时调整防御策略，可能降低多模裁决器的全局裁决结果正确性。另外，现有工作中异构体集需要轮询清理，数据同步带来的通信开销较大，防御成本较高。为解决上述问题，本文基于图 2 的系统模型，分别阐述自适应的拟态控制器中负反馈、执行体选择、多模裁决模块的工作机理。

3 自适应的拟态控制器

3.1 执行体信誉度更新机制

a) 信誉度指标：用 $y_j(t)$ 表示 t 时刻执行体 j 的本地裁决结果，$j \in \mathcal{S}(t)$，j=1,2,…,M。用 $\gamma(t)$ 表示 t 时刻多模裁决器的全局裁决结果。由于异构体功能相同，因此理论上，当多模裁决器做出正确的全局裁决时，未被攻击的执行体的本地裁决结果与多模裁决器的全局裁决结果基本一致，而受到恶意攻击的执行体的本地裁决结果和全局裁决结果存在较大差异。考虑到信息通信以及数据表示可能存在误差，我们允许执行体的本地裁决结果与全局裁决结果存在差异。用 η_y 表示执行体没有遭受攻击时，控制器允许的本地裁决与全局裁决之间的最大差异。η_y 的数值取决于控制器系统所涉及的业务内容，由控制器事先指定。

定义信誉度为一个执行体可以被信任的程度，一段时间内该执行体本地裁决结果与全局裁决结果差异

不超过 η_y 的频率。用 $r_i(t)$ 表示 t 时刻执行体 i 的信誉度，i=1,2,…,M。用 $\mathcal{T}_j(T)$ 表示截止 T 时刻，异构体 j 被选择为执行体的时刻的集合。T 时刻，执行体 j 的信誉度表示为

$$r_j(T)=\frac{\sum_{t\in\mathcal{T}_j(T)}\delta\left(\left|\gamma(t)-y_j(t)\right|\le\eta_y\right)}{\left|\mathcal{T}_j(T)\right|} \tag{1}$$

对于 t 时刻未被选中的执行体，信誉度仍然与前一时刻一致，保持不变。由上述描述可知，信誉度的动态更新准则表示为

$$r_i(t)=\begin{cases}\dfrac{\left|\mathcal{T}_j(t-1)\right|r_i(t-1)+\delta\left(\left|\gamma(t)-y_j(t)\right|\le\eta_y\right)}{\left|\mathcal{T}_j(t-1)\right|+1} & i\in\mathcal{S}(t)\\ r_i(t-1) & i\notin\mathcal{S}(t)\end{cases} \tag{2}$$

其中，t=1,2,...，$r_i(0)$ 表示执行体 i 的初始信誉度。$\delta(\cdot)$ 函数定义为 $\delta(x)=\begin{cases}1 & x=0\\ 0 & x\neq 0\end{cases}$。用 $\mathbf{r}(t)=\left[r_1(t),r_2(t),...,r_N(t)\right]$ 表示 t 时刻所有执行体的信誉度，$\mathbf{r}(t)\in\mathbb{R}^{1\times N}$。

当 t 时刻的本地判决结果与全局判决结果差异超过 η_y 时，认为该执行体在 t 时刻受到恶意攻击。换言之，若 $\left|\gamma(t)-y_j(t)\right|>\eta_y$，认为执行体 j 很可能受到恶意攻击，应当降低多模裁决器对该执行体的信任程度，减少该执行体对全局裁决结果的影响。相反，$\left|\gamma(t)-y_j(t)\right|\le\eta_y$ 时，应当增加多模裁决器对该执行体的信任程度。由于正常情况下 $\gamma(t)-y_j(t)$ 来源于数据的误差，考虑到这类误差通常由信道噪声或数值表示造成的，同时结合现有文献的通常做法[13,14]，本文也假设对于不受恶意攻击的执行体，$\gamma(t)-y_j(t)$ 服从正态分布。

