

• 四川大学建校 130 周年特刊约稿 •

DOI:10.12454/j.jsuese.202600434



本刊网刊

熵变驱动的网络空间多域融合智能安全新范式

饶志宏¹, 张志勇¹, 陈 旻², 何健辉³, 徐若禹², 李柱成¹, 赵 鑫³, 陈剑锋¹

(1. 中国电子科技集团公司第三十研究所, 四川 成都 610041; 2. 西北工业大学 网络空间安全学院, 陕西 西安 710072;
3. 中国电子科技集团有限公司电子科学研究院, 北京 100041)

摘 要: 网络空间安全的本质是不确定条件下的攻防博弈, 对抗的胜负取决于对不确定性的驾驭能力。随着网络空间对抗从网络信息域向物理实体、电磁频谱、社会认知等领域深度延伸, 不确定性显著增加, 不再局限于单域内部的固有随机性与认知盲区, 更突出地表现为跨域传导与级联放大, 传统单域对抗视角已难以有效应对。然而, 现有研究缺乏统一的不确定性度量框架, 无法为多域融合对抗提供贯通度量、推演与判定的统一理论框架。为突破上述瓶颈, 本文提出熵变驱动的网络空间多域融合智能安全新范式, 将多域融合攻防博弈刻画为动态双向的熵控过程: 以熵为统一数学标尺度量和计算各类不确定性, 攻防双方均力图推动系统熵变朝着“己方熵减、对方熵增”的方向收敛。本文的核心理论贡献包括 3 项。第一, 创立了攻击熵与防御熵的对偶度量体系, 融合香农熵与相对熵, 将认知不确定性与策略有效性纳入同一量化标尺。第二, 构建了跨域不确定性动力学模型与攻防有效性判定定理, 通过随机差分方程刻画攻防行为驱动下不确定性在多域间的传导与放大, 并基于李雅普诺夫稳定性理论建立了策略有效性的形式化判据。第三, 提出了内嵌熵控逻辑的攻防博弈推演框架, 以层次化博弈推演模型为环境基座, 以信念驱动的多智能体策略生成方法实现自适应推演。数值推演实验结果表明: 攻击熵与防御熵能够将多域异质不确定性统一压缩为可比较的标量; 跨域耦合建模可有效避免单域独立推演导致的策略假收敛, 验证了多域融合的结构必要性; 基于熵控优化目标与对手镜像推演的策略生成闭环, 相较传统单域方法和无耦合方法具有显著优势。在新范式指导下, 本文确立了“多域融合、熵变驱动”的安全体系构建理念, 并以熵控逻辑阐释了防御形态从“杀伤链”向“杀伤网”演进的机理。结论部分从信念分布的参数化与熵计算的可解性、动力学模型的结构辨识与参数获取、博弈推演的实时性与策略空间的可扩展性 3 个层面, 界定了理论体系向实际应用落地所需正视的可计算性与可操作性边界。本文属于概念体系论证与理论框架构建, 为网络空间安全决策从经验依赖迈向可计算范式提供了数理基础。

关键词: 网络空间安全; 多域融合; 熵变驱动; 熵控理论; 攻击熵/防御熵; 多智能体博弈

中图分类号: TP393.08

文献标志码: A

文章编号: 2096-3246(2026)05-0360-13

随着数字技术与实体世界的深度交织, 网络空间已演变为支撑社会生产生活、承载国家核心利益、决定战略竞争优势的关键新疆域, “没有网络安全就没有国家安全”^[1]。网络空间安全的本质是不确定条件下的攻防对抗, 攻防双方的一切筹划与行动皆深陷于信息不对称、状态演化不可预测与对手意图难以洞察等困境^[2-3], 对抗的胜负在相当程度上取决于哪一方能更有效地驾驭各种不确定性。由此可见, 网络空间安全对抗的深层本质是围绕不确定性的博弈, 攻防双方都在试图操控这种不确定性: 一方面, 己方竭力通过态势感知^[4-5]、行为分析^[6-7]和效果评估^[8-9]等技术手段来降低自身面临的

不确定性; 另一方面, 又通过伪装、欺骗和动态变化等手段为对手制造不确定性, 增加其决策成本^[10-11]。

当前, 网络空间对抗正经历一场深刻的范式转型, 其边界已全面突破传统的网络信息域, 向物理实体、电磁频谱、社会认知等领域深度延伸, 形成了四域深度耦合的复杂对抗格局^[12-13]。其中, 物理实体域涵盖物理设施的空间位置与运行环境, 电磁频谱域涵盖无线通信的频段、功率与信号特征, 网络信息域涵盖信息系统的协议、拓扑与数据流转, 社会认知域涵盖人员决策、组织行为与舆论传播。这种多域融合的趋势, 将对抗中的不确定性困境系统性放大。不确定性不再局限于单域内部的固

收稿日期: 2026-05-25 修回日期: 2026-07-17 网络出版日期: 2026-08-31

基金项目: 四川省基础研究领军科学家专项基金项目(2024JDKXJ0011)

作者简介: 饶志宏(1970—), 男, 正高级工程师, 博士。研究方向: 网络空间安全。E-mail: passet30@163.com

有随机性与认知盲区,更突出地表现为跨域传导与级联放大。传统的单域对抗视角,如同盲人摸象,只能观察到局部现象,无法理解博弈对抗的全局图景,更难以对不确定性实施有效管控。应对这一挑战的根本出路,恰恰在于构建多域融合安全体系,通过融合物理、电磁、网络、认知等域的信息,从单域视角升维到多域融合对抗视角,在更高维度上消减己方的不确定性,同时增加对手面临的不确定性。

然而,实现这一升维面临一个根本性的理论瓶颈:现有研究缺乏统一、可计算、可推演的不确定性度量框架,难以支撑多域融合条件下的体系化攻防决策。该瓶颈在以下3条研究路径中均有体现:一是基于马尔可夫决策过程、混合自动机等形式化工具刻画系统状态演化^[14],该方法多聚焦于物理域、网络域的状态转移,但对主观认知与策略互动的不确定性刻画不足;二是采用概率论与随机过程方法,该方法通过贝叶斯博弈等模型量化节点级风险^[15],但模型常依赖强先验假设,高维多域场景下可扩展性受限;三是基于逻辑与知识的方法,该方法能利用本体和规则实现认知不确定性表征^[16],但对概率性、动态演化描述能力弱。

为了突破这一困局,亟需一把能够统一度量各类不确定性、动态追踪其跨域演化过程的数学标尺。诸多工具中,熵因其物理意义明确、统一标尺的特性被引入安全领域,用于量化不确定性。部分研究将经典熵或其变体应用于具体安全场景,如病毒传播态势研判^[17]、攻击/异常检测^[18-20]、DDoS检测^[21-22]、恶意软件分类^[23]、网络拓扑鲁棒性评估^[24];部分研究对香农熵进行了数学扩展以处理态势感知时的多专家评价冲突^[25]或者证据理论中的不确定性问题^[26]。然而,这些工作仅将熵作为局部检测指标,停留在点状应用层面。饶志宏等^[27]在前期探索了基于条件熵的攻防不确定性度量,实现了多轮观测下的信念更新,但仍未延伸至双方策略驱动的状态演化与攻防有效性判定。值得关注的是,Janani^[28]于2025年独立提出了“熵注入”概念,同样将其提升为网络安全的新范式。然而,该工作侧重于对已有技术的综述与效能评估,尚未建立以熵为核心、贯通不确定性度量与策略生成的理论框架。

在国内研究方面,邬江兴院士团队提出了内生安全范式^[29],该范式将安全能力构建于系统架构内部而非依赖外部附加防护,通过拟态防御^[30]的动态异构冗余(DHR)架构主动改变系统的攻击面,以结构决定安全为核心思想,通过动态性、异构性与冗余性的有机融合增加对手对系统状态认知的不确定性(即测不准效应),与

本文“增敌之熵”的目标在方向上具有契合性。需要指出的是,现有文献已围绕拟态防御建立了较为完善的量化评估体系:如马海龙等^[31]定义了拟态熵和拟态变换增益概念,使用香农多样性指数与二次熵度量服务集异构度,并阐释了拟态防御(CMD)三定理以刻画异构度、冗余度与防御效能之间的关系;此外,共模逃逸概率、攻击成功概率、系统可用概率等指标也已经形成了标准化的评估方法^[32]。然而,上述度量方法主要聚焦于架构层面的系统属性,尚未从攻防博弈的宏观视角出发,引入熵度量统一刻画攻防双方各自面临的多源、异构不确定性。

上述工作与Janani^[28]提出的“熵注入”概念共同表明,不确定性管控这一安全思想正在形成共识。本文在此基础上进一步推进:将不确定性管控从单向的防御策略升维为攻防双方共同参与的博弈机制,提出熵变驱动的网络空间多域融合智能安全新范式,其核心思想是:将多域融合的攻防博弈,构建为一个动态、双向的“熵控”过程——以熵为统一的数学标尺,度量和计算对抗中的各类不确定性;攻防博弈的终极目标,是推动整个系统的熵变朝着“己方熵减、对方熵增”的有利方向收敛。为给这一新范式奠定坚实的理论基础,本文做出了以下3项核心贡献:

第一,创立了以攻击熵与防御熵为核心的度量体系,从信息论的角度将认知不确定性与策略有效性评估纳入了统一的数学框架,为攻防双方对不确定性进行双向管控提供了对偶、可比较的标尺。这一度量体系使得“看清自己”与“迷惑对手”从经验直觉上升为可计算的量化指标。

第二,构建了跨域不确定性动力学模型,跟踪多域融合场景下攻防行为驱动不确定性演化的轨迹。基于此,建立了攻防行为有效性的形式化判定条件,为策略的优劣评判提供了严格的数学判据。两者构成了从动态推演到有效性证明的理论闭环。

第三,提出了内嵌熵控逻辑的攻防博弈推演框架:以层次化博弈推演模型构建可计算的博弈环境;通过信念驱动的多智能体策略生成方法,将不确定性度量与演化模型内嵌于框架推演流程中。该框架为攻防双方在不确定性条件下的自适应策略生成提供了系统化的方法支撑。

上述3项工作协同,为新范式提供了可计算、可推演、可判定的数学基础。图1给出了这一新范式的宏观概念模型:攻防双方在各自的信念空间中,并行运行度量、推演与判定、博弈与策略生成的核心流程,通过攻防行为交互驱动系统状态演化,构成“己方熵减、对方熵增”的双向熵控闭环。

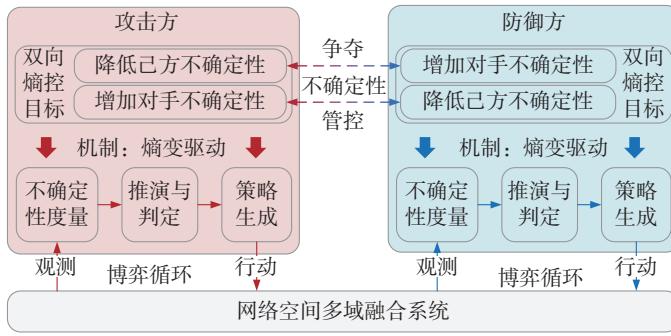


图 1 熵变驱动的多域融合智能安全概念模型

Fig. 1 Conceptual model of entropy evolution driven intelligent cybersecurity for multi-domain fusion

为验证该理论体系的可计算性与可操作性,本文以电力调度数据网为典型场景,给出了一个完整的多域融合安全防护数值推演示例。在此基础上,进一步论述了新范式对安全体系构建的指导意义,确立了“多域融合,熵变驱动”的核心理念和“道、法、术、器”的构建逻辑,阐释了对抗形态从“杀伤链”向“杀伤网”演进的深层机理。为论述简洁,本文后续章节将以防御方为主要分析视角,攻击方的对称逻辑不再赘述。

1 熵控理论与策略生成:框架与验证

1.1 基于熵的不确定性度量和策略优化准则

网络空间攻防博弈的本质特征在于信息的不对称性:攻击方与防御方均无法直接获知目标系统的真实状态,只能通过各自有限且可能被干扰的观测渠道,形成对系统状态的主观认知。这种认知在数学上可形式化为信念分布。

定义 1(系统状态与攻防信念) 设目标系统在时刻 t 的真实状态为多维随机向量 $\mathbf{X}(t)$,其分量分别刻画该系统在物理、电磁、网络、认知等域中的关键属性。攻防双方基于各自的观测信息,形成对 $\mathbf{X}(t)$ 的主观后验信念分布 $F_A(t)$ 和 $F_D(t)$:

$$F_A(t) = P(\mathbf{X}(t) | \mathbf{O}_A(t)) \quad (1)$$

$$F_D(t) = P(\mathbf{X}(t) | \mathbf{O}_D(t)) \quad (2)$$

式(1)~(2)中, $\mathbf{O}_A(t)$ 和 $\mathbf{O}_D(t)$ 分别表示攻防双方截至时刻 t 所获得的全部观测信息。信念分布 $F_A(t)$ 和 $F_D(t)$ 是双方进行一切攻防决策的唯一信息依据。

在此基础上,双方各自怀有对博弈结局的理想期望。攻击方的期望分布 F^- 高度集中于系统“被破坏、被控制”的状态集合上;防御方的期望分布 F^+ 则集中于系统“安全、可控”的状态集合上。两者与信念分布 $F_A(t)$ 和 $F_D(t)$ 属于同一数学对象,均为系统状态 $\mathbf{X}(t)$ 的联合概率分布,但互相对立,体现了攻防目标的零和性。期望分布的设定独立于具体的信念更新过程,

属于博弈开始前即已确立的战略目标。

攻击方与防御方的核心任务均可分解为两个相互关联的子目标:其一,在认知层面,尽可能降低自身对当前态势的认知不确定性;其二,在效果层面,推动系统状态向己方期望的方向演化。这两个子目标在传统安全研究中常被割裂处理——认知不确定性多由信息论度量,而策略效能多由风险评估方法评估——缺乏统一的数学表述。本文提出,以信息论中的香农熵度量认知不确定性,以相对熵度量当前信念与期望目标的偏离程度,并将二者融合为统一的攻击熵与防御熵定义。

定义 2(攻击熵与防御熵) 攻击方视角下的攻击熵 $H_A(t)$ 与防御方视角下的防御熵 $H_D(t)$ 分别定义为:

$$H_A(t) = D_{KL}(F_A(t) \| F^-) + \lambda_A \cdot H(F_A(t)) \quad (3)$$

$$H_D(t) = D_{KL}(F_D(t) \| F^+) + \lambda_D \cdot H(F_D(t)) \quad (4)$$

式(3)~(4)中: $H(\cdot)$ 表示香农熵; $D_{KL}(\cdot \| \cdot)$ 表示相对熵; λ_A 和 λ_D 为权衡系数,反映决策者对认知不确定性相对于目标偏离的相对重视程度。

该定义具有两个重要的理论性质:第一, $H_A(t)$ 和 $H_D(t)$ 均为非负,当且仅当 F^- 退化为单点分布且 $F_A(t) = F^-$ 时, $H_A(t) = 0$ (防御熵对称成立);第二,香农熵项与相对熵项的分离结构,使得攻击熵和防御熵能够同时捕捉认知不确定性与策略有效性两个维度,实现了对攻防态势的综合量化。上述性质保证了攻击熵与防御熵可以作为衡量攻防态势优劣的通用标尺,熵值越大,表明当前态势偏离理想目标越远。需要指出的是,最小值为 0 是数学上的理论极限,实际操作中,攻防双方只需推动熵值收敛至足够小的值,无须期望分布退化为单点分布。当 λ_A 或者 λ_D 取值为 1 时,攻击熵和防御熵在数学上分别等价于 $F_A(t)$ 与 F^- 、 $F_D(t)$ 与 F^+ 的交叉熵。

图 2 示意了攻防双方信念分布在熵控策略下相对于各自期望目标的演化,攻击熵与防御熵随之变化。期望分布和信念分布均可被视作状态空间中的点,其

上覆盖的概率密度函数曲线反映了认知不确定性的大小(曲线越扁平,香农熵越大);各信念分布与期望分布之间的距离度量了目标偏离程度,对应KL散度。在策略驱动下,图2中的防御方信念沿轨迹向 F^+ 收敛(熵减),攻击方信念则背离 F^- 演进(熵增)。图2呈现了防御熵 $H_D(t)$ 的完整构成,攻击熵 $H_A(t)$ 与之对称。

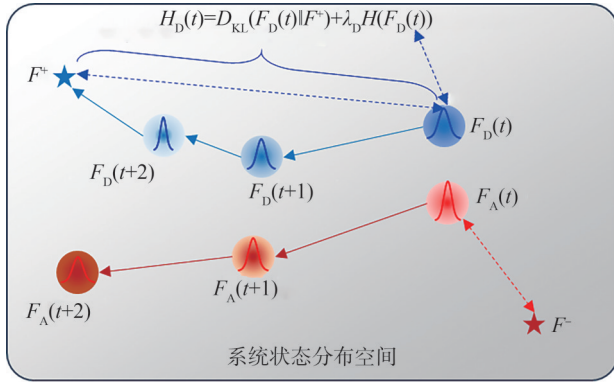


图2 攻击熵/防御熵的构成与演化示意

Fig. 2 Illustration of the attack/defense composition and entropy

基于上述度量,攻防双方在任何时刻的核心操作目标可以统一表述为,选择能够最小化己方攻击熵或防御熵,同时最大化对方熵值的行动。

定义3(熵控的策略优化目标) 设 $a(t)$ 和 $d(t)$ 分别表示攻击方和防御方在时刻 t 将要采取的行动。攻击方与防御方的行动选择可分别形式化为:

$$a(t) = \arg \min_a (\Delta H_A(t|a) - \gamma \Delta H_D(t|a)) \quad (5)$$

$$d(t) = \arg \min_d (\Delta H_D(t|d) - \gamma \Delta H_A(t|d)) \quad (6)$$

式中: $\Delta H_A(t|a)$ 和 $\Delta H_D(t|d)$ 分别表示攻击方和防御方采取行动后己方熵值的预期变化; $\Delta H_D(t|a)$ 和 $\Delta H_A(t|d)$ 分别表示攻击方和防御方采取行动后对方熵值的预期影响; γ 为意愿系数, $\gamma \geq 0$,反映决策者对“增敌之熵”相对于“降己之熵”的重视程度。

