(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111935071 B
(45)授权公告日 2022.11.18

(21)申请号 202010561767.7
(22)申请日 2020.06.18
(65)同一申请的已公布的文献号
申请公布号 CN 111935071 A
(43)申请公布日 2020.11.13
(73)专利权人 华南理工大学
地址 510641 广东省广州市天河区五山路381号
(72)发明人 陆以勤 陈卓星 覃键诚 程喆
(74)专利代理机构 广州嘉权专利商标事务所有限公司 44205
专利代理师 胡辉
(51)Int.Cl.
H04L 9/40(2022.01)
(56)对比文件
CN 110018895 A,2019.07.16
CN 110290100 A,2019.09.27
CN 110750802 A,2020.02.04
CN 106874755 A,2017.06.20
CN 110018895 A,2019.07.16
张杰鑫等.“面向拟态构造Web服务器的执行体调度算法”.《计算机工程》.2019,第45卷(第08期),
Guo, Wei, et al.."Scheduling sequence control method based on sliding window in cyberspace mimic defense.".《IEEE Access》.2019,(第8期),
Wu, Zhaoqi, and Jin Wei.." Heterogeneous Executors Scheduling Algorithm for Mimic Defense Systems".《2019 IEEE 2nd International Conference on Computer and Communication Engineering Technology (CCET)》.2019,
仝青等.“拟态防御Web服务器设计与实现”.《软件学报》.2017,第28卷(第04期),
张杰鑫等.拟态构造的Web服务器异构性量化方法.《软件学报》.2020,(第02期),第322-335页.
审查员 蒋联娇

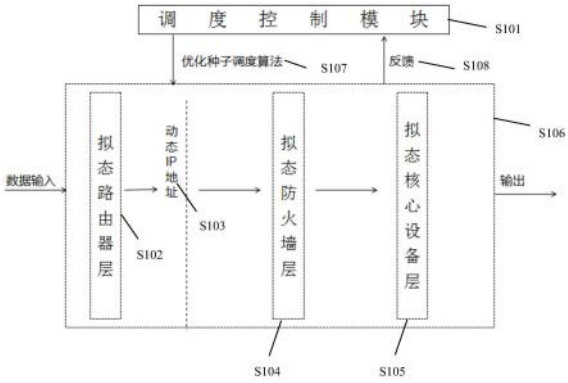
权利要求书3页 说明书11页 附图4页

(54)发明名称

多层拟态防御方法、装置、存储介质及多层拟态系统

(57)摘要

本发明公开了一种多层拟态防御方法、装置、存储介质及多层拟态系统,其中方法包括:第一阶段评估每一个执行体的实际性能,其中,所述实际性能包括每个所述执行体的初始性能与输出裁决器的累计反馈情况;第二阶段分别以每一个执行体作为种子执行体,综合考虑其余执行体的实际性能和其余执行体与种子执行体相互之间的异构性,从而得到兼顾性能与适配性的执行体集合及所述执行体集合的性能评估;第三阶段综合考虑所述执行体集合的整体性能与随机性,从当前时刻最适合调度的三个执行体集合中随机选择一个所述执行体集合进行拟态调度。本发明使得调度方法兼备完善性,可更新性和随机性,表现出更好的性能,可广泛应用于互联网中的信息安全技术领域。



CN 111935071 B

1.一种多层拟态防御方法,其特征在于,所述多层拟态防御方法包括三个阶段以及各所述阶段内拟态防御实施的各项指标评估,包括:

第一阶段评估每一个执行体的实际性能,其中,所述实际性能包括每个所述执行体的初始性能与输出裁决器的累计反馈情况;

第二阶段以每一个执行体作为种子执行体,综合考虑其余执行体的实际性能和其余执行体与种子执行体相互之间的异构性,从而得到兼顾性能与适配性的执行体集合及所述执行体集合的性能评估;

第三阶段综合考虑所述执行体集合的整体性能与随机性,根据第二阶段所得到的执行体集合性能评估,从当前时刻最适合调度的三个执行体集合中随机选择一个所述执行体集合进行拟态调度;

所述第一阶段评估每一个执行体的实际性能,包括:

采用评价指标S_per反映拟态防御中所述执行体的所述初始性能;

采用评价指标S_feedback反映由所述输出裁决器反馈的所述执行体的实际安全性能的累计加和;其中,所述输出裁决器反馈包括正反馈和负反馈;

对每一个所述执行体依据评价指标S_per和评价指标S_feedback权重加和,获得所述执行体的各自实际性能得分S_A,当所述执行体的实际性能得分S_A低于预设阈值时,将所述执行体清洗出执行体资源池;

所述第二阶段以每一个执行体作为种子执行体,综合考虑其余执行体的实际性能和其余执行体与种子执行体相互之间的异构性,包括:

采用评价指标S_H反映不同所述执行体间的异构性;

采用适配性得分S_B反映其余所述执行体分别对于所述种子执行体的兼顾性能的适配性;

当所述执行体的S_H低于预设的阈值时,所述执行体因与所述种子执行体的异构性指标不满足实际适配要求,所述执行体的适配性得分S_B设定为0;选定所述种子执行体的前提下,从其余执行体中选择适配性得分S_B排名前n-1的执行体,将被选中的执行体与所述种子执行体共同组成种子执行体的适配执行体集合,并将所述种子执行体的实际性能得分S_A与该执行体集合其余执行体的各自适配性得分S_B进行加和,从而得到执行体集合分数S_C,其中n表示拟态网络中执行体集合冗余度;

采用遍历的方法以每一个所述执行体作为所述种子执行体,得到m个所述执行体集合以及对应的执行体集合分数S_C,所述执行体集合分数S_C越高表示集合越适合当前时刻进行调度,其中m为执行体资源池中执行体个数;所述适配性得分S_B通过以下方式获得:

确定所述种子执行体,计算其余执行体和种子执行体之间的所述评价指标S_H;

将其余执行体的所述实际性能得分S_A和所述评价指标S_H权重加和,得到基于性能的适配性得分S_B。

2.根据权利要求1所述的一种多层拟态防御方法,其特征在于,所述评价指标S_per由所述执行体资源池初始化时获得,所述评价指标S_per包含以下三方面内容:

对各个所述执行体的硬件运行速度的测试评价;

对各个所述执行体的每秒事务处理次数、执行体网络延时、最大TCP并发连接数、吞吐量和执行体响应时间的测试评价;

由于不同所述执行体所使用的软硬件条件不同，对不同所述执行体设置百分制的优先分数。

3.根据权利要求1所述的一种多层拟态防御方法，其特征在于，所述正反馈为：当所述执行体的输出结果与所述输出裁决器所得到的输出结果一致时，反馈一个正值分数进行奖励，反映所述执行体在现阶段能够正常工作；

