专题：智能体通信与网络技术

面向6G智能体网络的行为安全协同架构

黄奥然，周华春，闫竟夫，范晓静
（北京交通大学电子信息工程学院移动专用网络国家工程技术研究中心，北京 100044）

摘　要：随着6G网络的演进，网络恶意行为呈现长期潜伏、持续渗透的特点，网络行为安全分析面临多路并行、证据分散、难以观察等挑战。针对6G网络中的行为安全防护需求，提出了“三层三域”多智能体协同网络架构。该架构分为感知层、编排层和执行层三大层级，并依托智能域、知识域、工具域的跨域协同，支撑网络行为安全分析的实现。在此基础上，给出了智能体与知识域、工具域交互的域通信协议，并结合A2A（agent-to-agent）协议，规范了多智能体协同开展网络行为安全分析的流程。最后以高级持续威胁（advanced persistent threat，APT）攻击场景下的攻击链构建任务作为网络行为分析实例，基于Clearscope-e3和Clearscope-e5数据集验证了所提架构能有效支撑6G智能体网络中的网络行为安全分析。

关键词：智能体网络；6G网络；网络行为；智能体通信协议；多智能体协同
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.DXKX260089

A collaborative behavior security architecture for 6G agent networks

Huang Aoran, Zhou Huachun, Yan Jingfu, Fan Xiaojing
National Engineering Research Center of Advanced Network Technologies, School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China

Abstract: With the evolution of 6G networks, malicious network behaviors are characterized by long-term lurking and persistent penetration. Accordingly, network behavior security analysis faces challenges such as parallel multi-path activities, fragmented evidence, and stealthy behaviors. To address the behavioral security protection requirements in 6G networks, a “three-layer, three-domain” multi-agent collaborative network architecture was proposed. This architecture was divided into three layers: the perception layer, the orchestration layer, and the execution layer. By leveraging cross-domain collaboration among the intelligence domain, knowledge domain, and tool domain, the implementation of network behavioral security analysis was supported. On this basis, a domain communication protocol for the interaction between agents and both the knowledge domain and the tool domain was specified. Together

收稿日期：2026−02−05；**修回日期：**2026−03−16
通信作者：周华春，hchzhou@bjtu.edu.cn
基金项目：国家自然科学基金资助项目（No.U2569201）；中央高校基本科研业务费资助项目（No.2025YJS015）
Foundation Items: The National Natural Science Foundation of China (No.U2569201), Fundamental Research Funds for the Central Universities (No.2025YJS015)

with the A2A protocol, a standardized workflow for multi-agent collaborative network behavioral security analysis was established. Finally, using the attack chain construction task under an advanced persistent threat (APT) attack scenario as an instance of network behavioral analysis, the effectiveness of the proposed architecture in supporting network behavioral security analysis in 6G agent networks was validated based on the Clearscope-e3 and Clearscope-e5 datasets.

Key words: agent network, 6G network, network behavior, agent communication protocol, multi-agent collaboration

0 引言

近年来，智能体在通信网络中的部署规模显著增长[1]，推动6G网络朝着通信、感知与智能相融合的方向演进[2]。多智能体协同可将复杂目标进行拆解，由专家智能体完成指定阶段的任务以适配网络业务需求，为6G网络赋予更灵活的扩展能力和更智能的编排能力[3]。受6G智能体网络异构部署、多阶段决策和去中心化协同等特征影响，其内部通信逐步从数据传输演进为需要依托通信网络支持的认知与意图交互。这种演进在提升网络智能水平的同时，也使传统依赖包级特征、流量统计和交互模式的方法难以有效识别网络行为，造成网络行为的可观测性降低、行为边界模糊化，导致恶意网络行为更容易在合法协同过程中长期潜伏并对网络安全形成持续性威胁[4]。

