

基于序参量的云边端分布式体系协同安全评估

范其纲, 蒋忠元, 李兴华, 马建峰

(西安电子科技大学网络与信息安全学院, 陕西 西安 710126)

摘要: 基于云边端的分布式计算体系成功服务于众多应用, 已经成为一种主流, 具有受众广、用户体验好、安全期望高等特点。然而, 近年来针对云、边、端的攻击事件频发, 给用户造成严重的安全隐患与巨大经济损失。当前云、边、端的防御机制各自为战, 抵御风险的能力差异大, 全域安全风险消除难。事前配置和事后“亡羊补牢”式的安全手段难以满足高负载、高实时的云边端协同网络的安全需求。其根源在于云、边、端分层架构各自为营, 未形成有效的协同防御体系, 导致产生跨域安全治理难度大、实时性差、协同一致性评估难等问题。提出了实时感知、动态决策、积极防御三位一体的云边端协同安全架构, 深度融合云、边、端, 形成安全协同能力, 并进行严格理论一致性证明; 提出了基于序参量的协同安全评估模型, 实现云、边、端风险感知一致, 策略决策一致, 攻击防御一致, 实行高效率、低成本的安全风险协同防护, 最大化系统性安全收益; 对一致性理论与评估模型进行仿真验证, 结果证明了提出的协同安全体系以及一致性评价模型的正确性与有效性。

关键词: 云边端; 协同一致性; 安全评估; 序参量

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2024038

Collaborative security assessment of cloud-edge-device distributed systems based on order parameters

FAN Qigang, JIANG Zhongyuan, LI Xinghua, MA Jianfeng

School of Cyber Engineering, Xidian University, Xi'an 710126, China

Abstract: Distributed computing systems based on cloud-edge-device have been successfully serving thousands of applications and have become mainstream, characterized by a wide audience, high user experience requirements, and high security expectations. However, in recent years, frequent attacks on cloud-edge-device systems have resulted in serious security risks and significant economic losses for users. The defense mechanisms of cloud-edge-device systems have been found to operate independently, leading to major differences in the ability to resist risks, which makes it

收稿日期: 2023-12-11; 修回日期: 2024-04-08

通信作者: 蒋忠元, zyjiang@xidian.edu.cn

基金项目: 陕西省重点研发项目 (2023-YBGY-270)

Foundation Item: The Key Research and Development Program of Shaanxi (2023-YBGY-270)

引用格式: 范其纲, 蒋忠元, 李兴华, 等. 基于序参量的云边端分布式体系协同安全评估[J]. 网络与信息安全学报, 2024, 10(3): 38-51.

Citation Format: FAN Q G, JIANG Z Y, LI X H, et al. Collaborative security assessment of cloud-edge-device distributed systems based on order parameters[J]. Chinese Journal of Network and Information Security, 2024, 10(3): 38-51.

difficult to eliminate global security risks. Security measures of the pre-configuration and post-event remedy type have been found to hardly meet the security needs of high-load and high real-time in cloud-edge-device collaborative networks. The root cause has been identified as the hierarchical architecture of cloud-edge-device systems being separate, and no effective collaborative defense system has been formed, leading to problems such as difficult cross-domain security governance, poor real-time performance, and difficult collaborative consistency evaluation. Firstly, a cloud-edge-device collaborative security architecture that integrates real-time perception, dynamic decision, and proactive defense was proposed. The cloud-edge-device security collaboration capability was established through rigorous theoretical consistency proofs. Secondly, a collaborative security assessment model based on the order parameter was put forward to achieve consistency of risk perception, decision, and defense. In this way, the efficient and low-cost collaborative protection of security risks could be realized to maximize systemic security benefits. Finally, the consistency theory and assessment method were verified through simulations. The results show that the proposed collaborative security system and consistency evaluation model are correct and effective.

Keywords: cloud-edge-device, collaborative consistency, security assessment, order parameter

0 引言

在《中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要》（“十四五”规划）中，国家将云计算作为发展的重要方向予以支持。云计算作为资源调度的方法，用户能够按需访问计算资源，如服务、存储或应用程序，是物联网、工业互联网等技术发展的重要支撑，已经成为数字化领域赖以发展的引擎，也是国家信息化发展水平的重要印证。随着网络安全形势愈发严峻，新型安全威胁层出不穷，进一步加大了云计算基础平台的风险，相关部门高度重视，出台了一系列政策、制度、标准，如GB/T 31167《云计算服务安全指南》、GB/T 31168《云计算服务安全能力要求》等。在数字化转型中，尤其是多终端、多任务的复杂应用场景下，云边端协同网络作为云计算和边缘计算的融合延伸^[1]，其协同安全对于传统的评估模式极具挑战性，重要程度不言而喻。

目前云、边、端体系在安全服务、风险化解方面分层防护、孤立作战，只考虑各自层面的个性安全问题，对于协同安全理论的研究不够充分，缺少对共性协同安全问题的思考。而且云、边、端三者资源配置不平衡、时空差异大、服务质量要求各异，导致设备的安全防护能力不同，很难通过统一的安全方案来满足各类服务的安全需求和进行安全评估^[2-4]。最后，鉴于不同计算防护系统安全生态的异质性，云边端协同网络所面临的主要安全风险和威胁挑战复杂多变^[5]，加上

不同层面设备防护的侧重点不同，仅依靠节点自身的防护能力，不能形成有效的云、边、端协同防御体系，难以消除云边端全域风险。

针对云边端协同安全困境，本文提出多维可定义的协同安全架构，准确量化云边端协同网络中的安全风险，协助跨域安全管理。其中，协同是该架构中节点共同防御的关键，而一致性是协同安全的核心指标。为了使协同安全的一致性贯穿安全评估的始终，引入协同理论序参量，以云服务商安全管理能力及云平台安全防护情况为切入点，分析中间人攻击、数据注入、权限和访问控制等安全问题，借助分布式多要素协同控制理论和建模方法，构建多角度、多层次的云边端协同网络的安全评估效能模型，正确评估云服务生命周期内攻防对抗的演化过程，主要贡献如下。

1) 针对协同安全理论缺乏的问题，提出一种安全风险感知、动态决策、积极防御三位一体的协同安全理论架构。

2) 针对协同安全效能评估难的问题，提出基于序参量的协同安全态势一致性评价体系并进行数学化证明，实时量化安全效能，实现动态响应与反馈优化。

3) 针对协同安全实验验证难的问题，进行了大量仿真验证与分析，说明模型的有效性和正确性。

1 相关工作

云计算的基础设施可以按照业务场景、时延、成本等需求进行灵活部署。但是限制用户使

用的关键问题是对隐私安全的担忧,不仅是云服务提供者 (cloud service provider, CSP) 的安全风险,还包括云客户端 (cloud client, CC) 自身的安全风险。因此全面、科学、定量的安全评估框架可以使用户对服务商的安全防护有更正确的认识。

传统的安全风险评估已经不适用于云计算自动化风险评估^[6],文献[7]设计了迭代和增量的评估云计算风险的方法,包括静态和动态两个维度的评估,并基于模糊多准则决策技术,利用计算安全系数进行云计算中的风险量化。然而该方法缺少对CC安全风险的评价。在云自适应安全评估模型^[8] (cloud adoption risk assessment model, CARAM) 中,通过选择特定CSP,帮助用户评估他们面临的危险。该模型的主要目标是进一步涵盖风险情景,并在威胁发生变化时进行安全保护。并且CARAM为每个CC-CSP对实现了风险评估,缺陷是需要安全专家来定义每个场景安全风险发生的可能性,因此不是通用的风险评估方案。文献[9]建立了可扩展的基于博弈论的安全风险评估模型来评估网络是否需要修复。针对边缘计算的使用场景,文献[10]基于动态博弈理论的纳什均衡矩阵,构建了边缘计算容器安全风险评估方法。根据边缘计算中容器存储、计算和资源有限的特点,分析容器在镜像攻击和内部攻击情况下的防御过程中,构建边缘计算容器风险评估动态博弈模型。