所述负反馈为：

当所述执行体的输出结果与所述输出裁决器所得到的输出结果不一致时，反馈一个负值分数进行惩罚，反映该执行体在现阶段存在被攻击的风险。

4.根据权利要求1所述的一种多层拟态防御方法，其特征在于，所述评价指标S_H通过以下方式获得：

利用预设的通用漏洞列表，对各个所述执行体的相同或相近网络漏洞进行评估，并给出执行体之间的共生漏洞检测分数；

利用拟态防御中关于异构性的证明计算，评估组成不同执行体的各个构件之间的软硬件差异，并给出执行体之间差异性分数；

将所述共生漏洞检测分数和所述执行体之间差异性分数按照权重加和得到所述评价指标S_H。

5.一种多层拟态防御装置，其特征在于，包括：

至少一个处理器；

至少一个存储器，用于存储至少一个程序；

当所述至少一个程序被所述至少一个处理器执行，使得所述至少一个处理器实现权利要求1-4任一项所述的一种多层拟态防御方法。

6.一种存储介质，其中存储有处理器可执行的指令，其特征在于，所述处理器可执行的指令在由处理器执行时用于执行如权利要求1-4任一项所述一种多层拟态防御方法。

7.一种多层拟态系统，用于执行如权利要求1-4任一项所述的一种多层拟态防御方法，其特征在于，包括：

动态IP地址模块，用于设置为定时跳变IP；

拟态路由器层，用于实现异构冗余的路由器的动态调度，生成拟态的路由表，阻断针对路由器漏洞的恶意攻击；

拟态防火墙层，用于实现异构冗余的网络防火墙的动态调度，依照预设的网络安全规则，允许或是限制传输的数据通过，筛选进入核心设备的数据；

拟态核心设备层，用于实现异构冗余的网络核心设备的动态调度；

调度控制器，用于从各个拟态层的执行体资源池中动态进行执行体调度，并接收各层输出裁决器的反馈信息；

所述拟态路由器层、所述拟态防火墙层和所述拟态核心设备层中均包含输入分发器，执行体资源池，上线执行体集合和输出裁决器，各层内输入数据经输入分发器，复制分发到由拟态系统调度控制器所调度的执行体集合的各个执行体中，执行体各自独立地进行运算并得到输出结果，将其传输至输出裁决器中，输出裁决器依据大数裁决得到该拟态层的输出，并将裁决结果与各个执行体的输出结果反馈至调度控制器中；

由所述拟态路由器层、所述动态IP地址、所述拟态防火墙层和所述拟态核心设备层依

先后顺序组成拟态网络防御模块，上一个拟态层的输出裁决器与下一个拟态层的输入分发器之间相连，实现拟态层之间的连接，各个拟态层工作时互相独立，通过多层拟态实现协同防御。

多层拟态防御方法、装置、存储介质及多层拟态系统

技术领域

[0001] 本发明涉及互联网中的信息安全技术，尤其涉及一种多层拟态防御方法、装置、存储介质及多层拟态系统。

背景技术

[0002] 拟态防御技术是我国邬江兴院士于2016年在《信息安全学报》上首次正式提出的一种新型网络防御技术。这种技术借鉴了自然界中一种生物模仿另外一种生物的外观和行为以获得生存好处的拟态现象，设计了一种网络构件动态变化的防御技术，故名拟态防御。具体地，就是改变传统网络静态单一，只能被动防御的特性，通过设计网络构件的多个冗余异构的硬件变体以及相应的软件变体，并动态地、伪随机地对这些异构执行体进行调度，从而实现网络的主动防御。这种防御技术最大的优点在于，基于“执行体都可能存在一定安全缺陷，但极少出现在独立完成同样任务时，多数执行体存在同样安全缺陷的情形”的公理前提，可以实现对网络中未知漏洞，后门和木马的有效防御，这在传统网络防御技术中是难以实现的。

[0003] 在拟态防御技术中，输入数据经分发器，复制分发到由一定的调度策略所调度的执行体集合的各个执行体中，执行体各自独立地进行运算并得到各自的输出结果，将其传输至输出裁决器中，输出裁决器依据裁决规则得到最终的输出结果。在这个过程中，调度策略决定了每一次调度中，多个异构执行体之间以何种方式合理地选出部分组合在一起，从而起到较高效的防御效果，是拟态防御可以实现动态性的关键。因此，调度策略的性能好坏很大程度上影响着一个拟态防御网络的实际效果，也是拟态防御中一个热点研究问题。

[0004] 目前常见的拟态防御调度方法包括以下四种：1、执行体完全随机的调度方法；2、执行体先到先换的调度方法；3、优先选择调度权重大的执行体进行调度的调度方法；4、考虑了执行体间异构性和其各自网络服务质量的随机种子调度方法。简单介绍如下：

[0005] 现有技术一：执行体完全随机的调度方法。

[0006] 原理：在调度决策时刻，对执行体资源池中的异构冗余执行体采用完全随机进行调度的方法，从而可以显著降低调度的复杂度，有利于减少网络开销，也使得拟态网络对攻击者呈现最大的不确定性，使得网络难以被测定。

[0007] 缺点：完全随机的策略并不意味着得到的是执行体的较优组合，例如随机选择的执行体之间如果是用相同的操作系统实现的，可能会存在相同的未知漏洞，从而被网络攻击者简单攻破。此外，这种策略下拟态网络不受网络管理人员的约束与管理，拟态网络的调度不受控制。

[0008] 现有技术二：执行体先到先换的调度方法

[0009] 原理：执行体集合中先被调度的执行体有最长的上线工作时间，已经在网络中暴露得最久，更容易被网络攻击者利用其未知漏洞。因此在调度决策时刻，上线时长最大的执行体首先被更换。

[0010] 缺点：执行体上线时间长，往往也意味着之前未受到网络攻击，因此具有较优的安

全性能，这个角度来说其不宜被更换。此外执行体先到先换本身就是一种规律，其周期很容易被网络攻击者探知，这使得拟态网络变为一种类似静态的网络，失去应有的安全性。

[0011] 现有技术三：优先选择调度权重大的执行体进行调度的调度方法

[0012] 原理：基于在理论上每一个执行体的具体表现是不相同的，因此通过实践或者人为设置的方式，设定每一个执行体的调度权重，从而选择网络管理人员更偏爱或与实际网络需求比较契合的的执行体进行调度。这种方法也使得网络具有一定不确定性。

[0013] 缺点：执行体的调度权重一旦设定，执行体的先后关系就随之确定且不易改变，这样的拟态网络缺乏灵活性。此外，调度权重过度依赖网络管理人员的人为设置，网络管理人员要花费大量精力在异构执行体的权值赋予上，并且调度权重更改起来较为复杂。

[0014] 现有技术四：考虑了执行体间异构性和其各自网络服务质量的随机种子调度方法。

[0015] 原理：这种调度算法考虑了执行体间异构性和其各自网络服务质量。该方法先参数初始化，并测试各个执行体的各种网络服务质量属性值，除去网络服务质量过差的执行体。在调度决策时刻，在剩余执行体中随机选择一个作为种子执行体，再进一步除去和种子执行体异构性小于阈值的执行体。这时，将剩余的备选执行体组成多个执行体集合，从中选出综合指标ES最大的集合进行调度。从而得到随机种子执行体的一个较优组合。