上述优化目标的一个关键前提是:攻防双方的一切策略推演,均基于己方的认知而非上帝视角的客观全知信息。以防御方为例,式(6)中 $\Delta H_D(t|d)$ 的计算基于其自身的信念分布 $F_D(t)$ 和期望目标 F^+ ;而 $\Delta H_A(t|d)$ 的计算,则需要构建一个针对攻击方信念的镜像推断模型,模拟攻击方的认知过程,推断攻击方所持的信念 $F_A(t)$,再结合攻击方的期望目标 F^- 进行评估。这种在己方认知世界中代入对手视角的双重推演结构,构成了多智能体博弈决策的理论基础。

1.2 跨域不确定性动力学模型与攻防有效性判定

网络空间攻防博弈的本质是动态演化的:持续的攻防行为不断扰动系统状态,攻防双方对系统状态的认知,即各自的信念分布,也随之持续更新。因此,新

范式的第2项理论任务,是构建能够描述这一动态认知过程的演化模型,并在此基础上建立攻防有效性的形式化判据。

需要强调的是,本节建立的动力学模型与第1.1节的熵度量函数在理论体系中承担不同的角色。动力学模型通过追踪攻防双方的信念分布 $F_A(t)$ 或 $F_D(t)$ 在攻防行为驱动下的变化轨迹,提供不确定性演化的客观规律,属于对事实的推演。而攻击熵 $H_A(t)$ 与防御熵 $H_D(t)$ 将演化结果转化为可比较的决策依据,回答演化是否有利,属于对价值的判断。

1.2.1 跨域不确定性动力学模型

在多域融合对抗环境中,系统的状态演化受到两类因素的共同驱动:一是攻防行为在单个域内产生的直接影响;二是风险在物理、电磁、网络、认知等域之间的跨域传导。前者可类比为物理系统中的“漂移”,后者则是“耦合”。为刻画这一复杂过程,首先将系统状态的信念分布参数化,进而建立以随机差分方程为核心的跨域不确定性动力学模型。

定义4(信念分布的参数化) 设系统状态的真值分布 $F(t)$ 属于由参数向量 $\theta(t)$ 唯一决定的分布族,即 $F(t) = P(X(t); \theta(t))$ 。攻防双方基于各自的观测,分别形成对参数的估计 $\theta_A(t)$ 和 $\theta_D(t)$ 。在此参数化下,攻击熵与防御熵可分别等价地写为 $\theta_A(t)$ 和 $\theta_D(t)$ 的函数。

将信念分布参数化的意义在于,它将高维、复杂的概率分布空间映射到低维的参数空间,使得对不确定性动态演化的追踪在数学上变得可处理。基于此,可构建以防御方视角为例的跨域耦合不确定性动力学模型。

定义5(跨域不确定性动力学模型) 以防御方视角为例,设 $\theta_D^i(t)$ 表示 t 时刻防御方对第 i 域($i \in \{1, 2, 3, 4\}$,其中,1对应地理,2对应电磁,3对应网络,4对应社会)内的信念分布的参数估计。该参数在攻防行为驱动下的演化满足如下随机差分方程:

$$\theta_D^i(t+1) = f^i(\theta_D^i(t), \hat{a}(t), d(t)) + \sum_{j \neq i} C_{ij} \phi(\theta_D^j(t)) + \varepsilon^i(t) \quad (7)$$

式中: $\hat{a}(t)$ 为防御方对攻击行为的估计; $f^i(\cdot)$ 为域内漂移函数,刻画攻防行为 $\hat{a}(t)$ 和 $d(t)$ 在第 i 域内对系统状态的直接影响;第2项为域间耦合项, C_{ij} 为耦合强度矩阵, $\phi(\cdot)$ 为耦合函数,共同刻画不确定性从第 j 域向第 i 域的传导效应; $\varepsilon^i(t)$ 为独立随机扰动项,表征系统内在的不可预测性。耦合矩阵 C_{ij} 的行索引 i 为目标域,列索引 j 为源域,元素值量化了第 j 域不确定性向第 i 域的传导强度。由于域内影响已由漂移函数刻画,耦合项专门负责域间传导,因此其对角线元素恒为零。非对角线元素非负,实际部署中多呈稀疏特性。当每个域

由多个状态分量描述时, C_{ij} 可扩展为分块矩阵, 为清晰起见, 在理论定义和数值实验中均以域级耦合标量示例, 这不影响模型的可扩展性。

图 3 呈现了跨域不确定性动力学模型的工作机

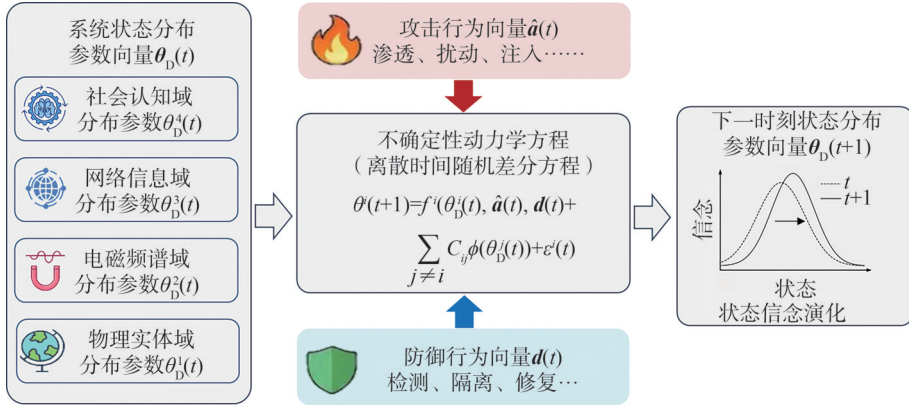


图 3 跨域不确定性动力学模型(防御方视角)

Fig. 3 Cross-domain uncertainty dynamics model (from defender's perspective)

攻击方视角下的动力学方程可对称定义, 仅需将参数 $\theta_D^i(t)$ 替换为 $\theta_A^i(t)$, 将防御行为 $d(t)$ 替换为攻击行为 $a(t)$, 将攻击行为的估计 $\hat{a}(t)$ 替换为防御行为的估计 $\hat{d}(t)$ 。

在工程实践中, 漂移函数 $f^i(\cdot)$ 和耦合函数 $\phi(\cdot)$ 的具体形式可通过数据驱动与机理建模相结合的方式确定: 一方面利用仿真数据与历史记录进行参数学习, 另一方面嵌入物理约束与领域知识以保证模型的可解释性。

1.2.2 基于李雅普诺夫稳定性的攻防有效性判定

动力学模型能够追踪认知的演化轨迹, 却无法评价演化方向的优劣。为此, 本节引入李雅普诺夫稳定性理论, 建立攻防有效性的形式化判据。

在网络空间攻防博弈中, 防御方的根本目标是推动系统朝向安全可控的理想状态收敛, 攻击方则相反。从控制论的视角看, 这正是一个典型的动态系统稳定性问题: 一个策略的有效性, 等价于它能否驱使系统从当前的高熵对抗状态, 渐近稳定地收敛至期望的低熵目标状态。李雅普诺夫稳定性理论为分析此类问题提供了理想工具^[33-34]; 对于动态系统, 若存在一个满足正定条件的标量函数 V , 且 V 沿系统轨迹的差分始终为负, 则无须显式求解系统的演化方程, 即可判定该系统是渐近稳定的。

第 1.1 节定义的攻击熵与防御熵恰好满足构造李雅普诺夫函数的全部条件。其一, 正定性—— $H_A(t)$ 和 $H_D(t)$ 均非负, 且除理想状态外, $H_A(t) > 0$ 和 $H_D(t) > 0$ 恒成立。其二, 其演化完全由动力学模型驱动——它们分别是动力学模型状态变量 $\theta_A(t)$ 和 $\theta_D(t)$ 的函数, 轨迹完全由动力学方程确定。因此, 攻击熵 $H_A(\theta_A(t))$

和防御熵 $H_D(\theta_D(t))$ 可分别构造为攻防双方的李雅普诺夫函数。基于此, 建立如下判定定理。

定理 1(攻防有效性判定定理) 对防御方而言, 策略序列 $\{d(t)\}$ 是有效的, 当且仅当存在有限时刻 T , 使得对所有 $t > T$, 李雅普诺夫函数 ($V_D(t) = H_D(\theta_D(t))$) 沿动力学轨迹单调递减并最终收敛至足够小的邻域内, 即:

$$\Delta V_D(t) < 0, \text{ 且 } V_D(t) < \delta \quad (8)$$

式中: $\Delta V_D(t) = V_D(t+1) - V_D(t)$; δ 为预设的收敛阈值, $\delta > 0$ 。

$\Delta V_D(t) < 0$ 的物理含义在于, 防御方的认知日益清晰(香农熵降低), 同时系统状态日益趋近期望的安全目标(KL 散度降低); 反之, 若防御方的干预无法使 $V_D(t)$ 趋于收敛, 则该策略在数学上被判定为无效。

1.3 内嵌熵控逻辑的攻防博弈推演框架

攻击熵与防御熵为博弈态势提供了度量标尺, 动力学模型与判定定理为策略评价提供了理论准则。然而, 在多域融合、高度不确定的对抗条件下, 攻防双方如何基于有限观测动态生成博弈策略, 仍需系统化的机制设计。本节提出内嵌熵控逻辑的攻防博弈推演框架以解决该问题。