上述模型都是基于单一视角进行评估,覆盖面窄、局限性大,简单使用单个节点的安全性,反映整体服务的安全状况,缺少对全域网络安全态势的整合研究,风险攻击级联的分析能力薄弱。然而,在协同网络安全攻防对抗中,从无序到有序的演化过程是必不可少的,并且自治协同能力作为云边端协同网络的优势,强调设备节点间的能力互补、协同防御,这点在传统的评估生命周期内也无法体现。因此新的云边端协同安全效能模型,必须能够实现节点领域间或全局协同联动的安全效能评估防护。

2 基于序参量的云边端协同安全架构

局限于评估单一风险点所得到的安全数据互

为“孤岛”,容易忽视对协同防护中风险传播的建模,导致在分布式系统中的风险响应不及时。此时,能够评估和引导网络协同安全表现的指标至关重要。

2.1 云边端协同安全架构

协同安全评估涵盖了基本的应用、网络、设备安全等,贯穿了云边端协同网络的计算协同、数据协同和安全协同。将安全要素信息定义为网络节点正常运行的必要因素,通常包括通信、计算、监听、决策、防御等。

这些要素分布于不同层次的计算节点或系统架构中,云边端协同安全架构如图1所示,总结划分为3类安全要素:感知、决策、防御。从横向上看,同域内各安全要素需要在网络风险威胁中维持态势信息的一致性,从感知风险,到决策风险,再到部署防御措施,完成安全评估的整体流程。从纵向上看,同类安全要素跨域关联交互形成态势垂直的一致性。

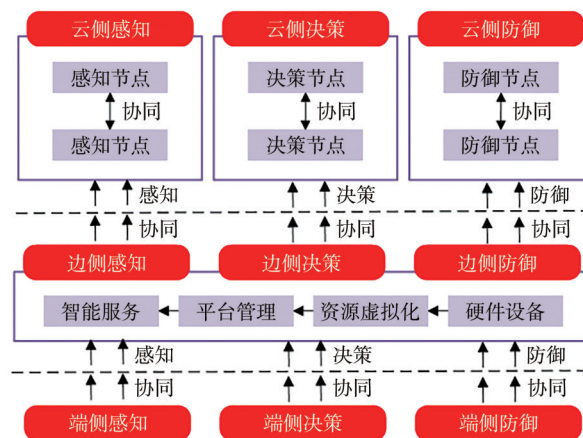


图1 云边端协同安全架构
Figure 1 Collaborative security architecture for cloud-edge-device

(1) 网络安全态势的感知

感知的关键是异构网络中海量数据的挖掘与融合,根据经典的态势感知模型,分为态势要素提取、态势理解和态势预测3个阶段^[11]。在云边端协同网络中为了实现安全态势的实时采集、融合和处理,并确保评估模型和决策要素的准确性,需要对各个层次的通信设备及终端设备的态势感知信息进行域内融合,跨域关联等处理,从而实现获取当前网络安全状态的目的。例如,网络正遭受何种攻击,攻击的影

响范围涉及多少个层次、多少个节点态势信息如何推送。

(2) 决策要素的响应

现有静态的入侵响应决策，多数是基于攻击威胁和对策成本最小化进行自动响应^[12]。在云边端协同网络中，静态响应的方法，容易忽视跨域设备间的关联性和对服务质量的影响，使决策节点选择错误的对策或者部署到错误的位置，甚至中断用户的服务进程，同时防御资源利用率低。为了适应协同网络的复杂性和不确定性，决策要素应以防御能力最大化、服务影响最小化等多目标优化为理念，构建动态入侵响应框架^[13]，实时跟踪网络环境配置的变化，整合关联的决策态势信息，制定分布式联合决策。

(3) 防御要素的反馈机制

其为服务可持续性和自治的重要组成部分。考虑协同网络的健壮性和可靠性，在其遭受攻击时，服务应在可接受的时间范围内迅速恢复可用性。要求防御要素对系统的功能性指标进行实时监控，在发现下降后及时向决策中心进行反馈，自适应优化，保证业务的持续平稳运行。

云边端协同网络通常由上百个云数据中心、上万个边缘计算节点和海量的终端设备组成。借助图的性质，来反映真实的协同网络安全状况。根据要素的划分标准，将云边端协同网络抽象成“感知—决策—防御”三网合一的立体拓扑网络。

一张无向图可以表示为 $G = (V, E)$ ，其中一组节点可以表示为 $V = \{1, 2, 3, \dots, n\}$ ，边的集合则表示为 $E \subseteq V \times V$ 。使用 $A = [a_{ij}]$ 表示为图 G 的邻接矩阵，其中 $a_{ij} = 1$ 表示为节点 i 和节点 j 相连，反之当 $a_{ij} = 0$ 时，表示为节点 i 和节点 j 没有连接。将 $L(G) = D - A$ 定义为图的拉普拉斯矩阵。其中 $D = \text{diag}(d_1, \dots, d_n)$ 是对角矩阵，节点 i 的出度表示为 $d_i = \sum_{j=1}^n a_{ij}$ 。 $\{s, c, p\}$ 定义为节点属性的安全态势信息，分别代表为感知、决策和防御态势信息。此关系可以描述成式 (1)。

$$\begin{cases} \dot{s}(t) = f_s(s, y_c) + u_s, & y_s = h_s(s) \\ \dot{c}(t) = f_c(c, y_s, y_p) + u_c, & y_c = h_c(c) \\ \dot{p}(t) = f_p(p, y_c) + u_p, & y_p = h_p(p) \end{cases} \quad (1)$$

其中， u_s, u_c, u_p 分别代表感知、决策、防御要素的控制输入， y_s, y_c, y_p 分别代表感知、决策、防御要素的结果输出， $f_s(s, y_c)$ 表示感知态势信息和决策结果对感知状态变化率 $\dot{s}(t)$ 的影响， $f_c(c, y_s, y_p)$ 表示决策态势信息和感知、防御结果对决策状态变化率 $\dot{c}(t)$ 的影响， $f_p(p, y_c)$ 表示防御态势信息和决策结果对防御状态变化率 $\dot{p}(t)$ 的影响。只有当时间 t 到达某一时刻后， $t \rightarrow \Delta t, y_i - y_j \rightarrow 0$ ，称节点 i 和节点 j 的态势信息一致。

2.2 协同安全一致关系

在云边端协同安全理论架构中，3类安全要素在时间层面上保持行动的有序一致，并且在态势信息层面各个要素间的结果输出一致，形成有效的协同防御网络。

首先，时间的一致性以服务或计算任务为载体，将感知、决策和风险细化，以服务运行生命周期为风险评估的时间轴，进行实时监控、量化风险、动态调整。时间一致性关系如图2所示，从态势的自感知到决策中心的策略裁决，两者的响应间隔取决于一致性时延的长短。这意味着“感知—决策—防御”要素之间的信息同步是协同防护的关键。

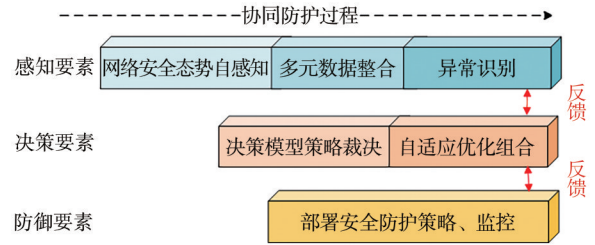


图2 时间一致性关系
Figure 2 Time consistency relationships

其次，态势的一致性，根据云边端协同网络的分布式系统架构可知，任务不再局限运行于单一的中心云资源，而是以云为中心，向边缘设备和用户边界进行拓展和延伸。为了实现最终全局协同安全的状态，三者相互协作，在整个服务运行的生命周期内，中心云、边缘设备、终端设备这3类的安全态势信息必须始终一致，即感知要素与感知要素间、决策要素与决策要素间、防御要素与防御要素间保持一致稳定的安全工作状态。