b) 信誉度指标可行性说明：由上述信誉度定义及更新机制可知，执行体的信誉度表示一段时间内执行体不受恶意攻击的频率。由于不受恶意攻击的执行体的 $\gamma(t)-y_j(t)$ 服从正态分布，则 $\delta\left(\left|\gamma(t)-y_j(t)\right|\le\eta_y\right)$ 服从二项分布。因此，不受攻击的执行体的 $r_i(t)$ 也服从正态分布。而对于受到恶意攻击的执行体，本地裁决结果存在较大错误，由此可知受攻击的执行体的 $r_i(t)$ 与不受攻击的执行体的 $r_i(t)$ 统计概率特性必然不同。因此，根据公式(2)负反馈控制器可以正确地赋予执行体信誉度，从而减少恶意执行体对全局裁决结果的影响，使多模裁决器得到正确地全局裁决结果。

3.2 基于信誉度与相异度联合优化的执行体选择算法

由于拟态防御的理论基础是“独立开发的装置或模块发生共性设计缺陷导致共模故障的情况属于小概率事件”，因此，我们引入相异度指标，使执行体选择模块在选择选择相异度高的异构体的同时，尽可能选择信誉度较高的异构体，构成执行体集。

a) 相异度指标：相异度指标用于度量不同异构体之间的相异性。我们从代码级、模块级、传输级、运行级四个层次度量执行体之间的相异程度。代码级度量考虑所用编程语言、关键数据结构、全局符号、程序布局因素，得到执行体代码级的相异指标数值，用 $c_i(t)$ 表示；模块级考虑语义距离、实时逻辑任务因素，得到执行体模块级的相异指标数值，用 $m_i(t)$ 表示；传输级上，考虑到有多种能实现传输数据的传输协议，各协议之间相异度不同，功能相同。因此，在传输级从协议特征的角度，评价各协议之间的差异度，得到执行体传输级的相异指标数值，用 $b_i(t)$ 表示；运行级考虑操作系统、CPU 架构、编译方式，得到执行体运行级的相异指标数值，用 $o_i(t)$ 表示。用 w_1, w_2, w_3, w_4 表示四个层次相异度的权重，则执行体 i 的相异指标 $d_i(t)$ 表示为 $d_i(t) = w_1 c_i(t) + w_2 m_i(t) + w_3 b_i(t) + w_4 o_i(t)$ 。用 $\mathbf{d}(t) = \left[d_1(t), d_2(t), ..., d_N(t)\right]$ 表示 t 时刻异构体集合中所有执行体的相异度指标， $\mathbf{d}(t) \in \mathbb{R}^{1\times N}$ 。

b) 基于信誉度与相异度联合优化的执行体选择算法: 由前文描述可知，相异度指标可以表征异构体之间的相异程度。执行体选择模块兼顾相异度与信誉度，选择相异度与信誉度都尽可能高的执行体集合，从而实现拟态防御。因此，执行体选择问题描述为

$$\begin{aligned} &\mathcal{S}^*(t) = \arg \sum_{\mathcal{S}(t)} \sum_{i,\, j\in\mathcal{S}(t)} \left\| d_i(t) - d_j(t) \right\| + \sum_{t\in\mathcal{S}(t)} r_i(t) \\ &s.t. \quad \left|\mathcal{S}(t)\right| = M \end{aligned} \tag{P.1}$$

由于满足条件 $|\mathcal{S}(t)| = M$ 的 $\mathcal{S}(t)$ 可枚举，因此，问题(P.1)可通过穷举法获得最优解。

3.3 自适应的拟态负反馈模块

拟态防御理论认为执行体尽可能异构化，才能最大限度地降低系统发生故障的概率。因此，执行体的选择应当主要取决于相异度。为了达到上述目的，本文认为如果负反馈模块发现信誉度降低的执行体，则认为该执行体很可能受到恶意攻击，需要告知异构体池清洗相应的异构体，同时负反馈模块调整其信誉度等指标回到初始数值，避免执行体选择算法只选择信誉度高的异构体，而导致执行体之间的相异度不够高。