[0016] 缺点：1、该方法未引入反馈，只考虑异构性和网络服务质量是不够的；2、该方法中种子执行体是随机选择的，其安全质量无法保证，由此得到的执行体集合可能只是一个局部最优解；3、如果执行体资源池没有更新，则综合指标ES不变，各个种子执行体对应的执行体集合是固定的，算法缺乏灵活性。

发明内容

[0017] 为了解决上述技术问题之一，本发明的目的是提供一种应用优化种子调度算法的一种多层拟态防御方法、装置、存储介质及多层拟态系统。

[0018] 本发明所采用的技术方案是：

[0019] 一种多层拟态防御方法，所述多层拟态防御方法包括三个阶段以及各所述阶段内拟态防御实施的各项指标评估，包括：

[0020] 第一阶段评估每一个执行体的实际性能，其中，所述实际性能包括每个所述执行体的初始性能与输出裁决器的累计反馈情况；

[0021] 第二阶段以每一个执行体作为种子执行体，综合考虑其余执行体的实际性能和其余执行体与种子执行体相互之间的异构性，从而得到兼顾性能与适配性的执行体集合及所述执行体集合的性能评估；

[0022] 第三阶段综合考虑所述执行体集合的整体性能与随机性，从当前时刻最适合调度的三个执行体集合中随机选择一个所述执行体集合进行拟态调度。

[0023] 进一步，所述第一阶段评估每一个执行体的实际性能，包括：

[0024] 采用评价指标S_per反映拟态防御中所述执行体的所述初始性能；

[0025] 采用评价指标S_feedback反映由所述输出裁决器反馈的所述执行体的实际安全性能；

[0026] 对每一个所述执行体依据评价指标S_per和评价指标S_feedback权重加和，获得

所述执行体的各自实际性能得分S_A，当所述执行体的实际性能得分S_A低于预设阈值时，将所述执行体清洗出执行体资源池。

[0027] 进一步，所述评价指标S_per由在所述执行体资源池初始化时获得，所述评价指标S_per包含以下三方面内容：

[0028] 用于测试各个所述执行体的硬件运行速度；

[0029] 用于测试各个所述执行体的每秒事务处理次数、执行体网络延时、最大TCP并发连接数、吞吐量和执行体响应时间；

[0030] 由于不同所述执行体所使用的软硬件条件不同，对不同所述执行体设置百分制的优先分数。

[0031] 进一步，所述输出裁决器反馈包括正反馈和负反馈；

[0032] 所述正反馈为：

[0033] 当所述执行体的输出结果与所述输出裁决器所得到的输出结果一致时，反馈一个正值分数进行奖励，反映所述执行体在现阶段能够正常工作；

[0034] 所述负反馈为：

[0035] 当所述执行体的输出结果与所述输出裁决器所得到的输出结果不一致时，反馈一个负值分数进行惩罚，反映该执行体在现阶段存在被攻击的风险。

[0036] 进一步，所述第二阶段以每一个执行体作为种子执行体，综合考虑所述执行体的所述实际性能与相互之间异构性，包括：

[0037] 采用评价指标S_H反映不同所述执行体间的异构性；

[0038] 采用适配性得分S_B反映其余所述执行体分别对于所述种子执行体的兼顾性能的适配性；

[0039] 当所述执行体的S_H低于预设的阈值时，所述执行体因与所述种子执行体的异构性指标不满足实际适配要求，所述执行体的适配性得分S_B设定为0；

[0040] 选定所述种子执行体的前提下，从其余执行体中选择适配性得分S_B排名前n-1的执行体，将这些被选中的执行体与所述种子执行体共同组成种子执行体的适配执行体集合，并将所述种子执行体的实际性能得分S_A与该执行体集合其余执行体的各自适配性得分S_B进行加和，从而得到所述执行体集合分数S_C，其中n表示拟态网络中执行体集合冗余度；

[0041] 采用遍历的方法以每一个执行体作为所述种子执行体，分别得到m个所述执行体集合以及对应的执行体集合分数S_C，所述执行体集合分数S_C越高表示集合越适合当前时刻进行调度，其中m为执行体资源池中执行体个数。

[0042] 进一步，所述评价指标S_H通过以下方式获得：

[0043] 利用预设的通用漏洞列表，对各个所述执行体的相同或相近网络漏洞数量进行评估，并给出执行体之间的共生漏洞检测分数；

[0044] 利用拟态防御中关于异构性的证明计算，评估组成不同执行体的各个构件之间的软硬件差异，并给出执行体之间差异性分数；

[0045] 将所述共生漏洞检测分数和所述执行体之间差异性分数按照权重加和得到所述评价指标S_H。

[0046] 进一步，所述适配性得分S_B通过以下方式获得：

[0047] 确定所述种子执行体，计算其余执行体和种子执行体之间的所述评价指标S_H；

[0048] 将其余执行体的所述实际性能得分S_A和所述评价指标S_H权重加和，得到基于性能的适配性得分S_B。

[0049] 本发明所采用的另一技术方案是：

[0050] 一种多层拟态防御装置，包括：

[0051] 至少一个处理器；

[0052] 至少一个存储器，用于存储至少一个程序；

[0053] 当所述至少一个程序被所述至少一个处理器执行，使得所述至少一个处理器实现上所述方法。

[0054] 本发明所采用的另一技术方案是：

[0055] 一种存储介质，其中存储有处理器可执行的指令，所述处理器可执行的指令在由处理器执行时用于执行如上所述方法。

[0056] 本发明所采用的另一技术方案是：

[0057] 一种多层拟态系统，包括：

[0058] 动态IP地址模块，用于设置为定时跳变IP；

[0059] 拟态路由器层，用于实现异构冗余的路由器的动态调度，生成拟态的路由表，阻断针对路由器漏洞的恶意攻击；

[0060] 拟态防火墙层，用于实现异构冗余的网络防火墙的动态调度，依照预设的网络安全规则，允许或是限制传输的数据通过，筛选进入核心设备的数据；

[0061] 拟态核心设备层，用于实现异构冗余的网络核心设备的动态调度；

[0062] 调度控制器，用于从各个拟态层的执行体资源池中动态进行执行体调度，并接收各层输出裁决器的反馈信息；

[0063] 所述拟态路由器层、所述拟态防火墙层和所述拟态核心设备层中均包含输入分发器，执行体资源池，上线执行体集合和输出裁决器，各层内输入数据经输入分发器，复制分发到由拟态系统调度控制器所调度的执行体集合的各个执行体中，执行体各自独立地进行运算并得到输出结果，将其传输至输出裁决器中，输出裁决器依据大数裁决得到该拟态层的输出，并将裁决结果与各个执行体的输出结果反馈至调度控制器中；