2.3 协同安全一致性挑战

纵向来看, 在云侧由于基础设施的不同, 易受到高级别持续性威胁 (advanced persistent threat, APT) 和拒绝服务 (denial of service, DoS) 攻击。边侧在位置上更靠近用户, 但存储和计算资源受限, 安全部署能力较弱, 会面临数据注入、分布式拒绝服务攻击等安全风险, 端侧则会面临钓鱼攻击、窃听、中间人攻击等安全风险。在业务中, 云边端协同网络统一调度各种计算资源, 使用户隐私信息数据与协同网络深度绑定。一旦在任意一个层面受到攻击或数据泄露, 都会直接造成用户损失, 给企业运营带来恶劣的影响。云边端安全挑战如图3所示, 攻击者在某一时刻对云、边、端3个层面同时发起 APT、DoS 等攻击。感知的一致性要求各设备对环境中的风险数量和类型有准确的评估, 意味着图3中的设备都应该能检测网络环境中存在的 DoS 攻击或其他攻击。但是, 仅凭一个终端或边缘平台的软硬件资源, 感知能力有限, 难以部署复杂的感知算法来检测所有的攻击。

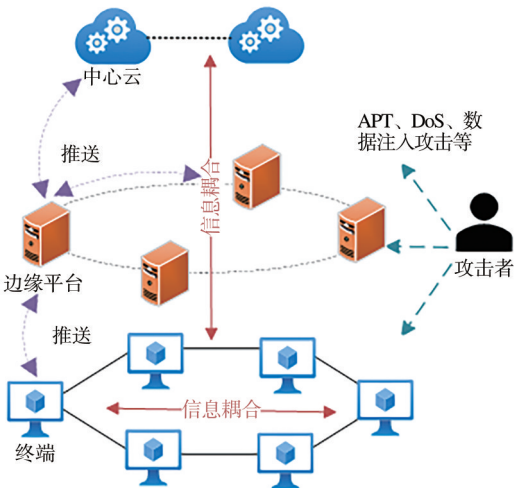


图3 云边端安全挑战
Figure 3 Cloud-edge-device security challenges

为了解决该问题, 需要最大化地聚合整个网络的感知能力, 核心思想是协同感知。令边缘平台或其他设备在感知到确切的风险类型时, 将感知态势信息向跨域的中心云、终端和同域的边缘平台推送。被攻击的设备再通过对收到的信息进行解析耦合, 与自身的感知态势信息对照, 查缺补漏, 最大程度地了解网络环境范围内存在的风险

威胁。例如, 中心云检测到了 DoS 攻击, 但是边缘平台由于检测能力或攻击者还未实施攻击等原因, 未能检测到 DoS 攻击。此时中心云就可以将该攻击的信息向边缘平台推送, 进行补充或预警, 做好事前防护, 这是协同感知一致性的额外体现。然而, 在推送和信息耦合的过程中, 还可能存在中间人攻击、丢失、篡改、误报等问题。确认推送信息流收发的一致性就显得尤为必要, 也是实现后续协同决策、防御机制的基础。

决策的一致性与感知息息相关。分布式协同决策如图4所示, 以边缘平台为攻击目标, 由于设备自身的防御资源有限, 入侵响应覆盖的攻击种类范围小, 容易出现疏漏, 并且不是所有的设备都有余力部署决策算法。面对该问题, 考虑由部分计算资源丰富的设备兼任决策中心, 负责在本地对策库缺少对应防御措施时, 关联其邻居或备用设备的防御资源, 考虑服务迁移和防御资源调度的可能性, 做到风险与策略裁决一一对应。然而在针对同一个攻击目标时, 不同的决策中心所链接的攻击目标的邻居节点不同, 导致获取的感知信息不同, 进一步影响了决策信息的差异。

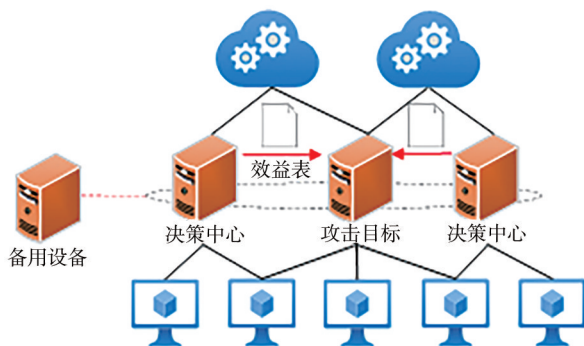


图4 分布式协同决策
Figure 4 Distributed collaborative decision making

在有能力决策的基础上, 面对分布式协同决策的多结果, 决策一致性额外还体现为安全效益的最优选择。对于 DoS 攻击来说, 在获取上一阶段的感知信息后, 不同的决策中心对可执行的防御决策计算出安全效益表, 其中一个决策中心的效益表可能包含服务迁移等决策, 另一个决策中心可能包含过滤等决策。在多个决策下, 最终仍要回归到攻击目标自身的视角, 进行最优解的选择。若运行的服务要求不能中断, 则偏向于过滤

优先，否则迁移也是待选的方法，确保每一个决策的安全能力符合全局业务需求，是协同决策的重点。

最后的防御一致性是安全管理的最终阶段，在防御措施部署的过程中，环境中的风险威胁不断变化，需要对设备进行实时监控，保证防御能力达到预期的结果，否则需要迅速定位出错的位置，动态反馈给决策中心，进行策略优化，确保网络中的所有设备在各个阶段正常运行。

2.4 协同安全一致性量化的关键：序参量

量化上述协同安全一致性的关键是依靠协同理论中的序参量。协同理论由Haken提出^[14]，该理论研究各子系统间的协调效应和开放复合系统从无序到有序的演化规律，实现系统最终的高度有序。协同理论的本质是序参量，该概念最早在金兹堡-朗道理论中提出，用于描述热力学中的相变。Haken将其概括为慢弛豫变量，在系统状态变化的过程中，衰减速度较慢，对系统的自组织起积极的作用，是引导系统产生有序结构的关键因素。

在复杂网络同步化过程中，序参量用于描述所有节点或局域网络的整体行为，是网络协同运作的集中体现^[15]。当节点的状态与节点间的耦合强度差异过大时，意味着节点未形成一致性关系，网络的行为不相干。若节点间的耦合强度足够大，节点就能够发生状态的转变，在一个时间段内锁定状态，形成协同的节点集群，这是网络协同的开始。然后在序参量的引导下，更多的节点被引入节点集群，最后网络将处于协同一致的状态。

在云边端协同网络中，安全管理的目标是使云、边、端保持安全状态的一致性。该安全状态的变化，与网络的同步化相似，不同层次的安全要素协同防御，相互作用，相互影响。借助序参量整合所有设备的安全态势信息，再基于序参量的变化，引导节点间的态势信息耦合，保证失衡设备恢复云边端协同网络的正常运行。在宏观上，这3类安全要素决定了协同网络的安全服务行为，使安全状态演化趋近于平衡的状态，形成稳定的安全架构，可以被称为序参量。