1.3.1 层次化博弈推演模型

多域融合攻防博弈的复杂性, 源于其同时涉及两种性质迥异的动态过程: 一是攻防博弈的阶段推进^[35]——攻击方从侦察、渗透到目标达成的阶段跃迁, 防御方从监测、识别到响应恢复的阶段应对; 二是各阶段内部系统状态、观测与攻防动作之间的微观交互^[36]。为刻画这两种动态特性, 本文采用基于双层概率图模型的层次化博弈推演模型。

定义6(层次化博弈推演模型) 该模型由宏观层与微观层构成。

宏观层将攻防博弈的推进过程抽象为阶段间的转移,以马尔可夫决策过程(MDP)建模:状态空间 S 为博弈各阶段的集合,以 k 表示阶段序号,转移概率 $P(s_{k+1}|s_k)$ 刻画攻防博弈的阶段跃迁规律。例如,阶段可依次对应攻击方的侦察探测、武器化与投送、攻击利用与渗透,以及防御方的检测识别、阻断响应、恢复巩固与溯源反制等攻防对抗的不同进程。每一阶段 $s_k \in S$ 对应一组攻防动作空间 $A_A(s_k)$ 和 $A_D(s_k)$,为微观层的策略生成提供阶段相关的动作约束。

微观层针对每一阶段 s_k ,构建动态贝叶斯网络(DBN)刻画时刻 t 到 $t+1$ 的状态演化。DBN节点包括系统状态 $X(t)$ 、攻防动作 $a(t)$ 和 $d(t)$ 、攻防双方的观测 $O_A(t)$ 和 $O_D(t)$ 。条件概率分布 $P(X(t+1)|X(t), a(t), d(t))$ 刻画状态演化不确定性, $P(O_A(t)|X(t))$ 和 $P(O_D(t)|X(t))$ 刻画观测不确定性。 $P(a(t)|O_A(t))$ 和 $P(d(t)|O_D(t))$ 刻画双方策略选择的不确定性。

宏观层与微观层通过以下机制耦合:每一阶段 s_k 的动作空间 $A_A(s_k)$ 和 $A_D(s_k)$ 限定了微观DBN中攻防动作的可选范围;微观层中攻防行为驱动系统状态 $X(t)$ 演化,当演化结果触及预设的阶段跃迁条件时,宏观MDP从阶段 k 转移至 $k+1$ 。该混合模型将博弈过程的阶段转移结构与不确定性刻画统一到同一个框架中,为攻防博弈推演提供了可计算的环境基座。

图4为该模型的层次化结构示意。微观层DBN中的向量节点在图4中以单个节点示意。实际建模时,各向量需以分量为节点展开,且分量间可能存在依赖关系,具体结构由建模场景决定,本文不做细化规定。

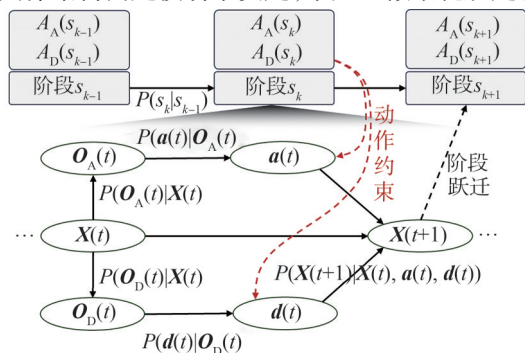


图4 层次化博弈推演模型

Fig. 4 Hierarchical game-theoretic reasoning model

1.3.2 多智能体博弈策略生成

在层次化博弈推演模型的基础上,攻防双方的博弈推演问题转化为:如何基于各自有限且带噪的观测,动态更新对系统状态和对手策略的信念,并据此生成自适应博弈策略。双方策略处于相互适应的动态

循环之中,防御策略的调整会引发攻击行为的相应变化,反之亦然。这种“行动—反应—再行动”的对抗本质,决定了任何一方的策略优化都不能在静态环境中完成,而必须在与对手的持续博弈中动态演进。因此,本节提出多智能体博弈策略生成方法:攻防双方各为一个独立智能体,每个智能体内嵌对手镜像模型,运行“信念更新—对手推演—策略选择”的3步决策流程,并通过层次化博弈推演模型进行交互。以下以防御方智能体 G_D 为例,阐述其内部决策流程。

步骤1:信念更新。 G_D 基于当前观测 $O_D(t)$,利用动力学模型对信念分布参数 $\theta_D(t)$ 进行递推更新,获得更新后的信念分布 $F_D(t)=P(X(t); \theta_D(t))$ 。这一更新综合了先验知识与最新观测信息,为后续的对手推演和策略决策提供了更准确的认知基础。

步骤2:对手镜像推演。 G_D 在自身的认知框架下,构建对攻击方智能体 G_A 的镜像推断模型,模拟 G_A 的认知过程与决策逻辑,推断 G_A 所持信念 $\hat{F}_A(t)$ 及其可能行动 $\hat{a}(t)$ 的概率分布。这一步骤同时服务于双向熵控:一方面,准确的镜像模型降低了防御方对对手行为的认知不确定性;另一方面,为计算防御方视角下的攻击熵值变化 ΔH_A 提供了信息基础。

步骤3:熵控策略选择。 G_D 基于步骤1的更新信念 $F_D(t)$ 和期望目标 F^+ ,以及步骤2对攻击方的推断结果,依据定义3的优化目标,在降低己方防御熵与增加对手攻击熵之间取得权衡,选择当前最优行动 $d(t)$ 。

攻击方智能体 G_A 与防御方智能体 G_D 并行运行对称的决策流程,它们各自独立维护自身信念与对手镜像模型,通过层次化博弈推演模型中的攻防行为交互影响系统状态,共同驱动推演进程的持续演化。对防御方而言, G_A 的存在为 G_D 提供了真实的博弈对手,使得 G_D 的策略在博弈中不断优化。两者在持续的攻防迭代中构成对抗训练闭环,螺旋上升。这一机制构成了多智能体博弈的核心运行框架。

上述策略选择的每一步并不显式验证定理1的条件,但二者存在内在一致性:定义3的优化目标旨在每一步推动 H_D 下降、 H_A 上升,其长期累积效果正是促使能量函数 $V_D(t)$ 沿动力学轨迹单调递减,从而满足定理1的渐近稳定性条件。定理1由此承担了层次化博弈推演模型中宏观阶段跃迁的判据角色:当满足收敛条件时,当前阶段的防御目标宣告达成,驱动宏观层阶段跃迁,博弈进入下一阶段;反之,则需在阶段内继续迭代推演与策略优化。

需要指出的是,定义2中的权衡系数、定义3中的意愿系数和定理1中的收敛阈值,共同构成了理论框

架中可调节的关键参数。它们的取值取决于决策者当前所处的攻防态势与风险偏好：在紧急响应场景中，可增大权衡系数和意愿系数以优先确保自身态势收敛，并设定较低的收敛阈值以快速判定防御成效；在主动反制场景中，可减小意愿系数以侧重增敌之熵的评估。上述参数的具体选取属于理论框架的应用层问题，可结合具体场景通过专家经验、历史基线或数据驱动方法确定，本文不做细化规定。

综上，本章以熵为核心，构建了熵变驱动新范式的理论内核，将“降己之熵、增敌之熵”从定性原则落实为可度量、可推演、可判定的理论体系，并将其贯通于策略生成流程，完成了从抽象原理到生成机制的闭环。

1.4 数值推演实验

1.4.1 实验设计与场景设定

为验证理论框架在工程实例中的可落地性与相对于现有方法的理论优势，以区域电网调度控制中心的多域融合安全防护为场景，开展数值推演实验。

1) 场景设定

假设攻击方通过电力无线专网(230 MHz频段)实施电磁压制，同时向调度数据网注入伪造 IEC 61850 MMS 控制指令，试图诱导调度员执行误操作，形成多域联动的复合渗透态势。防御方融合 4 类异质信息：物理域同步相量测量装置采集的母线电压频率偏差 Δf 、电磁域频谱监测设备的信噪比(SNR，记为 r_{SN})、网络域流量探针采集的 SCADA 系统心跳包丢包率(PLR，记为 r_{PL})、认知域由调度员操作工作站审计终端的响应时延(DLY，记为 t_{DLY})。各属性原始观测值基于 Min-Max 标准化方法映射至无量纲状态空间[0,1]，获得归一化状态向量 $\mathbf{X}=(X_1, X_2, X_3, X_4)$ 。各分量与属性的对应关系及归一化映射函数如表 1 所示。

表 1 四域状态属性归一化映射

Tab. 1 Normalized mapping of four-domain state attributes		
属性	原始量范围	归一化函数
Δf	[-0.10,0.10] Hz	$X_1=(\Delta f+0.10)/0.20$
r_{SN}	[0,50] dB	$X_2=r_{\text{SN}}/50$
r_{PL}	[0,30%]	$X_3=r_{\text{PL}}/0.30$
t_{DLY}	[0,30] s	$X_4=t_{\text{DLY}}/30$