[0064] 由所述拟态路由器层、所述动态IP地址、所述拟态防火墙层和所述拟态核心设备层依先后顺序组成拟态网络防御模块，上一个拟态层的输出裁决器与下一个拟态层的输入分发器之间相连，实现拟态层之间的连接，各个拟态层工作时互相独立，通过多层拟态实现协同防御。

[0065] 本发明的有益效果是：本发明分阶段对执行体做出调度评估，第一阶段先评估每一个执行体的各自实际性能，第二阶段再得到每一个执行体各自最适配的执行体集合，第三阶段选出较优的执行体集合进行调度，使得调度方法兼备完善性，可更新性和随机性，表现出更好的性能。

附图说明

[0066] 图1是本发明实施例提供的一种应用了优化种子调度算法的多层拟态防御网络的模块化示意图；

[0067] 图2是本发明实施例提供的一种优化种子调度算法的流程示意图；

[0068] 图3是本发明实施例提供的一种多层拟态防御装置的结构框图；

[0069] 图4是本发明实施例提供的一种具有拟态层间协同防御功能的多层拟态结构的示意图；

[0070] 图5是本发明实施例提供的一种优化种子调度算法中涉及的反馈方法流程图。

具体实施方式

[0071] 下面详细描述本发明的实施例，所述实施例的示例在附图中示出，其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的，仅用于解释本发明，而不能理解为对本发明的限制。

[0072] 在本发明的描述中，需要理解的是，涉及到方位描述，例如上、下、前、后、左、右等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。

[0073] 在本发明的描述中，若干的含义是一个或者多个，多个的含义是两个以上，大于、小于、超过等理解为不包括本数，以上、以下、以内等理解为包括本数。如果有描述到第一、第二只是用于区分技术特征为目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量或者隐含指明所指示的技术特征的先后关系。

[0074] 本发明的描述中，除非另有明确的限定，设置、安装、连接等词语应做广义理解，所属技术领域技术人员可以结合技术方案的具体内容合理确定上述词语在本发明中的具体含义。

[0075] 针对现有拟态防御技术缺乏一种完善灵活的调度方法，缺乏系统的多层防御体系，难以抵御高级持续威胁的问题，本发明实施例分阶段对执行体做出调度评估，第一阶段先评估每一个执行体的各自实际性能，第二阶段再得到每一个执行体各自最适配的执行体集合，第三阶段选出较优的执行体集合进行调度；具体地，就是通过S_per，S_feedback，S_H，S_A，S_B，S_C这六个指标分别对资源池中各个执行体的由实际测试和人为经验判定的初始性能，实际执行安全反馈，执行体间异构性，实际综合性能，与种子执行体的适配性能，执行体集合整体性能做出了量化评估；在量化评估的基础上可以有效选出当前调度时刻最适合的三个执行体集合，并在其中随机选择一种进行调度，使得调度方法兼备完善性，可更新性和随机性，表现出更好的性能；提出一种可以整合多个拟态层以及在此基础上实现协同防御的系统化拟态防御网络，从而有效抵御高级持续威胁所带来的协同控制攻击，解决了上述的问题。

[0076] 如图1所示，本发明实施例提供的一种应用了优化种子调度算法的多层拟态防御网络，该网络包含下列模块：

[0077] S101：调度控制模块，是调度算法的核心模块，包含调度控制器与资源管理器，负责执行体资源池的具体调度与资源，状态管理；

[0078] S102：拟态路由器层，实现异构冗余的路由器的动态调度，生成拟态的路由表，阻断针对路由器漏洞的恶意攻击，从信息源头上给整个网络提供一个初步的安全基础；

[0079] S103：动态IP地址，定时跳变IP；

[0080] S104:拟态防火墙层,实现异构冗余的网络防火墙的动态调度,依照网络管理人员制定的网络安全规则,允许或是限制传输的数据通过,筛选进入核心设备的数据。

[0081] S105:拟态核心设备层,实现异构冗余的网络核心设备的动态调度,网络核心设备是整个拟态网络的最终防御目标,一旦被网络攻破,将给防御者带来损失;

[0082] S106:拟态网络防御模块,集成了拟态路由器层S102,动态IP地址S103,拟态防火墙层S104,拟态核心设备层S105,是整个多层拟态系统的主体部分,可以通过多层拟态实现协同防御;

[0083] S107:优化种子调度算法,本发明实施例所提供的一种调度算法,是可应用于多层拟态防御的完善的执行体调度评价方法;

[0084] S108:反馈模块,包含拟态路由器层S102,拟态防火墙层S104,拟态核心设备层S105各拟态层输出裁决器对调度控制模块S101的反馈,用以反映各层执行体的实际工作情况与安全性能。

[0085] 如图2所示,本发明实施例提供的一种优化种子调度算法的流程包括下列步骤:

[0086] 步骤S201:先初始化资源池,给每个执行体依次进行编号,设置阈值S_A0,S_B0。进行执行体性能检测,包括运算速度,QoS,专家主观评测。

[0087] 步骤S202:将步骤S201所得各项分值归一化,并加和,得到初始性能得分S_per,完成执行体的初始性能评测。

[0088] 步骤S203:每一次裁决器输出后,将输出结果反馈至调度控制器,并更新反馈分数S_feedback。

[0089] 步骤S204:当调度决策时刻到来,开始按照优化种子调度算法进行调度。不失一般性,设定为从m个冗余执行体中选择n个进行调度。(m≥n>1)

[0090] 步骤S205:计算每一个执行体实际性能得分S_A,S_A=权重1*S_per+权重2*S_feedback,S_A综合了执行的初始性能与实际反馈的安全性能,若执行体的S_A低于阈值S_A_0,将其清洗出资源池。

[0091] 步骤S206:在执行体资源池之中,依顺序选择一个执行体作为种子执行体yi(i=1,2,3...m)。

[0092] 步骤S207:确定种子执行体yi后,计算其余执行体对yi的异构性评估S_H。

[0093] 步骤S208:计算其余执行体对于种子执行体yi的适配性得分S_B_k,S_B_k=权重1*S_A_k+权重2*S_H_k(k=1,2,3,...m-1),若执行体的S_B低于阈值S_B_0,其S_B设置为0。

[0094] 步骤S209:从其余(m-1)个执行体中选出S_B得分最高的前(n-1)个执行体,和种子执行体yi组成一个适配的执行体集合,并计算该执行体集合总分S_C_i,$S\_C_i=S\_A_i+\sum S\_B_p$(p为本步骤中所选中的n-1个执行体)。

[0095] 步骤S210:查询是否将所有执行体均分别作为种子执行体,得到与其适配的执行体集合。若已全部遍历,则转到步骤S211,否则转到步骤S206。

[0096] 步骤S211:从执行体集合总分S_C最大的前三中随机选择一个优化组合进行调度,调度决策完成。

[0097] 参见表1-表3,本发明实施例提供的一种优化种子调度算法的运算过程,包括下列阶段:

[0098] S301:第一阶段,通过将每一个执行体依据S_per和S_feedback权重加和,评估每

一个执行体的各自实际性能S_A,其中S_per是在各个执行体初始化时得到的包括硬件运行速度、执行体网络服务质量、人为优先级的初始性能评估,S_feedback是对输出裁决器所表明的各层执行体的实际工作情况与安全性能的反馈评估。

[0099] 用评价指标S_per反映拟态防御中执行体初始性能,S_per由在执行体资源池初始化时得出,包含三方面的内容:网络管理人员测试各个执行体的硬件运行速度,得到百分制的执行体硬件运行速度得分;网络管理人员测试各个执行体的每秒事务处理次数、执行体网络延时、最大TCP并发连接数、吞吐量和执行体响应时间,权重加和后得到百分制的执行体网络服务质量得分,具体权重由实际应用的具体网络类型决定;由于不同执行体所使用的软硬件条件不同,网络管理人员根据实际应用需求和其主观经验,对不同执行体设置百分制的人为优先分数;将这三个方面的得分按照权重加和得到评价执行体初始性能的指标S_per,具体权重由实际应用的具体网络类型决定。

[0100] 用评价指标S_feedback反映由输出裁决器反馈的执行体实际安全性能,包含了正负两个方面的反馈:如果一个执行体的输出结果与输出裁决器所得到的输出结果一致,则反馈一个正值分数进行奖励,表明该执行体在现阶段能够正常工作,该正值分数是固定的;反之如果输出结果不一致,则反馈一个负值分数进行惩罚,表明该执行体在现阶段存在被攻击的风险,该负值分数为前文所述正值分数的2^t倍,t代表该执行体的输出结果与输出裁决器所得到的输出结果不一致的历史累计次数;评价指标S_feedback在每一个执行体加入资源池时初始化为0,此后的评价指标S_feedback为累计的,直到该执行体被清洗出资源池。

[0101] 如表1所示,对每一个执行体依据S_per和S_feedback权重加和,从而得到执行体的各自实际性能得分S_A,加和所用权重是会依据具体网络要求变化的,执行体实际安全性能S_feedback的权重会随着网络调度次数的增加而增大,这种方法的目的在于随着网络调度次数的增加,执行体调度时更加注重输出裁决器反映的执行体实际安全性能;此外,当一个执行体的实际性能得分S_A低于资源池初始化时网络管理人员设定的阈值时,该执行体因实际性能不足而被清洗出执行体资源池。

[0102] 表1:对每一个执行体得到执行体的实际性能得分S_A

[0103]

执行体序号	S_per(w_1%)	S_feedback(1-w_1%)	S_A
1	S_per_1	$S\_feedback_1$	S_A_1
2	S_per_2	$S\_feedback_2$	S_A_2
3	S_per_3	$S\_feedback_3$	S_A_3
4	S_per_4	$S\_feedback_4$	S_A_4
m	S_per_m	$S\_feedback_m$	S_A_m

[0104] S302:第二阶段,在各层中,分别以资源池中每一个执行体为种子执行体得到其各自兼顾性能与适配性的执行体集合,从而得到执行体集合评估分数S_C;具体过程是首先选定种子执行体,之后计算其余执行体和种子执行体之间的异构性指标S_H,再将其余执行体的实际性能得分S_A和异构性评估S_H权重加和得到适配性得分S_B,如表2所示,选择适配性得分S_B排名前(n-1)的执行体,将其与种子执行体共同组成执行体集合,并将执行体集合中种子执行体的实际性能得分S_A与其余执行体的适配性得分S_B进行直接加和,从而得到执行体集合分数S_C,其中n表示拟态网络中执行体集合冗余度。

[0105] 用评价指标S_H反映不同执行体间的异构性,S_H包含两方面内容:利用网上公开的通用漏洞列表,对各个执行体的相同或相近网络漏洞数量进行评估,并给出执行体之间的共生漏洞检测分数;利用拟态防御中关于异构性的证明计算,评估组成不同执行体的各个构件之间的软硬件差异,并给出执行体之间差异性分数;将两方面分数按照权重加和得到S_H,具体权重由实际应用的具体网络类型决定。

[0106] 用评价指标S_B反映其余执行体分别对于种子执行体的兼顾性能的适配性,具体过程为:先确定种子执行体,之后计算其余执行体和种子执行体之间的异构性指标S_H,再将其余执行体的实际性能得分S_A和异构性得分S_H权重加和得到基于性能的适配性得分S_B,具体权重由实际应用的具体网络类型决定。

[0107] 当一个执行体的S_H低于网络管理人员设定的阈值时,该执行体因与种子执行体的异构性指标不满足实际适配要求,其适配性得分S_B设定为0。

[0108] 选定种子执行体的前提下,从其余执行体中选择适配性得分S_B排名前(n-1)的执行体,将其与种子执行体共同组成执行体集合,并将种子执行体的实际性能得分S_A与该执行体集合其余执行体的各自适配性得分S_B进行直接加和,从而得到该执行体集合分数S_C,其中n表示拟态网络中执行体集合冗余度。

[0109] 采用遍历的方法分别以每一个执行体作为种子执行体,得到m个执行体集合以及对应的执行体集合分数S_C,S_C越高表示该集合越适合当前时刻进行调度,其中m为执行体资源池中执行体个数。

[0110] 表2:分别得到与第i个执行体最适配的执行体集合(i＝1,2……m)

[0111]

执行体序号	S_A(w_2%)	S_H(1-w_2%)	S_B
1	S_A_1	S_H_1	S_B_1
2	S_A_2	S_H_2	S_B_2
i-1	S_A_{i-1}	S_H_{i-1}	S_B_{i-1}
i+1	S_A_{i+1}	S_H_{i+1}	S_B_{i+1}
m	S_Am	S_Hm	S_B_m

[0112] S303:第三阶段,从第二阶段S302得到的各个执行体集合性能评估S_C前三中,随机选择一种执行体集合进行调度,如表3所示。

[0113] 表3

[0114]

执行体集合分数	S_C前三	调度执行体集合
S_C_1,S_C_2,S_C_3,S_C_4,S_C_m	S_C_a,S_C_3,S_C_γ	S_C前三随机选择

[0115] 如图4所示,本发明实施例提供的一种具有拟态层间协同防御功能的多层拟态系统,该系统结构包括:

[0116] 输入S401:拟态网络的输入数据;

[0117] 边界S402:拟态网络结构内部与外界网络的网络边界;

[0118] 分发器S403:将输入拟态网络的数据复制分发到各个上线工作的路由器中;

[0119] 调度控制器S404:动态调度的核心构件,负责对各拟态层的冗余执行体进行调度与管理,接收各拟态层输出裁决器的反馈信息,给网络管理人员提供人机交互接口;

[0120] 资源管理器S405:管理各个拟态层中所有执行体的状态信息和资源信息,状态信息包括初始化,上线,休眠,清洗,资源信息包括软硬件配置信息,存储空间容量,上线时长,

创建时间;在调度控制器进行调度前向其提供执行体的详细信息,在调度控制器发出调度指令后同步更改执行体状态信息;