2.5 协同安全一致性理论证明

在云边端协同安全理论架构中，使用序参量

进行协同安全一致性评估的前提是态势信息耦合存在一致性关系的变化，对此进行理论证明。按照安全要素的划分，协同网络可以看作是感知网、决策网和防御网的融合，因此，节点根据云、边、端层次的不同，安全需要的不同，肩负多种不同的安全要素能力。以节点间的一致性为例，假定云边端协同网络，每个节点 i 在 t 时刻的状态模型 $x_i(t) \in R^m$ 由 m 个维度的属性组成，可以具体表示为感知态势、决策态势、防御态势等相关的特征信息，相应的拥有 n 个节点的网络态势表示为矩阵 $\mathbf{x}(t) = [x_1, x_2, \dots, x_n]^T$ ，协同网络的态势变化可以表示为：

$$\dot{\mathbf{x}}(t) = -f(t, \mathbf{x}) \quad (2)$$

其中， $f(\mathbf{x})$ 是一个齐次的向量场，且 $f(0) = 0$ 。考虑网络服务的冗余设计，为了及时填补设备受到攻击出现的节点缺失，需要额外加入备份节点，因此网络结构会随着时间改变，加入 $\sigma(t)$ 表示一个分段的连续时间函数，将网络在时间层面上分割成离散固定的网络结构。

$$\dot{\mathbf{x}}(t) = -f_\sigma(t, \mathbf{x}) \quad (3)$$

为每个节点 i 定义一致性协议 $u_i(t)$ ：

$$\dot{x}_i(t) = u_i(t) \quad (4)$$

并通过 $f(\mathbf{x})$ 描述每个相邻节点间的不一致错误累积，形成新的关系。

$$u_i(t) = f(e_i), e_i = \sum_{j \in N_i^\sigma} a_{ij}(x_j(t) - x_i(t)) \quad (5)$$

其中， N_i^σ 表示 i 节点 $\sigma(t)$ 时刻的邻居节点， e_i 表示节点 i 和节点 j 间的感知风险数量或决策效益等特征的不一致。该值越大，说明领域内的风险隐患越大，导致一致性的快速下降。当 $x_1 = \dots = x_n$ ，说明各个节点和邻居的态势认知是一致的，正确识别处理了所有风险威胁，使网络处于安全稳定的状态。将网络全局的误差表示为：

$$\mathbf{e} = [e_1, e_2, \dots, e_n]^T = -L(G_\sigma)\mathbf{x} \quad (6)$$

一致性收敛的关键是证明误差 $\mathbf{e}$ 的收敛性，在有限的时间内趋近于0。核心思想是定义一个非光滑函数 $V(\mathbf{x})$ ，考虑最大值和最小值的关系变化。

$$V(\mathbf{x}) = \max \{x_1, \dots, x_n\} - \min \{x_1, \dots, x_n\} \quad (7)$$

引理1 $V(\mathbf{x})$ 是利普希茨连续^[16]。

引理2 $V(\mathbf{x}(t))$ 在时刻 t^* 拓扑的结构发生改

变, 此时 $V(x(t))$ 不可微, 但存在一个时刻 $\varepsilon_i > 0$, 使 $V(x(t))$ 在 $\forall t \in [t^* - \varepsilon_i, t^*) \cup (t^*, t^* + \varepsilon_i]$ 是可微的^[16]。

定理 1 一个动态网络 $G_o(t)$, 其系统 $\dot{x} = -f_o(t, x)$ 的全局渐进平衡点是其原点。

证明 当 $x \notin \ker L(G) = [x: x_1 = \dots = x_n]$ 时, $V(x) > 0$ 是有界的。当 $V(x) = 0$ 时, $x \in \ker L(G)$ 。由引理 1 可知 $V(x(t))$ 连续可微, 且 $\dot{V}(x(t)) \leq 0$ 。根据引理 2 可知 $V(x(t))$ 在这些离散的时间点上是不可微的 $[t_1^*, t_2^*, \dots, t_n^*]$, 但是 $\forall t \in (t_i^*, t_{i+1}^*)$ 是连续可微的。在 $\dot{V}(x) = f(e_j) - f(e_k)$ 中, 当 $x_j = x_{\max}$, $x_k = x_{\min}$ 时, 再基于 e 的定义可得 $e_j < 0$, $e_k > 0$, 可以得到以下结果:

$$\dot{V}(x) = -(|f(e_j)| + |f(e_k)|) < 0, \forall t \in (t_i^*, t_{i+1}^*) \quad (8)$$

利用拉塞尔不变性原理^[17]可以证明渐近收敛性, 令 $E = \{x \in R^n \setminus \ker L(G) | \dot{V}(x) = 0\}$, $x(t) \in E$ 的非零子区间 (t_i^*, t_{i+1}^*) 。根据式 (8) 推导, 当 $\dot{V}(x) = 0$ 时, $f(e_j) = f(e_k) = 0$, 按照一致性协议 $x_j = x_i = 0, i \in N_j^o$ 。通过反复迭代, 只要节点 i 和节点 j 存在连通的路径, 可以得到 $x_i = x_j$ 。最后根据不变性原理, $V(x)$ 是不断递减的, 直到 $L(G_o)x = 0$, 说明网络中的节点态势信息最终认知是一致稳定的。

3 基于序参量的云边端分布式系统协同安全效能评估模型

面对各种潜在的未知风险, 以协同网络的高可用、高可靠和高可信为目标, 要求态势感知、动态决策、积极防御等要素进行协同防护。在本节, 首先基于一致性理论设计简单的协同防护方案, 形成云边端的安全态势一致性。然后以这 3 个序参量一致性评估为目标, 构建“感知—决策—防御”三位一体的序参量安全效能评估模型。对协同防护和评估过程涉及的基本符号说明见表 1。

3.1 协同安全一致性设计

根据文献[18-19], 可知协同防御的关键是节点与节点间进行通信来更新自身的安全态势信息, 从而产生有效的协同防御体系。

表 1 基本符号说明
Table 1 Basic symbol description

符号名称	符号	备注
感知态势信息	s	风险识别和节点间链路状态
决策态势信息	c	决策权重和各安全效益值
防御态势信息	p	服务正常运行的功能性指标
服务影响	K_q	服务的可用性
安全成本	K_h	防御措施占用的计算资源
防御能力	K_b	决策防御成功的概率
防御决策库	Ω	所有可选的决策方法
决策方法	cm	—
安全效益评估函数	Q	—
决策权重	w	—
安全效益阈值	Γ	判断协同决策一致性
个性态势误差函数	φ	节点自身的安全风险
共性态势误差函数	ϕ	节点间的安全风险

协同感知、决策、防御如图 5 所示。在协同感知阶段, 感知态势信息主要由数据流和攻击类型的检测组成。根据式 (5), 图中节点 1 在感知时, 遍历节点 $N_1^{o(t)}$, 判断其是否需要跨域或同域间推送。若节点 1 和节点 4 之间共同执行某计算子任务, 依赖程度高, 业务关联性强, 节点 1 就将攻击信息推送, 反过来, 节点 1 也会收到节点 4 推送的感知态势信息。然后, 基于式 (4), 解析接收到的攻击信息对节点 1 的感知态势变化率产生影响, 不断消除感知分歧。例如, 节点 1 能够借助节点 4 的感知能力补充未感知到的 DoS 攻击风险。同时, 节点 4 也能使用自身的传感器对节点 1 的感知态势信息进行纠错。

在协同网络中, 各节点间的链路状态是态势信息交互成功的关键因素。若节点 4 在向节点 1 推送信息流时, 受到干扰, 发生态势信息的偏差、丢失、延迟等, 会对协同安全评估的实时性造成影响, 甚至会严重影响协同评估结果的准确性。为了保证节点间的实时链接, 采取多径推送。当节点 1 和节点 4 的链路断开时, 可以由节点 4 到节点 3 再到节点 1 的路径推送, 这样节点 1、4 间仍被看作保持着链接。考虑风险响应的实时性, 在路径搜索时还需要将跳数控制在合理的范围内。