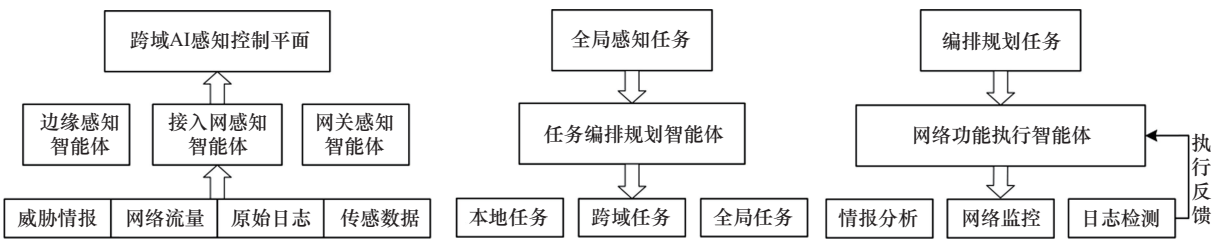
0.1 6G网络架构演进扩大了网络行为攻击面

3GPP TR 22.870[5]和TR 38.914[6]从用例和需求层面，阐述了原生智能、跨域协同、任务驱动等特性对6G网络智能感知、决策和执行能力的支撑作用。6G网络架构正从以连接和传输为核心，向以感知、编排和自主执行为核心的方向演进，可归纳为3类典型架构，如图1所示。

（1）跨域感知的6G智能体网络架构。该架构涵盖3GPP TR 22.870和TR 38.914中关于6G多源感知融合、环境重构等典型场景与用例。由于异构数据分布在边缘、接入网和不同自治域内，单一节点难以实现全局感知，因此，需要在靠近数据源处部署负责采集和预处理的智能体，作为6G网络智能感知的基础。同时，该架构引入大量长期暴露的交互接口，导致网络行为的攻击面显著扩大。

（2）任务驱动的跨域编排6G智能体网络架构。该架构覆盖了3GPP TR 22.870和TR 38.914中任务意图驱动的智能编排、多智能体协同决策、跨域协同等用例与需求。智能体须具备推理和全局能力，可根据网络任务实现本地、跨域和全局的智能编排，并对下游智能体进行调度和约束。然而，该架构也将攻击面可观测的网络行为融入智能推理过程中，为恶意行为提供了可隐藏的活动空间。

（3）网络功能执行的6G智能体网络架构。该架构对应3GPP TR 22.870和TR 38.914中关于自治执行、闭环控制、智能体执行动作等典型用例。该架构要求智能体具备自治执行能力，且关注执行的落地和效果，可在较少人工干预的条件下实现任务的执行、验证和动态调整。智能体受上层策略的约束，并向上反馈执行结果。在此架



（a）跨域感知的6G智能体网络　（b）任务驱动的跨域编排6G智能体网络　（c）网络功能执行的6G智能体网络

图1　3类典型6G智能体网络架构

构下，传统安全边界随之模糊，使得恶意行为更容易借助合法协同路径进行横向渗透。

不同类型的智能体承担着感知、编排和执行等功能互补且明确的任务，这与6G网络对感知智能、编排智能和执行智能的内生需求高度一致。这些层次化特征在推进6G智能体网络演进的同时，也扩大了恶意行为的攻击面并分散了特征，使其得以长期潜伏并成为常态化的威胁。

0.2　6G网络中网络行为安全保障面临新挑战

随着6G网络攻击面的逐渐扩大，恶意网络行为可以在合法行为的掩护下，沿多条路径长期潜伏并逐步扩展其威胁范围。这使得6G网络中的网络行为安全保障面临攻击路径多样、证据复杂、难以观测等挑战，传统单一、孤立的检测机制难以适用。6G网络演进过程中恶意网络行为的结构性来源如图2所示。

图2　6G网络演进过程中恶意网络行为的结构性来源

目前，抵御恶意网络行为的方法主要分为基于异常行为检测[7]和基于溯源分析的行为关联[8]两类。考虑到6G网络行为的复杂化趋势，基于异常行为检测的方法检测性能有限[9]。基于溯源分析的行为关联方法通过分析网络实体与事件之间的因果关联，能够更好地反映恶意网络行为在多路径并行潜伏、多阶段证据分散和长期低可观测性条件下的整体特征[10]。然而，6G网络中的异构智能导致网络行为分散在协同过程中，这种跨域、跨阶段的协同行为使得网络日志碎片化，实体与事件差异化，造成网络行为安全分析需要处理的网络日志数量激增，知识域构造复杂，前后文因果关联困难，从而增加了行为安全分析的难度[11]。因此，如何在6G智能体网络中实现对复杂网络行为的持续关联、协同分析与安全保障，成为亟待解决的问题。