依据层次化博弈推演模型，宏观层将当前的博弈阶段判定为“攻击利用与阻断响应阶段”(该阶段记为 s_k)。该阶段由前期侦察与渗透阶段演化而来，其动作空间为：防御方 $A_D(s_k)=\{d_1, d_2, d_3\}$ ，其中， d_1 为启用流量清洗规则阻断伪造控制指令， d_2 为提升发射功率并启用冗余通道， d_3 为维持当前配置；攻击方 $A_A(s_k)=$

$\{a_1, a_2\}$ ，其中， a_1 为持续电磁压制， a_2 为注入伪造控制指令。微观层在该阶段内部执行单步状态推演，从初始观测时刻 t_0 到策略执行后预测时刻 t_1 的熵变。

2) 实验目标

本实验设置两类验证目标，展示理论框架的核心能力：

a. 统一度量能力(定义 2)：验证攻击熵/防御熵能否将多源异质的不确定性压缩为单一可比较标量；

b. 跨域对抗认知能力(定义 1、3、5)：验证多域耦合与镜像推演的协同能否超越仅依赖单域自我感知的传统方法。

此外，基于推演结果演示层次化博弈推演模型中微观层与宏观层的闭环耦合机制(定义 6、定理 1)。

3) 对比基线

为验证上述理论优势，设置两类基线：

a. 基线 A(无跨域耦合推演)执行与本文相同的信念更新与熵计算流程，但在状态转移模型中令所有跨域耦合系数 C_{ij} 为 0，仅保留域内漂移项，用于检验忽略域间传导是否导致策略误判。

b. 基线 B(传统单域阈值告警)仅部署网络域心跳丢包率单阈值规则，触发后由值班调度员人工研判处置，未执行多域信息融合、对手镜像推演和跨域不确定性演化，代表局部感知、经验响应的模式。

4) 前提假设与参数设定

本节基于以下前提假设：各域状态分量服从高斯分布且相互独立(协方差矩阵为对角阵)，即信念分布属于高斯参数化族 $F(\mathbf{X}; \boldsymbol{\theta})$ ，其中， $\boldsymbol{\theta}=(\boldsymbol{\mu}, \boldsymbol{\sigma}^2)$ 为均值-方差参数向量。该假设使得贝叶斯更新、KL 散度和香农熵计算均具有解析或半解析解，单步计算复杂度为 $O(n)$ (n 为状态维度)。攻防双方的期望分布 F^- 和 F^+ 同样采用高斯参数化，以确保 KL 散度项的闭式可计算性。

取权衡系数 $\lambda_A=\lambda_D=0.5$ ，表示攻防双方对认知不确定性目标偏离的相对重视程度取均衡值；偏好系数 $\gamma=0.6$ ，表示防御方对“降己之熵”的权重略高于“增敌之熵”。对手镜像模型预估攻击方选择 a_1 为首要动作(概率 0.65)，选择 a_2 的概率为备选动作(概率 0.35)。其他实验参数详见附录 A 表 A1~A5。

1.4.2 实验结果与对比分析

1) 统一度量能力

基于初始观测，防御方获得后验信念 $F_D(t_0)$ ，镜像推断获得攻击方信念 $F_A(t_0)$ (过程数据见附录 A 表 A6~A9)。依据定义 2 及实验设定($\lambda_A=\lambda_D=0.5$)，在各属性独立假设的前提下，联合熵与联合 KL 散度可分解为各维度之和，计算得初始时刻 t_0 的攻击熵与防御熵，结果见表 2。

表 2 初始时刻的攻击熵与防御熵

Tab. 2 Attack entropy and defense entropy at initial moment

分量	$H(F_D)/$ bits	$D_{KL}(F_D F^+)/$ bits	$H(F_A)/$ bits	$D_{KL}(F_A F^-)/$ bits
X_1	4.607 1	3.892 5	5.208 1	7.962 3
X_2	6.310 1	6.952 4	6.684 2	1.284 8
X_3	4.690 2	10.057 5	5.471 1	16.665 7
X_4	6.523 7	2.313 6	6.643 2	2.545 1
总计	22.131 2	23.216 0	24.006 5	28.457 9

由表 2 总计可得:防御熵 $H_D(t_0)=22.67$ bits,攻击熵 $H_A(t_0)=26.23$ bits。该结果验证了熵度量体系的核心功能:将物理、电磁、网络、认知四域的多源异质不确定性(单位为 Hz、dB、%、s)压缩为单一可比较的数学标尺(单位为 bits)。表 2 同时展示了各域对总熵值的贡献差异,例如网络域 X_3 的 KL 散度在攻防双方均为四域中最高,反映出该域是当前态势偏离安全目标的最显著环节。

2)跨域耦合的必要性

为验证定义 5 所述跨域不确定性传导的结构性影响,在相同初始态势下,对 3 种防御策略分别进行完整推演与无跨域耦合推演(基线 A),所得的预期防御熵变化值见表 3(推演过程的中间结果详见附录 A 表 A10~A12)。

表 3 与基线 A 的策略对比

Tab. 3 Strategy evaluation with Baseline A

防御策略	本文方法熵变/bits	基线 A 熵变/bits
d_1	+0.085 4	-9.696 7
d_2	-7.282 7	-8.139 7
d_3	+58.776 7	+20.824 0

由表 3 可见,基线 A 预测 d_1 使防御熵下降 9.70 bits,将其误判为最优策略;然而本文方法的完整推演表明, d_1 实际使防御熵微增 0.09 bits,两者偏差达 9.78 bits。该差异源于 d_1 仅执行了网络域局部过滤,缓解了伪造指令的表面症状,但未对电磁域发射功率做任何调整,攻击方的电磁压制持续通过跨域耦合向网络域和认知域传导不确定性。忽略跨域耦合项,防御方将系统性的跨域风险误判为局部改善,产生策略假收敛。

对于 d_2 ,无耦合方法预测防御熵下降 8.14 bits,看似优于本文方法的 7.28 bits,但两者偏差仅 0.86 bits,属于无耦合方法对残余耦合效应的过度乐观估计。对于 d_3 ,无耦合方法预测防御熵增加 20.82 bits,而本文方法实际为 58.78 bits,偏差高达 37.95 bits,反映出无耦合方法严重低估了跨域传导的级联恶化效应。

3)多域对抗博弈优于单域自我修复

为验证多域耦合与镜像推演协同产生的整体优

势,将本文方法与基线 B(传统单域阈值告警)对比。在相同初始态势下,基线 B 依据网络域心跳丢包率超过阈值触发告警,由值班调度员人工研判后执行局部处置,如端口重启。基线 B 执行后的系统状态是基于模型假设的推演:设定值班调度员处置后 X_3 的均值降至 0.20, X_1 、 X_2 、 X_4 因未处置而按无动作条件继续推演(与 d_3 的推演结果一致),详见附录 A 表 A13。两种方法下的防御熵变化见表 4,其中,基线 B 的熵值基于上述推演值计算得到。

表 4 与基线 B 的策略对比

Tab. 4 Strategy comparison with Baseline B

方法	$H_D(t_1)$	ΔH_D	$H_A(t_1)$	ΔH_A
本文方法	15.390 9	-7.282 7	82.179 3	+55.947 1
基线 B	49.150 4	+26.476 8		

基线 B 使防御熵从 22.67 bits 恶化至 49.15 bits,增幅 26.48 bits;本文方法使防御熵降至 15.39 bits,降幅 7.28 bits,同时攻击熵升至 82.18 bits,增幅 55.95 bits。两种方法的差距并非单一因素所致:

其一,传统方法不考虑跨域耦合。端口重启仅处置网络域表象,电磁域的干扰通过跨域通道持续向其他域传导,最终导致全局失控。结果 2 已独立验证:忽略跨域耦合将导致策略假收敛误判,跨域耦合是态势推演的结构性必需。

其二,传统方法不考虑对手模型。其决策框架以恢复自身指标为唯一目标,策略选择始终自我中心的、单维度的。本文方法通过镜像推演,赋予防御方一个对手模型,使其能够在策略优选阶段预估候选动作对攻击方认知状态的扰动,并将其纳入定义 3 的优化目标进行综合权衡。基线 B 因缺乏镜像模型,其决策空间天然缺失“增敌之熵”的评估维度——它无法估计攻击方信念分布,因而不能计算攻击熵,更无法将其纳入策略评估。

4)层次化博弈的阶段贯通机制

本案例的攻防博弈在层次化博弈推演模型(定义 6)中展开,包含两个层次。宏观层将当前博弈判定为“攻击利用与阻断响应阶段”阶段,其动作空间已在第 1.4.1 节中界定。微观层的推演遵循 DBN 所定义的不确定性认知框架,通过状态节点、观测节点与动作节点间的概率依赖关系,将攻防博弈中分散的不确定性来源统一编码为结构化的条件概率结构,为推演提供了“应计算什么、以什么为条件”的结构蓝图。需要指出的是,虽然本实验中的实际计算由解析公式完成,但这些解析解可视为 DBN 推理在特定参数化假设(高斯独立分布、线性漂移函数)下的等价实现。在更一般的场景中,若解析公式不再适用,此时 DBN 的概率推理算法将成为推演的核心计算引擎,直接基于条件概率依赖关系执行信