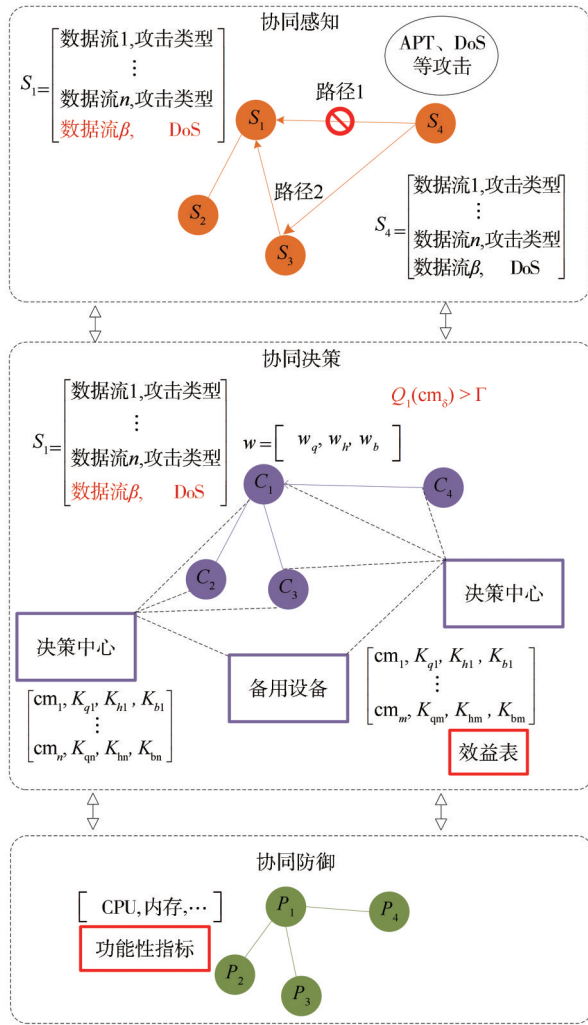


图5 协同感知、决策、防御

Figure 5 Collaborative perceptual, decision making, defense

在协同决策阶段，决策态势信息包含决策中心的安全效益值、权重矩阵 w 和可用决策 cm 。在感知态势 s_1 的基础上，针对攻击类型做出最优的防御决策 cm_s 。云、边、端中的设备关联动态变化，节点1需要遍历相连的决策中心。通过决策中心实时更新关关节点1的邻居配置信息，以服务影响最小化 K_q 、安全成本最小化 K_h 、防御能力 K_b 最大化为目标，计算各个决策的安全效益值形成安全效益表，实现动态入侵响应。

其中，服务影响关注的是服务的高可用，选择的防御对策是否会影响其他节点的服务运行；安全成本关注的是设备的可用防御资源，做出的决策是否会大量占用软硬件资源，导致服务阻塞等问题；防御能力关注的是防御策略的有效性，

也就是防御成功的概率。节点1在获得决策中心的效益值后，结合自身权重矩阵 w ，抉择出最优的防御决策 cm_s 。若最优决策 $Q_1(cm_s)$ 不满足领域内的协同服务要求 Γ ，则考虑备用的决策，迁移服务到备用设备的可能性。由于安全管理是贯穿云、边、端的，只要其中一个节点存在安全隐患，就会导致协同安全防线的溃败。

在协同防御阶段，部署防御措施后，防御态势包含CPU、内存、响应时间、连接状态等服务相关的性能指标。一旦节点出现故障，在有限时间内，部分指标恢复不到正常工作状态，就向上反馈信息，等待协同决策的重新组合。若还不能解决问题，决策中心向上继续反馈给感知节点，重新评估网络中存在的风险。

3.2 感知序参量模型

基于感知态势信息 s 评估网络的感知一致性：

$$r_s = \frac{1}{2M \cdot L} \sum_i \left| \lim_{\Delta t \rightarrow T_m} \frac{1}{\Delta t} \int_{t_r}^{t_r + \Delta t} e^{\phi(s_i(t), s'_i(t))} dt \right| \cdot \sum_{j \in N_i^c} \left| \lim_{\Delta t \rightarrow T_m} \frac{1}{\Delta t} \int_{t_r}^{t_r + \Delta t} e^{\phi(s_i(t), s_j(t))} dt \right| \quad (9)$$

其中， r_s 表示感知序参量， M 表示网络的节点数， L 表示网络的总边数， T_m 表示评估周期， t_r 表示起始时间， s_i 表示每个节点的网络安全态势感知信息，包含攻击的类型、持续时间、端口、数据包传输速率等其他信息， s'_i 表示节点所处环境实际存在的安全风险信息， $\phi(\cdot)$ 和 $\phi(\cdot)$ 是计算态势误差的向量场。各个节点的安全部署能力不同，根据式 (9) 中的 $\phi(s_i(t), s'_i(t))$ 量化感知与实际存在的风险误差。从攻击的发起，到数据流的异常检测，再到感知态势更新，存在时间上的延迟。因此感知与实际的风险信息有一定的误差，造成 r_s 的下降。若后续没有新的风险生成， r_s 迅速恢复至协同状态，实现节点对安全风险感知的完备性。在局域范围内， $\phi(s_i(t), s_j(t))$ 量化节点 i 和节点 j 间对共性攻击检测的一致性，例如，检测网络中存在的注入攻击，并确保云、边、端同域或跨域推送信息流的一致性，是协同感知交互的基础。可通过多径路由、数字签名、事务消息等多种方法，保证信息一致性，最小化故障错误的影响。

3.3 决策序参量模型

基于决策态势信息 c 评估网络防御一致性:

$$r_c = \frac{1}{2M \cdot L} \sum_i \left| \lim_{\Delta t \rightarrow T_m} \frac{1}{\Delta t} \int_{t_i}^{t_i + \Delta t} e^{\varphi(c_i(t), c'_i(t))} dt \right| \cdot \sum_{j \in N_i^c} \left| \lim_{\Delta t \rightarrow T_m} \frac{1}{\Delta t} \int_{t_j}^{t_j + \Delta t} e^{\phi(c_i(t), c_j(t))} dt \right| \quad (10)$$

其中, r_c 表示防御序参量。

云边端协同网络的协同决策以入侵响应为基础, 针对各类攻击, 云边端不同层次的决策中心根据防御资源以安全效益最大化进行协同动态决策, 共同组成一道防护边界, 抵抗安全威胁, 也就是说, 设备节点自身部署的安全策略组合必须在基准线 Γ 之上, 使用 c_i 表示获得的决策态势信息, 包括决策中心的安全效益、权重 w 等信息。 c'_i 表示风险实际所需要的决策态势信息。 $\varphi(c_i(t), c'_i(t))$ 表示决策节点有能力对一个或多个攻击, 做出正确的防御策略裁决。例如 DoS 攻击可以作用于网络层、传输层和应用层, 意味着云、边、端都有可能面临此种风险, 相应的防御对策库有重定向、过滤机制、降低报文的响应速率等方法, 需要在感知正确的情况下, 选择有效的措施进行安全部署。然后, 使用 $\phi(c_i(t), c_j(t))$ 代表节点 i 和节点 j 之间分布式决策安全效益选择达成一致, 在 Γ 之上, 实现协防能力 “1+1>2” 的效果, 这是云边端分布式决策协同能力的核心体现。

3.4 防御序参量模型

基于防御态势信息 p 评估网络的防御一致性:

$$r_p = \frac{1}{M} \sum_{i=1}^M p_i \quad (11)$$

其中, r_p 表示防御序参量。

在安全防护措施部署到相应的设备时, 还需要对其进行防御效果的评估, 来保证云边端协同网络的服务安全。在开展业务的过程中, 用户将敏感数据上传至云, 这就意味着数据在云、边、端间自由流通, 且安全性面临多方的安全挑战, 所以防御一致性要求对所有涉及的节点的性能指标 p_i 进行评估, 反馈给决策要素。在各个节点独立安全运行的基础上, 构建立体化的协同安全评估架构。