[0121] 加密路由器资源池S406:资源池用于储存各个冗余异构的路由器;

[0122] 调度线S407:单向传递调度控制器S404对加密路由器资源池S406的调度管理信息;

[0123] 上线路由器执行体集合S408:是一个逻辑上的集合,由同时上线工作的路由器组成,路由器作为第一层拟态防御,是网络信息的交互中心,通过生成拟态的路由表,从信息源头上给整个网络提供一个初步的安全基础,同时为方便表示,本结构示意图中有3个同时上线工作的且相互异构的路由器;

[0124] 路由器1S409,路由器2S410,路由器3S411:同时上线工作的路由器执行体;

[0125] 拟态路由器层输出裁决器S412:将上线路由器执行体集合S408中各个执行体的输出结果进行多模裁决,得到一个拟态路由器层的最终输出;

[0126] 拟态路由器层反馈线S413:将拟态路由器层输出裁决器S412的输出与上线路由器执行体集合S408中各个执行体的输出结果进行比对,并将结果单向反馈至调度控制器S404;

[0127] 动态IP地址S414:设置为定时跳变IP;

[0128] 分发器S415:将经过拟态路由器层后,输入拟态防火墙层的外部数据复制分发到各个上线工作的防火墙中;

[0129] 加密防火墙资源池S416:资源池用于储存各个冗余异构的防火墙;

[0130] 调度线S417:单向传递调度控制器S404对加密防火墙资源池S416的调度管理信息;

[0131] 上线防火墙执行体集合S418:是一个逻辑上的集合,由同时上线工作的防火墙组成,防火墙作为第二层拟态防御,依照网络管理人员制定的网络安全规则,允许或是限制传输的数据通过,同时为方便表示,本结构示意图中有3个同时上线工作的且相互异构的防火墙;

[0132] 防火墙1S419,防火墙2S420,防火墙3S421:同时上线工作的防火墙执行体;

[0133] 拟态防火墙层输出裁决器S422:将上线防火墙执行体集合S418中各个执行体的输出结果进行多模裁决,得到一个拟态防火墙层的最终输出;

[0134] 拟态防火墙层反馈线S423:将拟态防火墙层输出裁决器S422的输出与上线防火墙执行体集合S418中各个执行体的输出结果进行比对,并将结果单向反馈至调度控制器S404;

[0135] 分发器S424:将输入拟态核心设备层的数据复制分发到各个上线工作的核心设备中,此处核心设备指拟态系统所要防护的关键高价值目标;

[0136] 加密核心设备资源池S425:资源池用于储存各个冗余异构的网络核心设备;

[0137] 调度线S426:单向传递调度控制器S404对加密核心设备资源池S425的调度管理信息;

[0138] 上线核心设备执行体集合S427:是一个逻辑上的集合,由同时上线工作的核心设备组成,网络核心设备作为第三层拟态防御,是整个拟态网络的最终防御目标,具有很高的价值,比如可以是核心路由器,核心服务器,同时为方便表示,本结构示意图中有3个同时上

线工作的且相互异构的网络核心设备；

[0139] 核心设备1S428，核心设备2S429，核心设备3S430：同时上线工作的网络核心设备执行体；

[0140] 拟态核心设备层输出裁决器S431：将上线核心设备执行体集合S427中各个执行体的输出结果进行多模裁决，得到一个拟态核心设备层的最终输出；

[0141] 拟态核心设备层反馈线S432：将拟态核心设备层输出裁决器S431的输出与上线核心设备执行体集合S427中各个执行体的输出结果进行比对，并将结果单向反馈至调度控制器S404；

[0142] 输出S433：输入S401经过拟态网络到达网络拟态核心设备层后，最终由拟态核心设备层所产生的安全网络数据。

[0143] 如图5所示，本发明实施例提供的一种优化种子调度算法中涉及的反馈方法流程，包括下列步骤：

[0144] 步骤S501：在输出裁决器进行裁决输出之后，依顺序选择一个在线执行体i，并比较其输出是否与输出裁决器的输出一致，若一致转到步骤S502，否则转到步骤S503；

[0145] 步骤S502：反馈一个正值分数进行奖励，该正值分数是固定的，将该奖励分数与该执行体的S_feedback分数进行累计加和；

[0146] 步骤S503：反馈一个负值分数进行惩罚，该负值分数为前文所述正值分数的2^t倍，t代表该执行体的输出结果与输出裁决器所得到的输出结果不一致的历史累计次数，将该惩罚分数与该执行体的S_feedback分数进行累计加和；

[0147] 步骤S504：若所有在线执行体均完成了反馈，则结束本流程，否则转到步骤S501。

[0148] 综上所述，本发明实施例分阶段对执行体做出调度评估，第一阶段先评估每一个执行体的各自实际性能，第二阶段再得到每一个执行体各自最适配的执行体集合，第三阶段选出较优的执行体集合进行调度；具体地，就是通过S_per，S_feedback，S_H，S_A，S_B，S_C这六个指标分别对资源池中各个执行体的由实际测试和人为经验判定的初始性能，实际执行安全反馈，执行体间异构性，实际综合性能，与种子执行体的适配性能，执行体集合整体性能做出了量化评估；在量化评估的基础上可以有效选出当前调度时刻最适合的三个执行体集合，并在其中随机选择一种进行调度，使得调度方法兼备完善性，可更新性和随机性，表现出更好的性能；另外提出一种整合多个拟态层以及在此基础上实现协同防御的系统化拟态防御网络，从而有效抵御高级持续威胁所带来的协同控制攻击。

[0149] 如图3所示，本发明实施例还提供了一种多层拟态防御装置，包括：

[0150] 至少一个处理器301；

[0151] 至少一个存储器302，用于存储至302少一个程序；

[0152] 当至少一个程序被至少一个处理器301执行，使得至少一个处理器301实现上述方法。

[0153] 本实施例的一种多层拟态防御装置，可执行本发明实施例所提供的方法，可执行方法实施例的任意组合实施步骤，具备该方法相应的功能和有益效果。

[0154] 本发明实施例还提供了一种存储介质，其中存储有处理器可执行的指令，处理器可执行的指令在由处理器执行时用于执行如上所述方法。

[0155] 本实施例的一种存储介质，可执行本发明实施例所提供的方法，可执行方法实施

例的任意组合实施步骤，具备该方法相应的功能和有益效果。

[0156] 可以理解的是，上文中所公开方法中的全部或某些步骤、系统可以被实施为软件、固件、硬件及其适当的组合。某些物理组件或所有物理组件可以被实施为由处理器，如中央处理器、数字信号处理器或微处理器执行的软件，或者被实施为硬件，或者被实施为集成电路，如专用集成电路。这样的软件可以分布在计算机可读介质上，计算机可读介质可以包括计算机存储介质(或非暂时性介质)和通信介质(或暂时性介质)。如本领域普通技术人员公知的，术语计算机存储介质包括在用于存储信息(诸如计算机可读指令、数据结构、程序模块或其他数据)的任何方法或技术中实施的易失性和非易失性、可移除和不可移除介质。计算机存储介质包括但不限于RAM、ROM、EEPROM、闪存或其他存储器技术、CD-ROM、数字多功能盘(DVD)或其他光盘存储、磁盒、磁带、磁盘存储或其他磁存储装置、或者可以用于存储期望的信息并且可以被计算机访问的任何其他的介质。此外，本领域普通技术人员公知的是，通信介质通常包含计算机可读指令、数据结构、程序模块或者诸如载波或其他传输机制之类的调制数据信号中的其他数据，并且可包括任何信息递送介质。