念更新与状态预测。

在上述两层结构下,微观层在阶段 s_k 内部完成了一轮从信念更新、对手镜像推演到状态演化推演与策略选择的完整推理周期,并选定 d_2 为最优防御策略,预期使防御熵降低 7.28 bits。这一推演结果向宏观层传递了明确的量化信号,防御熵在所选策略下呈现单调递减态势。在此基础上,宏观层的阶段跃迁决策取决于防御熵是否满足定理 1 的收敛条件, $V_D(t_1)=15.39$ bits 若已满足 $V_D(t)<\delta$,则判定当前阶段的防御目标已达成,驱动博弈从“攻击利用与阻断响应阶段”跃迁至后续阶段(如“恢复巩固阶段”);若尚未满足收敛条件,则微观层将继续基于更新后的信念执行下一轮推演——或展开多步前瞻以观察累积效果,或在实际执行策略后基于新观测更新信念并重新判定,直至收敛。

上述过程实例化了宏观层状态演变由微观层判定结果驱动的耦合机制:宏观层定义阶段边界与动作约束,微观层承载概率推理与策略优选,定理 1 将微观层的熵变评估转化为宏观层的跃迁判据。两个层次协同,构成了度量、推演、判定、跃迁的决策闭环。

2 新范式指导下的安全体系构建

2.1 体系构建的熵控方法论

传统安全体系建设多遵循“威胁驱动”或“合规驱动”的路径——前者根据已知威胁部署防护措施,后者依据安全标准逐项达标——其共同局限在于将安全视为静态的、可穷举的防护对象集合,无法应对多域融合对抗中不确定性的动态演化。新范式将这一逻辑调整为“熵控驱动”:安全体系构建的根本目标不是封堵所有已知威胁,而是建立一套能够持续感知、度量和调控策略有效性和认知不确定性的运行机制,使己方能够将自身熵值控制在较低水平,同时迫使对手处于高熵的困境中。

这一方法论可沿“道、法、术、器”4个层次逐级展开。道即核心理念,确立“多域融合,熵变驱动”的根本指导思想:以多域融合为构建安全体系的基本途径,以熵变驱动为认知和决策的核心机制。法即构建法则,包含两项基本原则:其一,异构冗余——通过在物理、网络、认知等多域部署功能等价但结构异构的防御组件,降低共模失效的系统性风险;其二,动态反馈——以攻击熵/防御熵为度量标尺,以定理 1 的判定条件为收敛准则,构建“度量—推演—决策—执行—评估”的闭环运行机制。术即关键技术,涵盖多域态势感知、跨域联动响应、智能策略生成等支撑体系运行的方法集群,其共同特征是以熵控逻辑取代传统的规则匹配逻辑。器即工具平台,包括仿真推演环境、自动化编排引擎、量化评估系

统等工程载体,为熵控方法的落地提供可计算、可验证的技术底座。

2.2 防御形态的演进:从“杀伤链”到“杀伤网”

新范式的熵控视角,为理解网络空间防御形态的演进提供了深刻洞见。传统防御体系多围绕“杀伤链”概念组织——将攻击过程分解为侦察、武器化、投送、利用、安装、指挥控制、目标达成等线性阶段,防御方在每一阶段部署对应阻断措施^[37]。这种线性架构在早期单域对抗中行之有效,但在多域融合条件下暴露了结构性缺陷:任一环节的阻断失败即可导致全链崩溃,且攻击者可轻易变换路径绕过固定防线。从熵的视角看,杀伤链架构将防御资源集中于少数预设的攻击路径上,一旦攻击沿未预设的路径推进,防御方的认知不确定性将急剧上升,防御熵迅速失控。

新范式推动防御形态从“杀伤链”向“杀伤网”演进。杀伤网不再将防御资源固化为若干单一路径上的阻断点,而是将各域传感器、决策节点、响应单元构成动态可重构的网络^[38]。当攻击行为发生时,防御方基于层次化博弈推演模型和多智能体策略生成方法,实时评估不同响应方案对攻击熵和防御熵的预期影响,选择最优防御组合。在这一架构下,局部防线被突破不再意味着全局失效——杀伤网通过多路径冗余与动态重构,将攻击者的每一次推进都置于多域交叉验证之下,抵御了熵的急剧攀升,并将不确定性重新抛回攻击方。由此,杀伤链到杀伤网的演进,不仅是一种架构升级,更是熵控逻辑从被动应对到主动塑造的范式跃迁。

3 结论与展望

针对网络空间多域融合对抗中不确定性难以统一度量与系统性管控的理论瓶颈,提出了“熵变驱动的网络空间多域融合智能安全”新范式,并构建了其核心理论体系。该体系以熵为核心标尺,构建了度量、演化与判定、博弈推演 3 项协同的理论框架——以攻击熵与防御熵的度量体系为认知与决策提供可计算的标尺,以跨域不确定性动力学模型与攻防有效性判定定理为策略演化与评价提供数学准则,以内嵌熵控逻辑的多智能体博弈推演框架为不确定性条件下的自适应决策提供系统化方法论——将“降己之熵、增敌之熵”从定性原则转化为可度量、可推演、可判定的理论体系。在此基础上,确立了“多域融合,熵变驱动”的安全体系构建理念,并以熵控逻辑重新阐释了防御形态从“杀伤链”向“杀伤网”演进的深层机理。

本文的工作属于理论框架构建与概念体系论证,其重点在于提出新范式的核心思想并建立自洽的理论体系。然而,该理论体系落地到实际应用,仍需正视

3个层面的可计算性与可操作性问题:

1)信念分布的参数化与熵计算的可解性。熵度量的前提是将攻防双方的认知状态形式化为信念分布。这一过程的可计算性,取决于信念分布是否可被合理参数化,以及参数化后的香农熵与KL散度是否可解。对于连续型状态变量,高斯参数化提供了解析解,计算效率高;对于离散型状态或高维联合分布,熵的精确计算可能面临离散化误差或维数灾难,需引入变分推断、蒙特卡洛采样等近似方法,并在精度与效率之间做出折中。

2)动力学模型的结构辨识与参数获取。跨域不确定性动力学模型的核心是漂移函数与耦合矩阵。这两类函数的具体形式决定了模型的适用性:对于物理机理清晰的场景,可通过机理建模确定其结构;对于机理不清但数据丰富的场景,可采用数据驱动方法进行辨识;对于机理部分已知的场景,则需结合机理约束与数据学习进行混合建模。此外,如何量化模型不确定性对策略评估的传导影响,也是提升可操作性的关键。

3)博弈推演的实时性与策略空间的可扩展性。层次化博弈推演将攻防决策分解为宏观阶段转移与微观策略推演。当状态维度扩展至数十维、动作空间扩展至数十个候选策略时,跨域耦合预测的复杂度随状态维度呈平方数增长,推演实时性将面临挑战。高维场景下需引入稀疏近似、分层剪枝或启发式搜索等加速策略,在推演精度与实时性之间取得平衡。此外,镜像模型在多智能体博弈实践中如何通过对抗训练收敛至对手的真实决策逻辑,也是博弈推演框架从仿真走向实战的关键。

上述3个问题共同界定了熵变驱动理论体系在当前阶段的适用空间,突破这些边界,将推动新范式向更广泛的领域扩展,实现从理论构建到规模化应用的跨越。

附录见本刊网络版,扫描标题旁的二维码可阅读网络全文。

参考文献:

- [1] 国家互联网信息办公室. 国家网络空间安全战略[EB/OL]. (2016-12-27)[2026-05-14]. https://www.cac.gov.cn/2016-12/27/c_1120195926.htm from=timeline.
- [2] Zhang Yunxiao, Malacaria P. Dealing with uncertainty in cybersecurity decision support[J]. *Computers & Security*, 2025, 148: 104153.
- [3] Simpson A. Into the unknown: The need to reframe risk analysis[J]. *Journal of Cybersecurity*, 2024, 10: tyae022.
- [4] Alavizadeh H, Jang-Jaccard J, Enoch S Y, et al. A survey on cyber situation-awareness systems: Framework, techniques, and insights[J]. *ACM Computing Surveys*, 2023, 55(5): 1-37.
- [5] Gong Jian, Zang Xiaodong, Su Qi, et al. Survey of network security situation awareness[J]. *Journal of Software*, 2017, 28(4): 1010-1026. [龚俭, 臧小东, 苏琪, 等. 网络安全态势感知综述[J]. *软件学报*, 2017, 28(4): 1010-1026.]
- [6] Cho D X, Nguyen T T. A novel approach for APT attack detection based on an advanced computing[J]. *Scientific Reports*, 2024, 14: 22223.
- [7] Wang Zhiwei, He Xijie, Yi Xin, et al. Survey of attack and detection based on the full life cycle of APT[J]. *Journal on Communications*, 2024, 45(9): 206-228. [王郅伟, 何晞杰, 易鑫, 等. 基于APT活动全生命周期的攻击与检测综述[J]. *通信学报*, 2024, 45(9): 206-228.]
- [8] Duan Yancui, Cai Yonghua, Wang Zhikang, et al. A novel network security risk assessment approach by combining subjective and objective weights under uncertainty[J]. *Applied Sciences*, 2018, 8(3): 428.
- [9] Wu Jiacheng, Yu Xiao. A review of research on cybersecurity risk assessment methods[J]. *Electronic Science and Technology*, 2024, 37(3): 10-17. [吴嘉诚, 余晓. 网络安全风险评估方法研究综述[J]. *电子科技*, 2024, 37(3): 10-17.]
- [10] Wu Junlin, Kamhoua C, Kantarcioglu M, et al. Learning generative deception strategies in combinatorial masking games[C]// *Decision and Game Theory for Security*. Cham: Springer, 2021: 98-117.
- [11] Zhang Tao, Xu Changqiao, Shen Jiahao, et al. How to disturb network reconnaissance: A moving target defense approach based on deep reinforcement learning[J]. *IEEE Transactions on Information Forensics and Security*, 2023, 18: 5735-5748.
- [12] Slusher M N. Lessons from the Ukraine conflict: Modern warfare in the age of autonomy, information, and resilience: [R]. Washington D C: Center for Strategic and International Studies(CSIS), 2025.
- [13] National Institute for Defense Studies (Japan). Future of Multi-domain Operations and Campaigning: lessons for the Indo-Pacific[R]. Tokyo: NIDS, 2025.
- [14] Huang Mengyu, Tsang K F E, Li Yuzhe, et al. Strategic DoS attack in continuous space for cyber-physical systems over wireless networks[J]. *IEEE Transactions on Signal and Information Processing Over Networks*, 2022, 8: 421-432.
- [15] Chen Jun, Sun Xin, Tian Wen, et al. A Bayesian game approach for node-based attribution defense against asymmetric information attacks in IoT networks[J]. *PLoS One*, 2025, 20(3): e0316091.
- [16] Wu Dandan, Chen Jie, Xie Ruiyun, et al. OntoCSD: An ontology-based security model for an integrated solution of cyberspace defense[J]. *Frontiers of Information Technology & Electronic Engineering*, 2024, 25(9): 1209-1225.
- [17] Tang Wei, Liu Yujun, Chen Yuling, et al. SLBRS: Network virus propagation model based on safety entropy[J]. *Applied Soft Computing*, 2020, 97: 106784.
- [18] Liu Ke, Wang Mufeng, Ma Rongkuan, et al. Detection and localization of cyber attacks on water treatment systems: An entropy-based approach[J]. *Frontiers of Information Technology & Electronic Engineering*, 2022, 23(4): 587-603.
- [19] Siddiqui E F, Haleem M, Ahmad S F, et al. A multi-layered

- AI-driven cybersecurity architecture: Integrating entropy analytics, fuzzy reasoning, game theory, and multi-agent reinforcement learning for adaptive threat defense[J]. IEEE Access, 2025, 13: 170235–170257.
- [20] Li Rui, Zhang Luqiao, Li Haifeng, et al. Survey of entropy-based network traffic anomaly detection methods[J]. Computer Systems & Applications, 2017, 26(6): 36–39. [李蕊, 张路桥, 李海峰, 等. 基于熵的网络异常流量检测研究综述[J]. 计算机系统应用, 2017, 26(6): 36–39.]
- [21] Sinha M, Mukherjee J C, Bera P, et al. SynFloWatch: An entropy-based live defense system against SYN spoofing DDoS attacks in hybrid SDN[J]. Journal of Network and Systems Management, 2025, 33(4): 76.
- [22] Wang Miao, Wang Liming, Xu Zhen, et al. Research on DDoS detection in multi-tenant cloud based on entropy change[J]. Journal on Communications, 2016, 37(Z1): 204–210. [王淼, 王利明, 徐震, 等. 基于熵变的多租户云内 DDoS 检测方法研究[J]. 通信学报, 2016, 37(Z1): 204–210.]
- [23] Paik J Y, Jin Rize, Cho E S. Malware classification using a byte-granularity feature based on structural entropy[J]. Computational Intelligence, 2022, 38(4): 1536–1558.
- [24] Safaei F, Yeganloo H, Akbar R. Robustness on topology reconfiguration of complex networks: An entropic approach[J]. Mathematics and Computers in Simulation, 2020, 170: 379–409.
- [25] Yu Haiyun, Yang Xincun, Wang Liang. Network security situation prediction based on combining associated entropy and deep recurrent neural network[J]. Transactions on Emerging Telecommunications Technologies, 2022, 33(10): e4164.
- [26] Zhao Xiaolin, Guo Jiong, Jiang Xiaoyi, et al. Multi-layer network attack and defense model based on entropy method to measure network security[J]. Journal of Physics: Conference Series, 2019, 1302(2): 022068.
- [27] 饶志宏, 张志勇, 陈剑锋, 等. 一种基于熵的网络攻防不确定性度量计算方法: CN202410649771.7[P]. 2024–06–21.
- [28] Janani K. Cybersecurity through entropy injection: A paradigm shift from reactive defense to proactive uncertainty [PP/OL]. (2025–04–15) [2026–05–01]. <https://doi.org/10.48550/arXiv.2504.11661>.
- [29] Wu Jiangxing. Development paradigms of cyberspace endogenous safety and security[J]. Scientia Sinica (Informationis), 2022, 52(2): 189–204. [邬江兴. 网络空间内生安全发展范式[J]. 中国科学: 信息科学, 2022, 52(2): 189–204.]
- [30] Wu Jiangxing. Research on cyber mimic defense[J]. Journal of Cyber Security, 2016, 1(4): 1–10. [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.]
- [31] Ma Hailong, Wang Liang, Hu Tao, et al. Survey on the development of mimic defense in cyberspace: From mimic concept to “mimic+” ecology[J]. Chinese Journal of Network and Information Security, 2022, 8(2): 15–38. [马海龙, 王亮, 胡涛, 等. 网络空间拟态防御发展综述: 从拟态概念到“拟态+”生态[J]. 网络与信息安全学报, 2022, 8(2): 15–38.]
- [32] Ma Hailong, Ren Quan, Yi Peng. Modeling and quantitative evaluation of cyberspace mimic defense[J]. ZTE Technology Journal, 2022, 28(6): 57–62. [马海龙, 任权, 伊鹏. 网络空间拟态防御建模与量化评估技术研究[J]. 中兴通讯技术, 2022, 28(6): 57–62.]
- [33] Sontag E D. Mathematical control theory: Deterministic finite dimensional systems[M]. 2nd ed. New York: Springer, 1998.
- [34] Berkenkamp F, Turchetta M, Schoellig A P, et al. Safe model-based reinforcement learning with stability guarantees[C]// Proceedings of the Advances in Neural Information Processing Systems 30 (NeurIPS). Long Beach: Curran Associates, 2017: 6692.
- [35] Wang Qian, Wang Weilong, Wang Yan, et al. Multi-stage network attack detection algorithm based on Gaussian mixture hidden Markov model and transfer learning[J]. IEEE Transactions on Automation Science and Engineering, 2025, 22: 3470–3484.
- [36] Banda T V, Rens G B. Reinforcement learning of defensive strategies against attacks in partially observable local area networks[J]. Advances in Knowledge-Based Systems, Data Science, and Cybersecurity, 2025, 2(3): 337–374.
- [37] Hutchins E M, Cloppert M J, Amin R M. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains[C]// Proceedings of the Leading Issues in Information Warfare & Security Research. 2011, 1(1): 80.
- [38] Yang Yating, Zhu Quanyan. Toward a multi-echelon cyber warfare theory: A meta-game-theoretic paradigm for defense and dominance[EB/OL]. (2026–02–24) [2026–05–01]. <https://arxiv.org/abs/2509.08976>.

【校友简介】



饶志宏, 工学博士, 研究员, 中国电子科技集团有限公司总师召集人/首席科学家。于 1994 年取得四川大学本科学位, 曾在美国普渡大学做访问学者, 长期从事网络空间安全技术研究, 是中国网络空间多域融合智能安全领域学术带头人。获全国创新争先奖、国家“万人计

划”科技创新领军人才、首届国家网络安全先进个人。先后担任国家重点研发计划“网络空间安全”专项项目负责人、H863 计划电力系统安全技术专题首席科学家、863 计划和 973 计划专家, 在网络对抗、认知安全、监测预警和工业控制系统安全等方面取得系列成就, 创造了重大的社会效益和经济效益。获省部级一等奖 5 项 (均排 1) 等, 授权发明专利 70 余项, 出版学术专著 4 部、发表影响力论文 30 余篇。

Entropy Evolution-driven: A New Paradigm for Multi-domain Fusion Intelligent Cybersecurity

RAO Zhihong¹, ZHANG Zhiyong¹, CHEN Wu², HE Jianhui³, XU Ruoyu², LI Zhucheng¹, ZHAO Xin³, CHEN Jianfeng¹

(1.The 30th Research Institute of CETC, Chengdu 610041, China;

2.School of Cyberspace Security, Northwestern Polytechnical University, Xi'an 710072, China;

3.Electronic Science Research Institute of CETC, Beijing 100041, China)

Abstract:

Objective The essence of cyberspace security lies in attack-defense games under uncertainty, and the outcome of such games depends on the capability to characterize and control uncertainty. As cyberspace confrontation has extended from the network information domain to the physical domain, electromagnetic spectrum domain, and social cognition domain, uncertainty has increased significantly. The coupling among heterogeneous domains introduces new uncertainty sources and leads to cross-domain propagation and cascading amplification of uncertainty, making confrontation modeling and decision-making increasingly challenging. Traditional single-domain confrontation models are insufficient for characterizing such cross-domain uncertainty propagation. However, existing studies lack a unified uncertainty quantification framework that supports integrated modeling, reasoning, and decision-making for multi-domain fusion confrontation. This paper aimed to establish an entropy-evolution-driven intelligent cybersecurity paradigm, in which multi-domain fusion attack-defense games were characterized as dynamic entropy control processes.