3.5 云边端协同网络安全效能评估模型

$$r = r_s \times r_c \times r_p \quad (12)$$

在云边端协同网络中, 若 $r_s = 1$, 感知态势达到一致, 说明云边端协同网络中的所有攻击, 潜在风险都被识别到了; 下一步 $r_c = 1$, 各个节点都达到决策一致, 表示受攻击的节点都作出了安全效益最优的选择, 实现联合安全效益最优; 最后, 当所有节点都达到防御一致 $r_p = 1$, 证明协同网络形成了有效的防护网, 保证了服务的高可用性。从时间轴来看, 只有先达到了感知一致, 才能决策一致, 然后达到防御一致的闭环。最后, 将感知、决策、防御进行有机的结合, 构建云边端协同网络安全效能评估模型。

4 实验评估

实验的硬件环境为 16 GB 运行内存, 一个 2.2 GHz 的处理器, 仿真验证的语言为 Python。使用 CICIDS2017^[20] 作为正常数据和安全风险的来源, 对其进行重新标注, CICIDS2017 分组标签见表 2。再基于 Networkx 库创建不同属性的节点代表云、边、端各层次的设备, 为不同的节点配置可用的防御策略, 并在节点间生成任务关联, 以此模拟 “感知—决策—防御” 网络。

表 2 CICIDS2017 分组标签
Table 2 Grouping labels for CICIDS2017 dataset

新标签	原始标签	数量
Bengin	Bengin	2 271 320
Bot	Bot	1 956
Brute Force	FTP-Patator, SSH-Patator	13 832
DoS/DDoS	DDoS, DoS Hulk, httpstest, DoS, GoldenEye, DoS slowloris	3 979 748
Infiltration	Infiltration	36
PortScan	PortScan	158 804
Web attack	Webattack - Brute Force, Webattack - Sql Injection, Web attack - XSS	2 120

模拟的任一节点都具备感知、决策、防御要素, 节点间的差异主要体现在感知与决策能力, 其中云侧一般由计算资源丰富的集群组成, 其模拟的节点感知属性可选用复杂度更高的检测模型来提高检测精度。且在决策阶段对于各类的风险都有完善的配置, 这意味着对策库中对于 CICIDS2017 数据集中出现的攻击都有对应措施。边侧与云侧相比, 部分模拟的节点可能由于受到

计算资源的限制,无法部署深度学习环境,仅支持传统的机器学习算法。同时为了体现决策能力的差异,模拟的边侧节点只能针对部分攻击做出有效的防御措施。端侧节点的配置方式类似于边侧节点,在感知和决策方面都存在不足。还有一类特殊的节点作为决策中心统合领域内的效益表,辅助决策阶段的多目标优化,实现决策的最优。

在感知环节,以数据流作为攻击者的攻击行为,节点按照云、边、端能力的不同,部署深度置信网络^[21]、MLP (multilayer perceptron)、Birch+MLP^[22]等模型作为入侵检测的传感器。这是因为需要模拟云、边、端之间的感知能力差异和资源配置不均。在文献[23]中,对于传统的机器学习方法,决策树和朴素贝叶斯模型能够很好地识别正常流量和Brute Force类型的数据流量,且对于正常流量的识别精确率为1,但无法区分XSS和SQL类型的数据流量。这样的模型可以在缺少深度学习环境的节点设备中用于二分类。当其在识别到非正常的流量时,可以借助领域内节点的检测模型,做进一步风险识别,整合感知能力,实现协同感知。而类似深度置信网络这样的深度学习模型,对各种风险有较好的认识,可部署在本身计算资源丰富的节点处,以此协助边侧、端侧的节点进行感知。再通过多路径推送,确保节点消息收发的一致性,使用深度优先算法networkx.algorithms.simple_paths.all_simple_paths进行路径发现。

在决策中,针对上述攻击,节点根据事先配置的决策对策库与攻击类型进行匹配,判断是否有能力采取相应的防御措施进行协防。防御的方法可以是丢弃、过滤、限速、重启、关闭、服务迁移等。关键是决策节点通过SAW (simple additive weighting)^[24]对当前网络态势信息进行最优解的选取,并对攻击入侵做出自动响应,使用 Ω 表示所有可选的决策,具体过程是先依靠决策中心构建归一化的决策矩阵。

$$\begin{aligned}\tilde{K}_q(\text{cm}_i) &= \frac{K_q(\text{cm}_i)}{\max_{k \in \Omega} (K_q(\text{cm}_k))} \\ \tilde{K}_h(\text{cm}_i) &= \frac{K_h(\text{cm}_i)}{\max_{k \in \Omega} (K_h(\text{cm}_k))} \\ \tilde{K}_b(\text{cm}_i) &= \frac{K_b(\text{cm}_i)}{\max_{k \in \Omega} (K_b(\text{cm}_k))}\end{aligned} \quad (13)$$

其中, $\tilde{K}_q(\text{cm}_i)$ 表示归一化后,第*i*个方法 cm_i 表

示的服务影响数值, $\tilde{K}_h(\text{cm}_i)$ 表示归一化后的安全成本数值, $\tilde{K}_b(\text{cm}_i)$ 表示归一化后防御能力数值。

然后结合当前网络安全环境和节点自身服务配置构建相对应的优化目标权重矩阵:

$$\mathbf{w}_i = [w_q, w_h, w_b]^T \quad (14)$$

其中, w_q 表示服务影响的占比, w_h 表示安全成本的占比, w_b 表示防御能力的占比。

最后加权求和获得安全效益值并选择最优的决策 cm_δ 。

$$\begin{aligned}Q(c) &= [\tilde{K}_q(\text{cm}_i), \tilde{K}_h(\text{cm}_i), \tilde{K}_b(\text{cm}_i)] \cdot \mathbf{w}_i \\ \text{cm}_\delta &= \operatorname{argmax}_{i \in \Omega} Q(c)\end{aligned} \quad (15)$$

其中, $Q(c)$ 表示基于某个节点的*c*决策态势信息的安全效益评估函数计算,再根据 $Q(c)$ 找出最优的决策方法 cm_δ 。

对于防御阶段的监控,各个节点对自身的功能性指标进行监控。要求在防御措施部署完毕后,必须在有限的时间恢复到安全阈值以内,如在被攻击时的工作负载必须在0~5 s内降低至正常工作的状态,才能判断为该节点的防御成功,否则需要向上反馈进行重新决策或任务迁移启用备用节点。

4.1 感知一致性

首先评估协同网络在感知阶段的安全性能表现。在感知阶段,各个节点的检测模型须正确检测到服务环境中存在的安全风险,不遗漏任何一个潜在风险。但实际情况是入侵检测模型的准确率达不到1^[23,25]。如图6所示的感知序参量,节点感知曲线在受到攻击的时候,随着节点持续识别到攻击数据流,同步反映在感知序参量上,其值迅速下降,再逐步恢复。但是在最后感知序参量仍无法恢复到1,原因是准确率的问题,节点发现了攻击特征却误判了攻击的类别。另外,节点将攻击的数据流当成了正常的数据流,两者导致了感知网络的一致性失衡。

考虑在网络攻防中,类似于数据注入攻击,攻击者可实现的攻击目标众多,影响范围大。因此,节点间感知信息的共享异常重要,在协同感知设计的基础上,依据服务的依赖程度,进行信息流的推送,提高单个节点的感知精度和整个协

同网络的感知能力。针对上述序参量失衡的问题,如 Web attack 被误判成 DoS 的数据流,可以由邻居节点的传感器进行更高置信度的纠错,而类似遗漏 PortScan 攻击的情况,可以解析为多个由邻居节点推送信息流,分析其中的 PortScan 部分,根据节点的相关度,采用简单的赋权投票机制,决定 PortScan 是否可以作为节点自身感知信息的补充。正如协同感知曲线所表现的,各节点将自身感知的信息与其领域内的节点进行互补,形成全局网络的安全协同。保证对领域内的潜在风险进行完备的感知检测,使网络在遭受攻击后,迅速恢复至稳定一致的状态。