[0157] 上面结合附图对本发明实施例作了详细说明，但是本发明不限于上述实施例，在所述技术领域普通技术人员所具备的知识范围内，还可以在不脱离本发明宗旨的前提下作出各种变化。

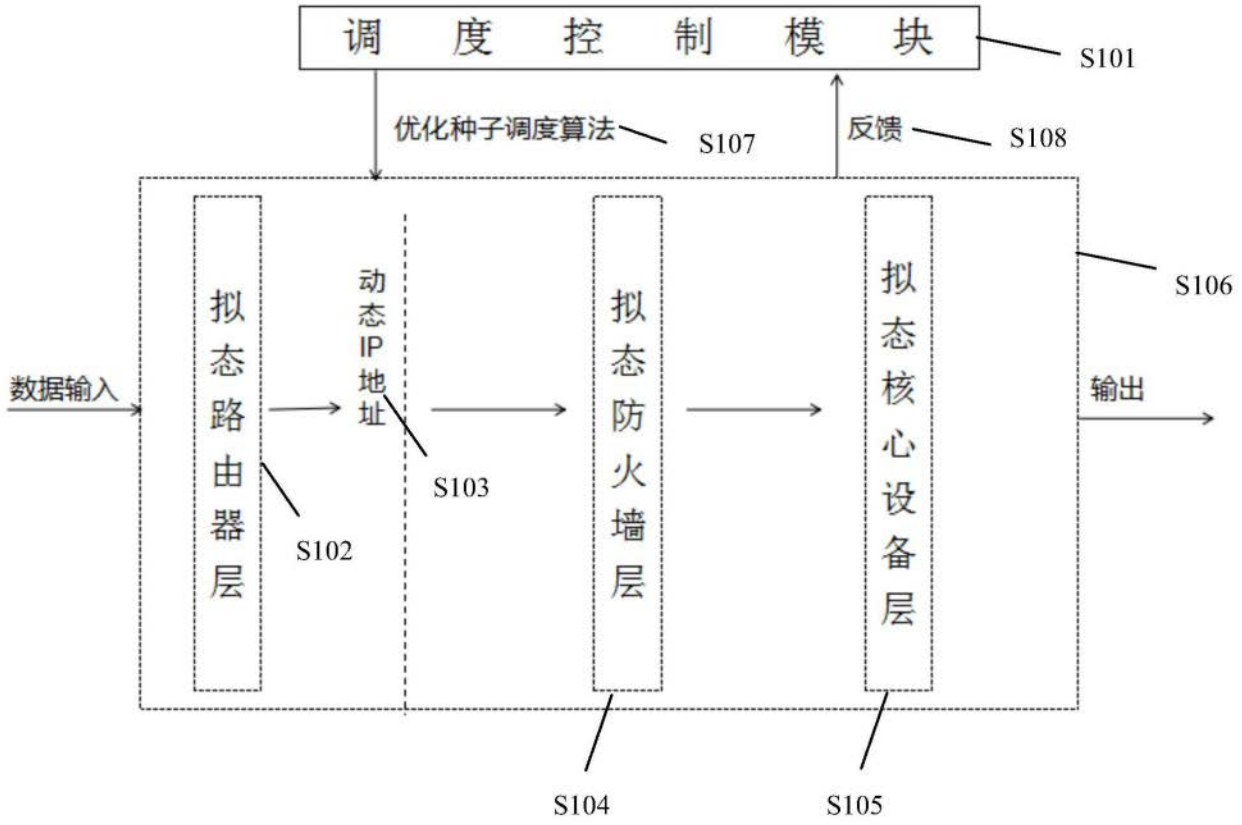

调 度 控 制 模 块
S101
优化种子调度算法
S107
反馈
S108
拟态路由器层
动态IP地址
拟态防火墙层
拟态核心设备层
S106
数据输入
输出
S102
S103
S104
S105

图1

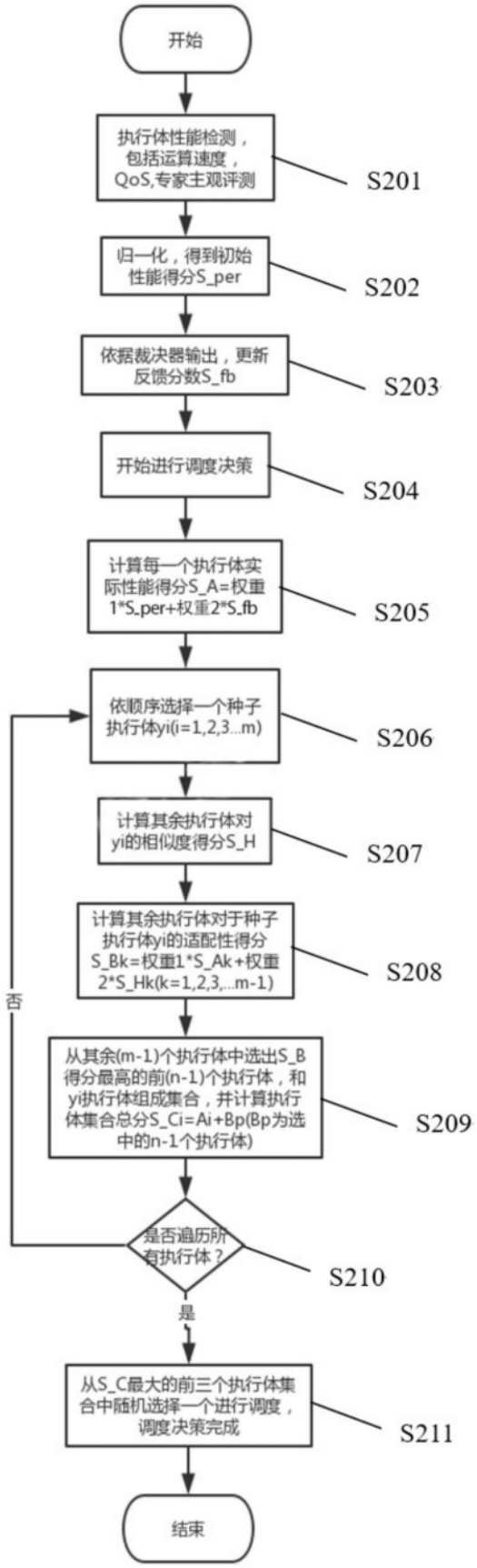

开始
执行体性能检测，包括运算速度，QoS,专家主观评测
S201
归一化，得到初始性能得分S_per
S202
依据裁决器输出，更新反馈分数S_fb
S203
开始进行调度决策
S204
计算每一个执行体实际性能得分S_A=权重1*S_per+权重2*S_fb
S205
依顺序选择一个种子执行体yi(i=1,2,3...m)
S206
计算其余执行体对yi的相似度得分S_H
S207
计算其余执行体对于种子执行体yi的适配性得分S_Bk=权重1*S_Ak+权重2*S_Hk(k=1,2,3,...m-1)
S208
否
从其余(m-1)个执行体中选出S_B得分最高的前(n-1)个执行体，和yi执行体组成集合，并计算执行体集合总分S_Ci=Ai+Bp(Bp为选中的n-1个执行体)
S209
是否遍历所有执行体？
S210
是
从S_C最大的前三个执行体集合中随机选择一个进行调度，调度决策完成
S211
结束