0.3　多智能体协同为6G网络行为安全提供新的架构基础

面向6G的智能体网络为网络行为安全分析提供了新的解决方案[12]。6G智能体网络面向网络行为安全分析演进的动机、挑战与方案如图3所示。分布式智能体能够契合零散网络行为的处理需求，凭借智能体较强的上下文理解和推理能力，可从网络行为中提取威胁情报等相关信息。结合智能体本身的知识[13]，使其在网络行为安全分析的不同阶段具备相应的能力，实现跨域、跨阶段的协同分析。不过，这一目标的实现依赖于智能体之间持续且可控的协同交互，要求通信网络不仅能够支持数据传输，还需要具备对智能体目标、状态、上下文以及协同关系的表达与承载能力。

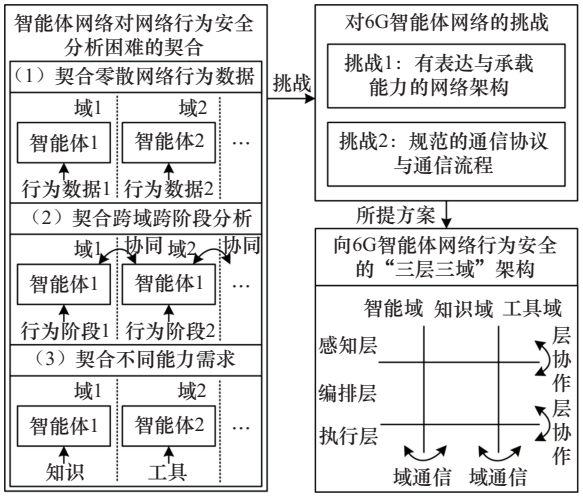


图3　6G智能体网络面向网络行为安全分析演进的动机、挑战与方案

现有以连接与会话为核心的传统网络难以满足这一需求，限制了多智能体在网络行为安全场景下的持续协同能力。面向6G智能体网络的网络行为安全需求，主要存在两个问题：（1）如何构建一种可融入6G网络的多智能体协同架构，使其能够在感知、编排和执行等层级上支撑复杂网络行为的协同分析；（2）如何规范多智能体通信协议和流程，明确任务驱动下智能体协同过程中的消息类型、上下文表达方式以及跨域协作流程，使多智能体协同成为6G网络的内在能力。

为此，本文从网络协议与智能体协同机制出发，面向6G智能体网络中的网络行为安全需求，提出了一种“三层三域”的多智能体协同网络架构。根据智能体在网络行为安全分析中的任务分工，结合现有6G智能体网络架构，抽象出感知层、编排层和执行层，并给出了各层级智能体之间的协同方式，以支撑网络行为安全分析。将智能体统一整合为智能域，并设置相应的知识域与工具域，设计了支持智能体按需获取知识和调用工具的域间通信协议，为多智能体在行为安全场景下的协同提供通信支撑。基于所提出的架构与通信机制，构建了一个完整的多智能体协同流程，明确了协同过程中所需的统一消息格式及关键消息类型。最后，以高级持续威胁（advanced persistent threat，APT）攻击场景下的攻击链构建任务作为一种典型网络行为安全分析实例，对所提多智能体协同网络架构与通信流程进行验证。

1 研究现状与基础

1.1 6G网络中智能体的融入

智能作为网络原生能力深度融入6G网络，推动网络智能由传统固定规则转向任务意图驱动。现有网络智能多通过学习特定的数据集获得，面对异构网络环境和复杂任务时，则难以有效落地应用。多智能体协同为6G网络侧智能在复杂场景和任务下的落地提供了可行路径，主流实现方法有去中心化、意图识别、任务感知等，为5G有限智能化向6G全面智能化演进[14]提供了支持。

去中心化智能为网络侧智能体提供了能够依据网络拓扑和动态负载落地的能力，使智能体能够下沉至网络边缘。文献[15]提出了一种去中心化执行的多智能体协作架构，有效提升了多智能体在移动网络场景中的时效性。文献[16]在去中心化多智能体架构基础上，提出了一种混合专家模型的框架，可以动态协调专家模型处理不同的通信任务。