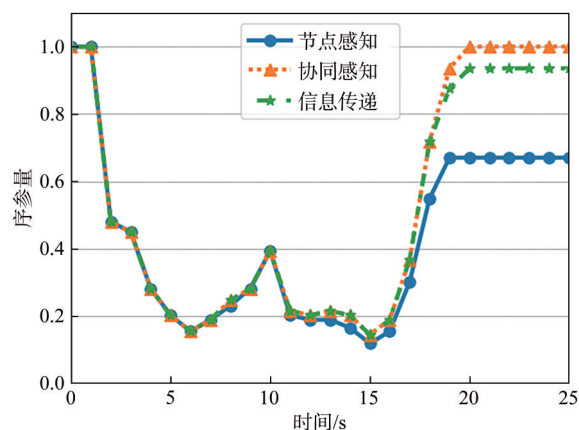


图6 感知序参量
Figure 6 Perceptual order parameter

然而考虑在信息推送的过程中,消息的一致性可能受到损害。实验设置一个概率使信息流推送失败,造成协同感知信息耦合的失败。于是信息传递曲线在协同曲线的基础上,按照 $\phi(s_i(t), s_j(t))$ 的定义,随着感知态势的信息缺失,协同能力减弱,部分节点无法达成感知一致。在采取了多路径传输方法后,能有效防止推送失败的发生,保证各个服务关联的节点间风险信息认知是一致的,恢复到原来协同曲线的性能表现。

4.2 决策一致性

在决策阶段,位于云边端协同网络不同层次的节点受限于硬件等问题,将节点分为决策中心和决策节点。决策中心计算安全效益,决策节点进行最优选取,并将决策的一致性,分为两个方面,一个是决策能力,另一个是决策安全效益。

首要是节点的决策能力,对于感知到的各类

风险信息,节点最重要的是具备对应的安全对策,才能有效地保护网络安全。在没有决策中心协助的情况下,只依靠预先配置的防御决策库,决策能力序参量如图7所示。

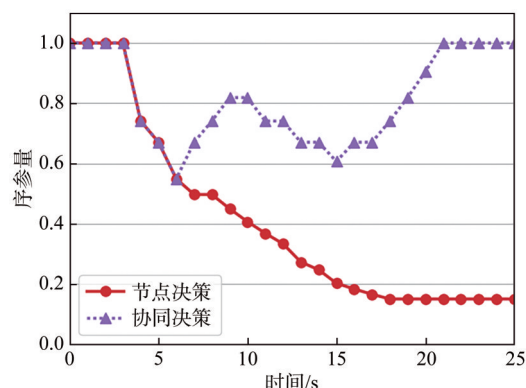


图7 决策能力序参量
Figure 7 Decision capacity order parameter

随着攻击的类型增加,部分节点可能缺少对 Brute Force、Web attack 等攻击类型的防御配置,导致决策序参量下降。尤其是在边侧、端侧,防御资源紧张,会出现更多这样的情况。所以在决策层面引入专用的决策中心统筹所有防御资源,若出现上述单个节点没有相应对策的情况,可以将其服务迁移到备份节点,或调整节点的服务占用资源,增强安全模块,进行安全策略的重新配置等。

其次是协同决策的另一层含义, $\phi(c_i(t), c_j(t))$ 决策安全效益的一致性, SAW (simple additive weighting) 是协同决策的关键。决策中心先根据受攻击节点运行的服务判断其邻居,计算所有可用对策的安全效益值 $[K_q, K_h, K_b]$ 。对策库中的一部分重启、限速等是决策节点自身具备的,另一部分迁移、防火墙重新配置等方法由决策中心提供。受攻击节点为了保证服务的质量,按照权重 $[w_q, w_h, w_b]$ 的配比,选择局部最优的对策 cm_s 。此时节点通过决策中心获得最低安全效益标准,保证不低于安全阈值 Γ 。否则, cm_s 会成为协同决策中薄弱的一环,可能导致用户的数据泄露。

决策安全效益序参量如图8所示,在协同决策曲线的基础上加入了安全效益的指标后,是更高层次的决策一致性体现。因此,若按照开始的

协同决策曲线的决策，部分决策并不是最优的且不满足安全效益，决策序参量会下降得更快，需要决策中心和决策节点重新评估组合相应的对策，才能恢复 r_c 的值。

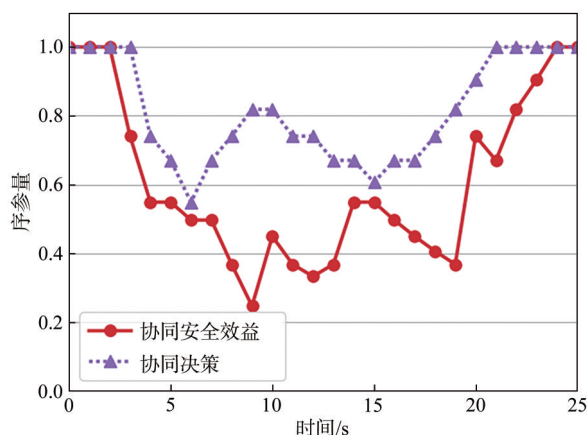


图8 决策安全效益序参量
Figure 8 Decision safety benefit order parameter

4.3 防御一致性

在防御阶段，在部署相应的安全策略后，对节点的性能实时监控，根据期望的网络性能，判断是否反馈给决策要素进行自适应优化，对感知外的攻击或错误的裁决进行修正，保证云服务的可信赖性。最终结合形成“感知—决策—防御”序参量，如图9所示。

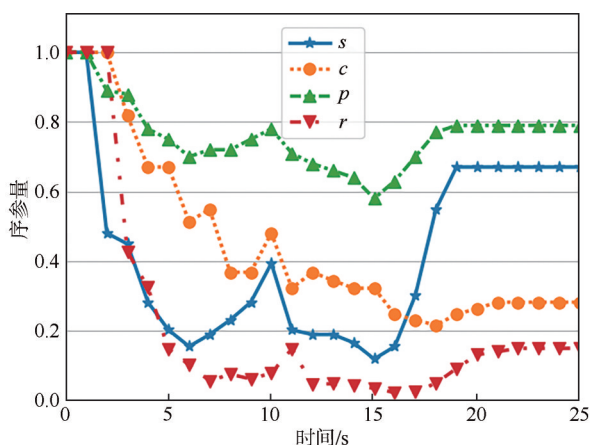


图9 “感知—决策—防御”序参量
Figure 9 Perception-decision-defence order parameter

从结果分析中发现安全效能模型曲线 r 分别受感知曲线 s 、决策曲线 c 和防御曲线 p 的影响。随着业务环境存在的攻击增多，感知、决策、防御曲线的性能开始下降，最终反映到安全效能曲

线上，且在没有协同的情况下，单个边侧和端侧的节点感知、决策、防御能力薄弱，对于一些攻击缺少处理的对策方案，整体的分层网络架构僵化，不能满足服务的可持续性要求。

协同“感知—决策—防御”序参量如图10所示，采用简单的协同安全一致性方法后，在遭受攻击时，云边端协同安全效能模型准确地反映了协同网络在初时受到攻击后，内部架构开始远离平衡，再到感知、决策、防御要素的引导下，逐渐恢复到平稳一致的协同演化过程。简单的协同策略维护了单一节点对风险感知的全面性、决策的充分性和防御的有效性。最终，实现云边端协同网络的横向一致和纵向一致。