结合上述负反馈模块的工作机理以及问题(P.1)，T 时间内的执行体选择算法描述由算法 1 给出。

算法 1 基于信誉度与相异度联合优化的执行体选择算法

输入 初始化 M，N，$\mathbf{r}(1) = [0,0,...,0]$，$\mathcal{T}_j(0) = \varnothing$, j=1,2,…,M，$\mathcal{S}(t-1) = \varnothing$

(1) **for** t=1:T **do**
(2) **for** i=1:N **do**
(3) **if** $i \in \mathcal{S}(t-1)$

(4) $\dfrac{\left|\mathcal{T}_j(t-1)\right| r_i(t-1)+\delta\left(\left|\gamma(t)-y_j(t)\right|\le\eta_y\right)}{\left|\mathcal{T}_j(t-1)\right|+1}$

(5) **else**

(6) $r_i(t)=r_i(t-1)$

(7) **end if**

(8) **if** $r_i(t)<r_i(t-1)$

(9) $r_i(t)=r_i(0)$, $\mathcal{T}_j(t)=\varnothing$

(10) **end if**

(11) **end for**

(12) **for** 满足$|\mathcal{S}(t)|=M$ 的集合 $\mathcal{S}(t)$ **do**

(13) 计算 $\sum_{i,j\in\mathcal{S}(t)}\left\|d_i(t)-d_j(t)\right\|+\sum_{t\in\mathcal{S}(t)} r_i(t)$

(14) **end for**

(15) 找到 $\sum_{i,j\in\mathcal{S}(t)}\left\|d_i(t)-d_j(t)\right\|+\sum_{t\in\mathcal{S}(t)} r_i(t)$ 最大时对应的 $\mathcal{S}(t)$ 即为所求

(16) **end for**

输出： $\mathcal{S}(t)$

算法 1 说明了执行体选择模块利用负反馈控制器发送的异构体信誉度，选择相异度与信誉度都尽可能大的异构体作为执行体。但由于各执行体信誉度不同，因此，还需要改进多模裁决器的裁决算法。

3.4 改进的基于信誉度的多模裁决算法

由于现有拟态控制器没有引入信誉度，多模裁决算法大多采用则多裁决，或者将本地裁决结果取与、或，无法得到最接近真实结果的裁决结果。本文结合 3.1 定义的信誉度指标，利用条件最大似然法得到多模裁决结果，该方式能够得到概率上最接近真实结果的裁决结果。

t 时刻负反馈模块根据多模裁决模块的全局裁决结果更新各执行体的信誉度，因此，*t*+1 时刻多模裁决器可以利用 *t* 时刻执行体的信誉度，得到全局裁决结果，该方式在数学上表示为

$$\gamma^*(t)=\arg\max_{\gamma(t)} P\left(y_1(t),y_2(t),...,y_M(t)\,|\,\gamma(t),\mathbf{r}(t)\right) \tag{3}$$

其中，$\gamma^*(t)$表示 *t* 时刻多模裁决器的最优全局裁决结果。$P\left(y_1(t),y_2(t),...,y_M(t)|\gamma(t),\mathbf{r}(t)\right)$表示以当前信誉度为前提，本地裁决结果的条件概率。

由此，多模裁决器利用负反馈模块发送的各执行体信誉度按公式(3)得到全局裁决结果，并将当前的全

局裁决结果发给负反馈模块。负反馈模块按公式(2)更新各执行体的信誉度，将信誉度反馈给执行体选择模块与多模裁决模块，执行体选择模块更新下一时刻的选择策略，多模裁决模块也同时更新下一时刻的裁决算法。

3.5 自适应的拟态控制器工作流程及优势分析

本文提出的自适应拟态控制器，兼顾执行体之间的相异度与执行体各自的信誉度，达到降低发生共性缺陷概率、提高控制系统安全性的目的，从而有效防御各类未知攻击。综合 3.2 至 3.4 节所述，自适应的拟态控制器工作流程图如图 3 所示。