对智能体在异构场景下的相关研究，促进了多接入、多链路与多自治域环境中的多智能体协同部署，为跨域编排与异构资源调度提供了网络侧落地支撑。文献[17]面向6G空天地一体化网络场景，设计了基于强化学习的智能体，使其能够根据不同场景完成拥塞控制决策。文献[18]考虑6G网络对车辆与异构实体互联的支撑需求，提出了一种基于注意力机制的多智能体方法，保障了异构场景下6G网络的时延可靠性。

智能感知与意图识别为智能体在网络层落地提供了标准化接口，使智能体能够通过统一的意图抽象对接网络管理与控制流程。文献[19]利用大语言模型（large language model，LLM）与上下文工具实现对多种网络设施的网络意图感知，完成6G网络配置冲突的协调与消解。文献[20]以LLM为核心，提出了一种基于意图的网络配置与管理方法，可对非结构化意图进行理解。

上述研究为智能体在6G网络中的部署与运行提供了重要支撑，验证了多智能体融入6G网络的可行性。然而，现有研究成果缺少对网络层和网络安全的关注，有必要将上述落地能力延伸到网络行为安全场景的跨域证据获取、协同分析与可复核输出中。本文所提的“三层三域”架构关注面向网络行为安全的多智能体协同机制，扩展了多智能体融入6G网络的新路线。

1.2　多智能体的协同

本文将智能体定义为智能的实体，可通过标准化消息进行交互，并调用工具和知识完成任务。其智能既可以来自传统神经网络，也可以依托LLM实现。多智能体协作模式主要分为3类：上下级协作[21]，即采用具备通用智能的核心智能体管控专用领域智能体以完成任务，文献[22]使用GPT作为大脑抽取语义信息进行协同，解决了通信数据冗余问题；同层级协作[23]，智能体间无明显的上下级控制关系，以对等身份开展协作，文献[24]提出一种区块链下分布式多智能体协作方法，实现了车辆调度场景下基础设施与边缘节点的负载均衡；竞争协作[25]，通过多智能体之间的竞争博弈完成任务目标，文献[26]将任务需求、智能体能力和性能指标进行整合，通过任务内和任务间竞争，实现了物联网场景中的最优任务匹配和资源分配。

实现上述3种协同模式的技术主要包括传统AI技术和大模型技术。其中，AI技术以强化学习应用最为广泛[27]，主要用于实现同级协作和竞争协作。各智能体在决策时，不仅要考虑自身收益，还需兼顾对其他智能体和整体的影响，开展协同决策[28]。大模型技术通常以LLM为核心构建上下级协作体系[29]，可以理解其他智能体的输入和输出，并基于整体需求去编排多智能体系统的协同方案。

6G网络中的多智能体协同需要考虑跨域通信、上下文关联等网络层问题，而现有协同算法研究忽略了其所依赖的网络架构和通信协议，对标准化通信方式、上下文表示以及通信协议的关注不足。现有的主流通信协议有：智能体网络协议（agent network protocol，ANP）、Agora、智能体交互与事务协议（agent interaction and transaction protocol，AITP）、模型上下文协议（model context protocol，MCP）与A2A（agent-to-agent）协议。ANP在开放网络下实现互联，支持跨域连接；Agora关注大规模智能体网络中的可扩展协作通信；AITP提供结构化交互与多方参与的协议框架。针对6G场景下安全分析中的跨域工具统一接入、任务交付等需求，这些协议仍需要额外的约束与支撑。MCP关注统一工具接口与上下文传递机制，A2A[30]则关注智能体之间的点对点与多点通信，二者更便于在“三层三域”架构中将工具域以标准化方式接入并支撑多角色智能体的协同调度。然而，却缺乏对知识增强的考虑，也未针对6G网络行为安全分析任务进行设计。本文在二者的基础上进行改进和利用，采用上下级协作模式，聚焦于网络架构的设置，借助通信协议和通信流程实现智能体对网络行为的安全分析。

1.3　智能体在网络安全领域中的应用

6G网络中攻击面的扩大，使得攻击者能够在网络中长期潜伏，并对薄弱环节发起攻击。传统单点式检测方案难以满足6G网络对安全问题进行多阶段推理和证据融合的要求。智能体技术提供分布式智能和跨域协同的支持，推动6G网络安全向智能化、协同化和原生化方向演进。