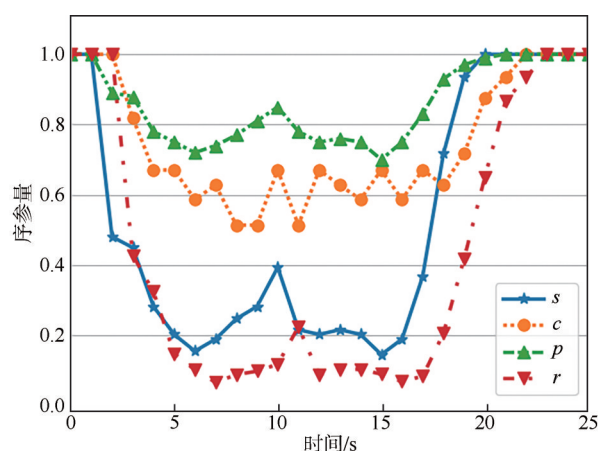


图10 协同“感知—决策—防御”序参量
Figure 10 Collaborative perception-decision-defence order parameter

5 结束语

根据云边端分布式体系协同安全的非平衡演变特点，分析了协同网络安全评估相关的问题，包括云边端协同安全架构问题、协同防护理论的一致性证明问题，构建了基于序参量的云边端分布式协同安全效能评估模型。首先，基于感知、决策和防御3类安全要素的时间、态势一致性关系，分析云侧、边侧、端侧设备间的协同防护能力。其次，证明了协同网络的协同安全态势信息能够收敛至平衡点，保持一致性。最后，引入感知、决策、防御序参量模型，分阶段描述云边端协同网络的安全防护的过程，评估其协同防护的能力。通过仿真验证一定程度上说明了基于序参量的安全效能评估模型的可行性与有效性。借助

简单的协同感知互补、分布式动态决策响应和防御反馈机制,序参量模型准确地反映了网络有序度从低到高的演变过程,为云边端协同网络的安全效能评估提供合理的参考。

参考文献:

- [1] 张晓东,吕从东.云边端协同安全隐私保护框架研究[J].南京大学学报(自然科学),2022,58(3):413-419.
ZHANG X D, LYU C D. A security and privacy protection framework for cloud edge collaborative[J]. Journal of Nanjing University (Natural Sciences), 2022, 58(3): 413-419.
- [2] 王文娟,杜学绘,王娜,等.云计算安全审计技术研究综述[J].计算机科学,2017,44(7):16-20+30.
WANG W J, DU X H, WANG N, et al. Review on security audit technology for cloud computing[J]. Computer Science, 2017, 44(7): 16-20+30.
- [3] MANIA H, ABDURACHMAN E, GAOL F L, et al. Survey on threats and risks in the cloud computing environment[J]. Procedia Computer Science, 2019, 161: 1325-1332.
- [4] HUANG Z Y, XIA G M, WANG Z H, et al. Survey on edge computing security[C]//Proceedings of the 2020 International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE). Piscataway: IEEE Press, 2020: 96-105.
- [5] 冉黎琼,翁越男,徐小玲,等.云、边缘和雾计算安全性研究综述[J].无线电工程,2023,53(2):247-261.
RAN L Q, WENG Y N, XU X L, et al. A review of cloud, edge and fog computing security[J]. Radio Engineering, 2023, 53(2): 247-261.
- [6] LATIF R, ABBAS H, ASSAR S, et al. Cloud computing risk assessment: a systematic literature review[M]. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014: 285-295.
- [7] SENDI A S, CHERIET M. Cloud computing: a risk assessment model[C]//Proceedings of the 2014 IEEE International Conference on Cloud Engineering. Piscataway: IEEE Press, 2014: 147-152.
- [8] CAYIRCI E, GARAGA A, SANTANA A, et al. A cloud adoption risk assessment model[C]//Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing. Piscataway: IEEE Press, 2014: 908-913.
- [9] FURUNCU E, SOGUKPINAR I. Scalable risk assessment method for cloud computing using game theory (CCRAM) [J]. Computer Standards & Interfaces, 2015, 38: 44-50.
- [10] LI K, YANG D, BAI L, et al. Security risk assessment method of edge computing container based on dynamic game[C]//2021 IEEE 6th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA). Piscataway: IEEE Press, 2021: 195-199.
- [11] ENDSLEY M R. Design and evaluation for situation awareness enhancement[J]. Proceedings of the Human Factors Society Annual Meeting, 1988, 32(2): 97-101.
- [12] GONZALEZ G G, BELHAOUANE M, DEBAR H, et al. RORI-based countermeasure selection using the OrBAC formalism[J]. International Journal of Information Security, 2014, 13(1): 63-79.
- [13] SHAMELI-SENDI A, LOUAFI H, HE W B, et al. Dynamic optimal countermeasure selection for intrusion response system[J]. IEEE Transactions on Dependable and Secure Computing, 2018, 15(5): 755-770.
- [14] HAKEN H. Synergetics[J]. Physics Bulletin, 1977, 28(9): 412-414.
- [15] ARENAS A, DÍAZ-GUILERA A, KURTHS J, et al. Synchronization in complex networks[J]. Physics Reports, 2008, 469(3): 93-153.
- [16] SAYYAADI H, DOOSTMOHAMMADIAN M R. Finite-time consensus in directed switching network topologies and time-delayed communications[J]. Scientia Iranica, 2011, 18(1): 75-85.
- [17] GÓMEZ-GUTIÉRREZ D, VÁZQUEZ C R, ČELIKOVSKÝ S, et al. On finite-time and fixed-time consensus algorithms for dynamic networks switching among disconnected digraphs[J]. International Journal of Control, 2020, 93(9): 2120-2134.
- [18] KHALIL H K. Control of nonlinear systems[M]. New York: Prentice Hall, 2002: 156-162.
- [19] LIU M, MA H, CUI J M, et al. Exploring information interactions in decentralized multiagent coordination under uncertainty[C]//Proceedings of 2020 5th IEEE International Conference on Big Data Analytics (ICBDA). Piscataway: IEEE Press, 2020: 304-308.
- [20] SHARAFALDIN I, HABIBI L A, GHOR-BANI A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization[C]//Proceedings of the 4th International Conference on Information Systems Security and Privacy. SCITEPRESS - Science and Technology Publications, 2018: 108-116.
- [21] BELARBI O, KHAN A, CARNELLI P, et al. An intrusion detection system based on deep belief networks[M]. Cham: Springer International Publishing, 2022: 377-392.
- [22] YIN Y, JANG-JACCARD J, SABRINA F, et al. Improving multilayer-perceptron (MLP)-based network anomaly detection with birch clustering on CI-CIDS-2017 dataset[C]//Proceedings of the 2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD). Piscataway: IEEE Press, 2023: 423-431.
- [23] MASEER Z K, YUSOF R, BAHAMAN N, et al. Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset[J]. IEEE Access, 2021, 9: 22351-22370.
- [24] KALISZEWSKI I, PODKOPAEV D. Simple additive weighting-a metamodel for multiple criteria decision analysis methods[J]. Expert Systems with Applications, 2016, 54: 155-161.
- [25] INAYAT Z, GANI A, ANUAR N B, et al. Cloud-based intrusion detection and response system: open research issues, and solutions[J]. Arabian Journal for Science and Engineering, 2017, 42(2): 399-423.

[作者简介]



范其纲（1999- ），男，福建福州人，西安电子科技大学硕士生，主要研究方向为复杂网络安全、云计算安全。



李兴华（1978- ），男，河南南阳人，西安电子科技大学教授、博士生导师，主要研究方向为网络与信息安全、安全协议形式化。



蒋忠元（1988- ），男，陕西榆林人，西安电子科技大学教授、博士生导师，主要研究方向为复杂网络安全、复杂网络传输动力学、网络功能虚拟化。



马建峰（1963- ），男，陕西西安人，西安电子科技大学教授、博士生导师，主要研究方向为无线网络安全、移动智能系统安全。