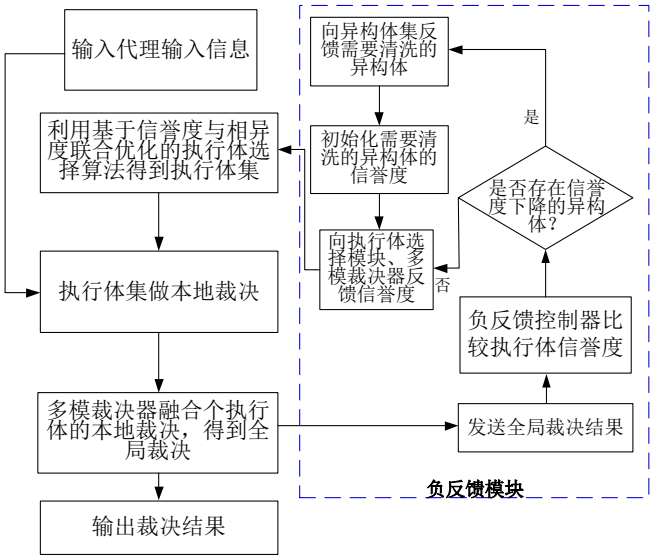

图 3 自适应的拟态控制器工作流程

首先，执行体选择模块根据负反馈模块提供的各异构体信誉度，利用算法 1 得到异构程度最高且脆弱程度最低的执行体集。接着，各执行体集根据输入代理分发的输入信息做本地裁决，得到本地裁决结果。之后，多模裁决器模块根据信誉度按公式(3)得到全局裁决，发给负反馈模块。最后，负反馈模块按公式(2)更新各执行体信誉度，同时判断是否存在需要清洗的执行体，并将更新后的信誉度发给选择模块。

与现有工作方式不同，本文改进的控制系统中引入相异度与信誉度两种指标，提出基于信誉度与相异度联合优化的执行体选择算法，并改进多模裁决算法。上述方式的优点在于：1）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；2）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；3）异构体清洗的时刻视其信誉度高低而定，不再需要轮询清理，能够防御未知攻击同时降低防御成本。当然该优势是以引入信誉度指标为代价获得的；4）拟态防御认为共模故障的情况属于小概率事件。因此，可以认为受攻击的执行体不超过一半是成立的。在此条件下，本文提出的方法总是奏效。

4 仿真结果

仿真中的相关参数设定为：1）执行体选择模块从 6 个异构体中选择 4 个形成执行体集。假设控制器执行相同的任务，因此认为异构体之间传输级、模块级安全性与性能相同。代码级与运行级的相异度指标如表 1 所示，且代码级的权重为 0.4，运行级的权重为 0.6。6 个异构体的架构如表 2 所示；2）各异构体初始信誉度均为 0.5。在 11、22、33 时刻，异构体 1、2、4 分别受到恶意攻击；3）仿真假设控制器需要向底层硬件设备下发指令，为量化说明指令是否正确，不失一般性地假设指令集为{0,1,2,3,4,5}。多模裁决器采用加权求均值再量化的方式得到全局裁决结果。假设真实的指令顺序变化为 3,5,4。

表 1 相异度指标数值设定

代码级 (权重 0.4)	代码类型	java	C++	python	c#		
	权重值	0.2	0.4	0.6	0.8		
运行级 (权重 0.6)	平台类型	Vmware Ubuntu	Virtualbox Ubuntu	Vmware Centos	Virtualbox Centos	Vmware Windows	Virtual Windows
	权重值	0.2	0.32	0.44	0.56	0.68	0.8

表 2 6 个异构体架构

异构体序号	代码类型	运行平台类型
异构体 1	java	Vmware Ubuntu
异构体 2	C++	Virtualbox Ubuntu
异构体 3	python	Vmware Centos
异构体 4	C#	Virtualbox Centos
异构体 5	python	Vmware Windows
异构体 6	C++	Virtualbox Windows