图2

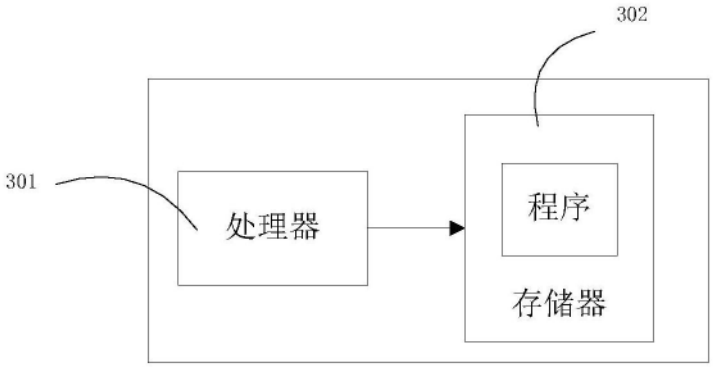

302
301
处理器
程序
存储器

图3

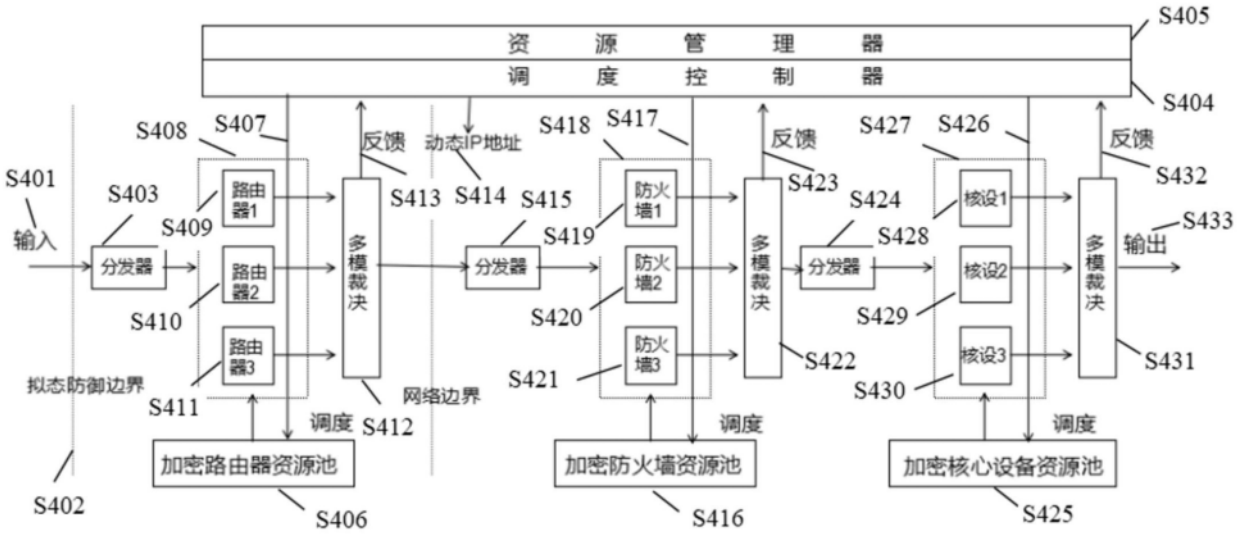

资 源 管 理 器
调 度 控 制 器
S405
S404
S401
输入
S402
拟态防御边界
S403
分发器
S407
S408
路由器1
路由器2
路由器3
S409
S410
S411
调度
加密路由器资源池
S406
反馈
S412
网络边界
S413
动态IP地址
S414
多模裁决
S415
分发器
S417
S418
防火墙1
防火墙2
防火墙3
S419
S420
S421
调度
加密防火墙资源池
S416
反馈
S423
多模裁决
S422
S424
分发器
S426
S427
核设1
核设2
核设3
S428
S429
S430
调度
加密核心设备资源池
S425
反馈
S432
多模裁决
S431
输出
S433

图4

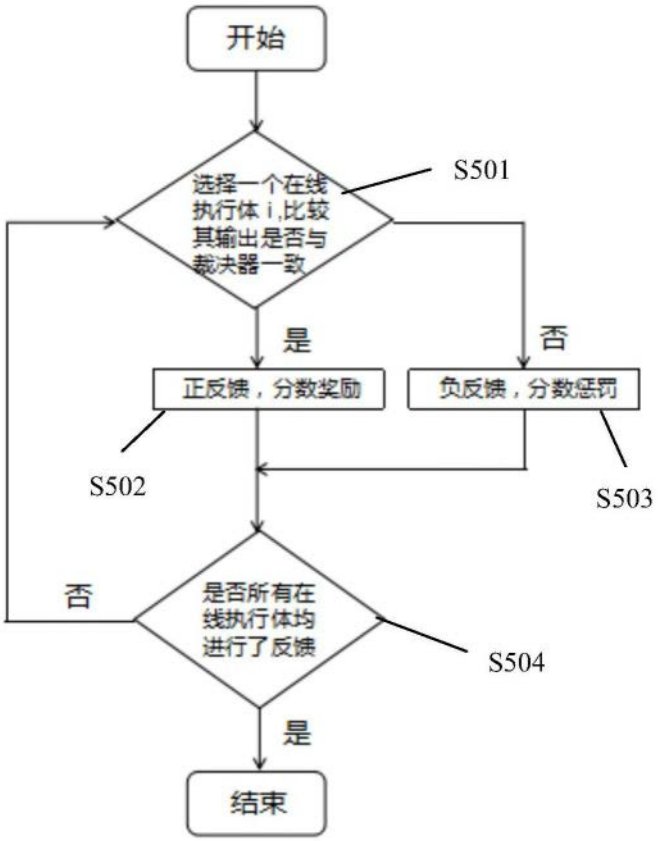

开始
选择一个在线执行体 i,比较其输出是否与裁决器一致
S501
是
否
正反馈，分数奖励
负反馈，分数惩罚
S502
S503
否
是否所有在线执行体均进行了反馈
S504
是
结束

图5