Methods Within this framework, entropy was introduced as a unified mathematical metric for quantifying heterogeneous uncertainty across multiple domains, and entropy evolution was employed to characterize the dynamic variation of uncertainty states driven by attack-defense interactions. The attack and defense processes were modeled as bidirectional entropy control mechanisms, where both sides attempted to regulate entropy evolution toward favorable states by reducing their own entropy while increasing the opponent entropy. To characterize the uncertainty states underlying entropy evolution, the attack-defense game was modeled from a probabilistic perspective, where the cognitive states of both sides were represented by belief distributions over uncertain environments and opponent strategies. A dual entropy metric framework integrating attack entropy and defense entropy was constructed, where Shannon entropy and relative entropy were incorporated to quantify cognitive uncertainty and characterize attack-defense strategy effectiveness within a unified entropy-based metric framework. The resulting entropy representation provided a common state space for describing the uncertainty evolution of both attack and defense processes, enabling subsequent dynamic analysis and strategic reasoning. Based on the entropy metrics, a cross-domain uncertainty dynamics model was constructed to describe the propagation and amplification of uncertainty among heterogeneous domains under attack-defense interactions. A stochastic difference equation was formulated to characterize entropy evolution, where cross-domain coupling effects were incorporated to capture the cascading transmission of uncertainty. A formal criterion for attack-defense strategy effectiveness was further established through Lyapunov stability theory to evaluate the convergence and stability of entropy evolution under different strategies. This criterion provided a theoretical basis for distinguishing effective strategies from ineffective strategies according to their influence on entropy evolution trajectories. The entropy control logic was further embedded into a game-theoretic reasoning framework to support adaptive attack-defense strategy generation. A hierarchical game-theoretic reasoning model was employed as the underlying reasoning environment, integrating a macroscopic stage-transition model based on Markov decision processes and a microscopic behavior reasoning model based on dynamic Bayesian networks. Based on the dual entropy representation, a belief-driven multi-agent strategy generation method with symmetric opponent modeling was incorporated to characterize both-side cognitive states and generate adaptive strategies under uncertain conditions, forming a closed-loop process among belief updating, entropy evolution, and strategy generation. Through this mechanism, uncertainty quantification, game-theoretic reasoning, and adaptive strategy generation were integrated into a unified computational framework.

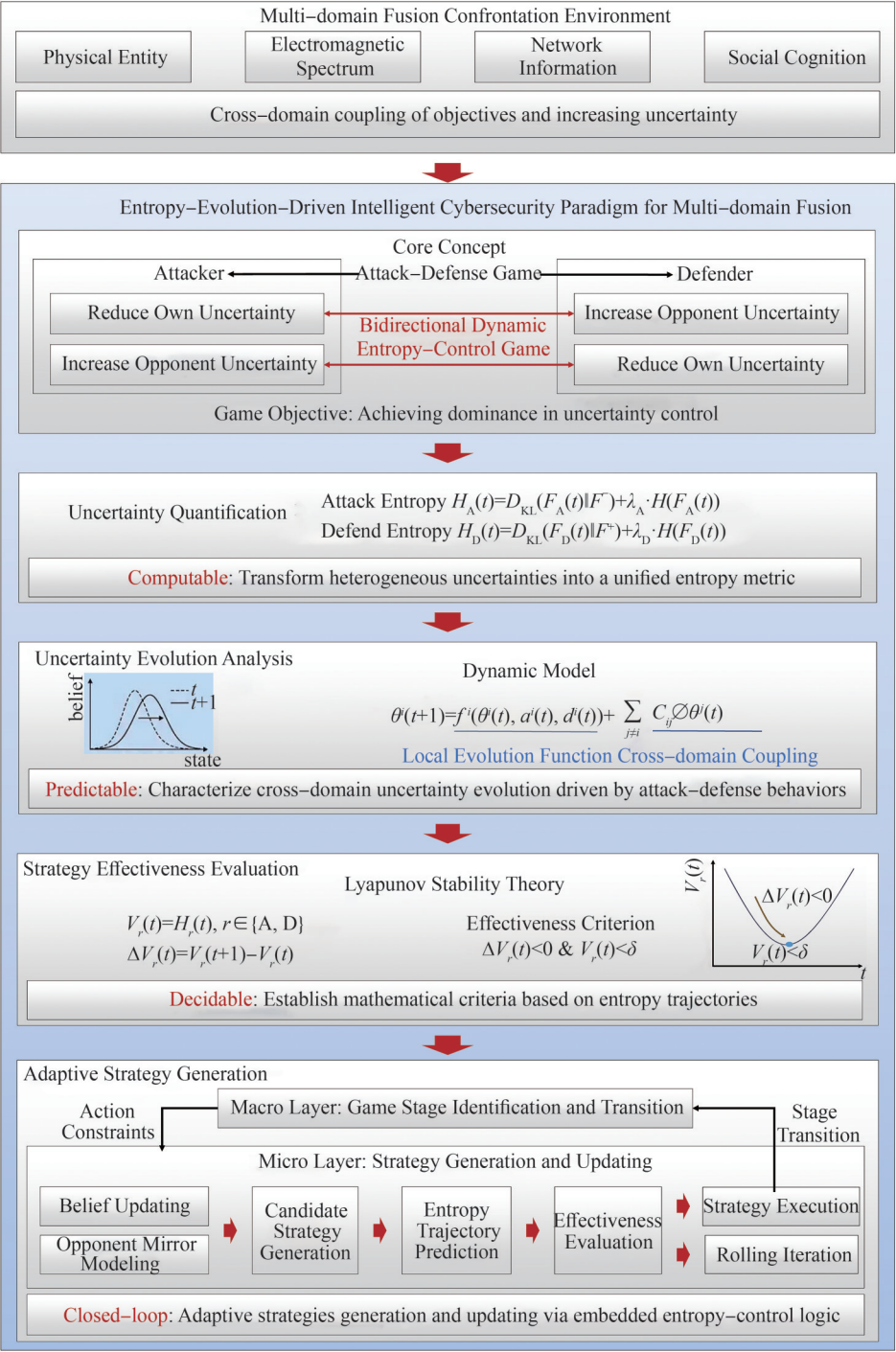
Results and Discussions Numerical reasoning simulations were conducted in a multi-domain security protection scenario of a regional power grid control center to validate the proposed entropy-evolution-driven framework. The results showed that attack entropy and defense entropy transformed heterogeneous uncertainties from the physical, electromagnetic spectrum, network information, and social cognition domains into comparable entropy representations. The analysis of cross-domain coupling effects demonstrated that ignoring uncertainty propagation among domains could lead to pseudo-convergence and misjudgment of strategy effectiveness. Compared with the uncoupled reasoning approach (Baseline A), the proposed method effectively captured the cascading amplification of uncertainty caused by cross-domain interactions and avoided the misjudgment of locally effective but globally ineffective strategies. Compared with the conventional single-domain threshold-based alerting approach (Baseline B), the proposed method enabled more effective defense decisions by integrating multi-domain information fusion, entropy-control objectives, and symmetric opponent modeling. Furthermore, the scenario reasoning demonstrated the closed-loop coupling mechanism between the microscopic-level reasoning process and the macroscopic-level stage transition process in the hierarchical game-theoretic model. The microscopic layer performed belief updating, opponent mirror modeling and reasoning, entropy evolution prediction, and strategy selection within the current confrontation stage, while the resulting entropy evolution provided quantitative criteria for macroscopic-level stage transition. This mechanism enabled the transformation from uncertainty quantification and strategic reasoning to decision-making and stage evolution, forming a unified computational loop for multi-domain fusion confrontation.

Conclusions The proposed paradigm establishes an entropy-evolution-driven framework for constructing multi-domain fusion cybersecurity architectures. Under this paradigm, defense evolution from kill-chain-oriented operations to kill-web-oriented architectures was interpreted through entropy control, where defensive effectiveness was achieved through coordinated regulation of uncertainty across multiple domains. By integrating entropy-based uncertainty quantification, dynamic modeling, and game-theoretic reasoning, the framework provides a mathematical basis for transforming cyberspace security decision-making from experience-dependent approaches toward computable paradigms. Future research will focus on improving the parameterization of belief distri-

butions and the tractability of entropy computation, advancing the structural identification and parameter acquisition of cross-domain uncertainty dynamics models, and enhancing the real-time scalability of game-theoretic reasoning with large strategy spaces.

Key words: cybersecurity; multi-domain fusion; entropy evolution driven; entropy control theory; attack/defense entropy; multi-agent game

Graphical abstract:



(编辑 吴芝明)

引用格式: Rao Zhihong,Zhang Zhiyong,Chen Wu,et al.Entropy evolution-driven: A new paradigm for multi-domain fusion intelligent cybersecurity[J].Advanced Engineering Sciences,2026,58(5):360–372.[饶志宏,张志勇,陈昨,等.熵变驱动的网络空间多域融合智能安全新范式[J].工程科学与技术,2026,58(5):360–372.]