图 4 给出了 6 个异构体的信誉度随时间变化的趋势。由图可知，执行体受到恶意攻击，信誉度下降，负反馈控制器反馈清洗异构体 1 的信息，并重新选择执行体集，从而保证全局裁决结果的正确性。例如，在初始 10 个时刻，没有发生攻击，选择模块根据相异度最大原则选择异构体 1，2，4，5 进行多模裁决。在第 11 时刻执行体 1 被攻击，信誉度从 1 下降为 0.9。于是，负反馈控制器要求执行体 1 下线清洗，重新选择的执行体集为 2，3，4，5。经过 5 个时刻执行体 1 清洗结束，信誉度回到初始值 0.5，且没有发生恶意攻击，于是异构体 1，2，4，5 继续进行多模裁决。在第 22 时刻，异构体 2 受到攻击，负反馈控制器反馈清洗异构体 2 的信息后，再次选择执行体 2，4，5，6 进行多模裁决。由此可知，信誉度的下降能表征执行体受到攻击。当受到恶意攻击的执行体被清洗后，执行体选择模块仍然会选择相异度最大的执行体，实现拟态防御。

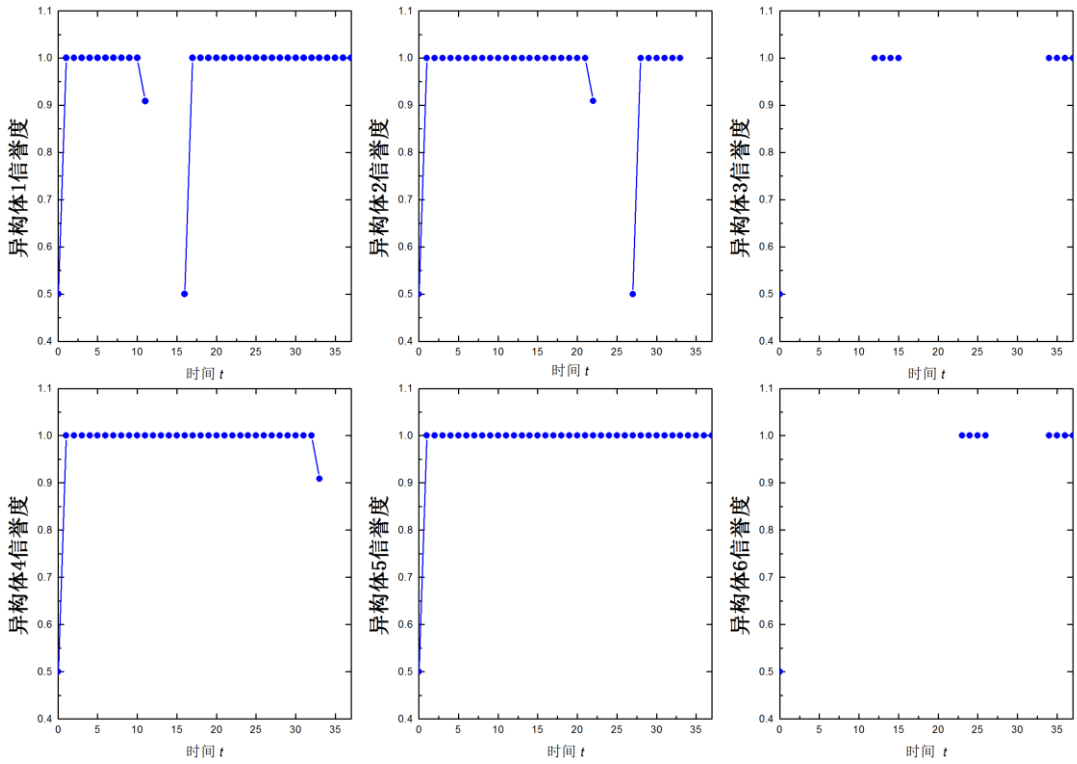

图 4 6 个异构体信誉度随时间变化趋势

图 5 给出了采用不同拟态控制器的全局裁决结果对比。图中红线表示现有的拟态控制器采用定期轮询清洗且随机选择执行体的方式，每隔 5 个时刻清洗一个异构体，选择模块总是随机选择执行体。由图可知，当清洗的时刻与执行体受攻击的时刻完全错开时，定期轮询的清洗不能发挥防御效果，且定期轮询清洗，引入了较大的防御成本。蓝色的线表示采用本文提出的自适应的拟态控制器后的全局裁决结果。利用本文提出的方法，清洗的时刻取决于执行体状态，较少产生错误。因此，本文提出的自适应的拟态控制器能提高全局裁决结果的正确性，同时由于只引入了信誉度指标作为清洗异构体的依据，防御成本相对较低。

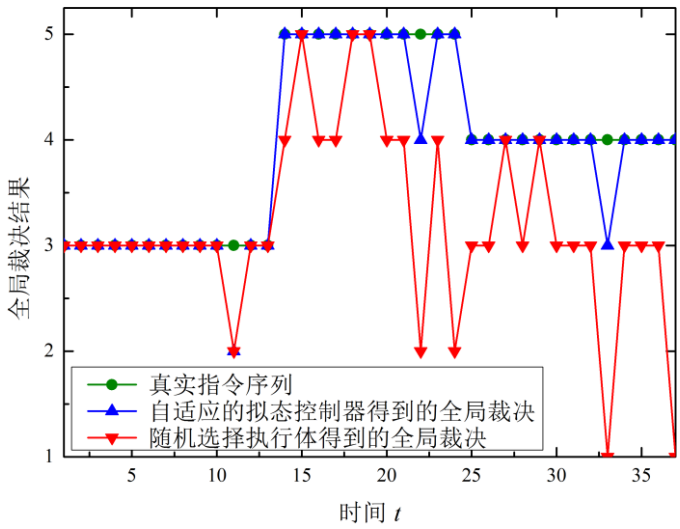

图 5 控制器不同工作方式对全局裁决结果的影响

5 结束语

本文研究了自适应的拟态控制器。我们引入动态更新的信誉度指标，实现各执行体脆弱程度的动态更新；定义相异性指标用于衡量各异构体之间的异构程度。基于前述指标，我们首先提出基于信誉度与相异度联合优化的执行体选择算法，兼顾所选异构体的相异度与信誉度，使执行体集中的执行体异构程度最高且脆弱程度最低，进一步降低发生共性缺陷的概率，提高控制系统安全性。另外，结合信誉度指标，我们改进现有多模裁决算法，获得最接近真实输出的多模裁决结果。最后，我们引入负反馈模块，动态更新各执行体的信誉度。由此，本文设计的拟态控制器包括基于信誉度与相异度联合优化的执行体选择、基于信誉度的多模裁决以及负反馈三大模块。仿真结果表明，所提出的方法能有效提高控制系统安全性，同时不造成过高的防御成本。

6 致谢

本文研究工作受支持的项目包括：之江实验室重大科研项目先进工业互联网安全平台(2018FD0ZX01)；国家重点研发计划(2016YFB0800201, 2016YFB0800102)；浙江省重点研发计划(2017C01064)；浙江大学自主科研计划项目(2016XZZX001-04)。

7 参考文献

[1] 邬江兴. 网络空间拟态安全防御[J]. 保密科学技术, 2014(10):4-9.

WU J X. Cyber Mimic Security Defense [J].secrecy science and technology, 2014(10):4-9.

[2] 邬江兴. 网络空间拟态防御研究[J]. 信息安全学报, 2016, 1(4):1-10.

WU J X. Research on Cyber Mimic Defense [J]. Journal of Cyber Security, 2016, 1(4):1-10.

[3] 谢敏, 吴亚雄, 闫圆圆,等. 基于改进动态自适应模糊 Petri 网与 BP 算法的电网故障诊断[J]. 中国电机工程学报, 2015, 35(12):3008-3017.

XIE M, WU Y X, YAN Y Y, et al, ZHU Yanhan. Power System Fault Diagnosis Based on Improved Dynamic Adaptive Fuzzy Petri Nets and Back Propagation Algorithm [J]. Proceedings of the CSEE, 2015, 35(12):3008-3017.

[4] CAI G, WANG B, LUO Y, et al. A Model for Evaluating and Comparing Moving Target Defense Techniques Based on Generalized Stochastic Petri Net[M]. Advanced Computer Architecture. Springer Singapore, 2016:184-197.

[5] JIAN S, MENG Y, WANG S, et al. Reliability and safety analysis of redundant vehicle management computer system[J]. Chinese Journal of Aeronautics, 2013, 26(5):1290-1302.

[6] 任权, 贺磊, 邬江兴. 基于离散马尔可夫链的不同抗干扰系统模型分析[J]. 网络与信息安全学报, 2018(4):1-4.

REN Q, HE L, WU J X. Analysis of different anti-interference system models based on discrete time Markov chain [J]. Chinese Journal of Network and Information Security, 2018(4).

[7] 李军飞, 胡宇翔, 邬江兴. 基于拜占庭容错提高 SDN 控制层可靠性的研究[J]. 计算机研究与发展, 2017, 54(5):952-960.

LI J F, HU Y X, WU J X. Research on Improving the Control Plane Reliability in SDN based on Byzantine Fault-Tolerance [J]. Journal of Computer Research and Development, 2017, 54(5):952-960.

[8] 李军飞, 兰巨龙, 胡宇翔,等. SDN 多控制器一致性的量化研究[J]. 通信学报, 2016, 37(6):86-93.

LI J F, LAN J L, HU Y X, et al. Quantitative approach of multi-controller’s consensus in SDN[J]. Journal on Communications, 2016, 37(6):86-93

[9] 常箫, 张保稳, 张莹. 一种面向网络拟态防御系统的信息安全建模方法[J]. 通信技术, 2018(1):165-170.

CHANG X, ZHANG B W, ZHANG Y. Information Security Modeling Method for CMD Systems[J]. Communications Technology, 2018(1):165-170.

[10] 马海龙, 江逸茗, 白冰,等. 路由器拟态防御能力测试与分析[J]. 信息安全学报, 2017, 2(1):43-53.

MA H L, JIANG Y M, BAI B, et al. Tests and Analyses for Mimic Defense Ability of Routers[J]. Journal of Cyber Security, 2017, 2(1):43-53.

[11] 王禛鹏, 扈红超, 程国振,等. 软件定义网络下的拟态防御实现架构[J]. 网络与信息安全学报, 2017, 3(10):52-61.

WANG Z P, HU H C, CHENG G Z, et al. Implementation architecture of mimic security defense based on SDN [J]. Chinese Journal of Network and Information Security, 2017, 3(10):52-61.

[12] 高洁, 邬江兴, 胡宇翔,等. 基于拜占庭容错的软件定义网络控制面的抗攻击性研究[J]. 计算机应用, 2017, 37(8):2281-2286.

GAO J, WU J X, HU Y X, et al. Research of control plane' anti-attacking in software-defined network based on Byzantine fault-tolerance [J]. Journal of Computer Applications, 2017, 37(8):2281-2286.

[13] WEI C, LIN H, CHEN P, et al. Target Localization Using Sensor Location Knowledge in Wireless Sensor Networks[J]. IEEE Wireless Communications Letters , 2017 , PP (99) :1-1

[14] HUG G, GIAMPAPA J. Vulnerability Assessment of AC State Estimation with Respect to False Data Injection Cyber-Attacks[J]. IEEE Transactions on Smart Grid, 2012, 3 (3):1362-1370

[作者简介]

 沈丛麒，女，1994 年出生于浙江，之江实验室网络信息安全研究中心工程师。主要从事网络安全、工业互联网安全等领域方向的科学研究工作。E-mail：shencq@zhejianglab.com

 吴春明，男，1967 年生于浙江萧山，博士，浙江大学计算机系统结构与网络安全研究所教授、博导。主要从事网络安全、互联网体系结构、柔性可重构网络、网络资源弹性管控与虚拟化等领域方向的科学研究工作。 E-mail: wuchunming@cs.zju.edu.cn