面对分布式拒绝服务（distributed denial-of-service，DDoS）攻击，现有研究多以构建能够检测大规模流量冲击的防御系统为目标。文献[31]针对链路故障问题，提出基于多智能体深度强化学习的自适应路径选择方案，提高了网络稳定性和动态适配能力。文献[32]基于混合专家模型，结合LLM与边缘场景智能体，提出了一种多场景的DDoS检测方案，有效提升了对未知DDoS攻击的检测率。目前，相关研究多围绕单点威胁展开，虽能有效缓解攻击，但缺少对跨域证据的联合分析，难以进行闭环的行为安全分析。

在加密流量与隐私敏感场景下，文献[33]提出了一种隐私保护型去中心化多智能体协作方法，可保证参与者的数据隐私，防范关键数据窃听风险。文献[34]面向车联网和元宇宙场景，将

多智能体迁移过程建模为马尔可夫决策过程（Markov decision process，MDP），采用近端策略优化（proximal policy optimization，PPO）算法缓解恶意流量攻击。该方向的已有研究构建的安全分析系统虽强调多方参与和数据隐私保护，但普遍缺少网络行为结构化证据表示，难以开展证据融合与攻击链推理。

针对攻击链长、隐蔽性强且阶段高度关联的APT攻击，多智能体协同有着更好的适配性。文献[35]通过多智能体共享防御信息和经验优化防御策略，应对APT中攻击行为的高不确定性和动态性。文献[36]提出了一种模块化的多智能体APT攻击检测方法，通过设置3种专用智能体结合上下文推荐系统，提高了APT攻击检测的准确率。上述方法虽具有共享协作的能力，但依赖固定任务的先验设置，缺少在网络架构与通信协议层面对消息语义、任务分配和证据分析的标准化约束。

综上，现有研究验证了智能体协同技术应用于6G网络安全的可行性，但大多将智能体作为攻击防御的上层应用工具，未能从网络体系结构和通信机制层面，将安全分析能力系统性地融入6G网络的转变。现有研究在安全分析系统与网络架构的深度融合方面存在不足、跨域证据分析困难，导致协作通信与编排机制难以适配原生网络架构。为此，本文面向6G网络恶意行为治理，提出“三层三域”协同架构，探索多智能体协同的网络架构与通信协议设计方法。

2　面向6G智能体网络行为安全的“三层三域”架构

图1所示的3类典型网络架构，分别体现了6G智能体网络在感知、决策与执行3个维度上的功能侧重，具备分布式感知能力、集中式决策与编排能力以及闭环执行能力。3类架构并非相互独立的并行方案，其智能体在功能定位、位置部署和协同模式上呈现出显著的层级化特征。这种层级化特征使网络行为碎片化，也为进一步抽象统一的智能体协同网络架构提供了基础。为在统一架构下同时实现跨域感知、任务驱动编排与网络功能执行，赋予6G智能体网络原生安全能力，本文提出“三层三域”网络架构。该架构以感知层、编排层、执行层贯穿行为感知、任务编排、证据推理的闭环安全分析流程，并采用A2A作为层通信支撑；以智能域、知识域、工具域明确协作主体、知识增强及工具能力的供给与调用边界，依托域通信协议实现域内通信支撑。

2.1　“三层三域”架构

面向6G智能体网络行为安全分析的“三层三域”网络架构如图4所示。该架构依托6G网络的演进特征，将多智能体协同能力内嵌为网络原生能力，以实现网络行为安全分析。根据行为感知、推理关联、证据验证、可解释输出的完整流程，结合感知智能、编排智能和执行智能的功能需求，该架构纵向设置感知层、编排层和执行层，并配置了6类功能互补的智能体，构建行为感知、任务编排与约束、证据整合与推理的闭环安全分析链路。为解决安全分析的协同效率与可靠性问题，该架构横向引入智能域、知识域和工具域，为因果推理、知识增强和智能体协同提供支撑，并明确智能、知识与工具能力的供给与调用边界。

感知层抽象于图1中的跨域感知架构，依托分布式智能对不同位置的异构数据进行感知，将原始数据转化为可供后续推理与检索的结构化线索及上下文信息。网络行为感知智能体部署在网络边缘，就近采集原始数据，并完成特征抽取和结构化描述，为编排层开展网络行为安全分析提供支撑数据。

编排层抽象于图1中的任务驱动型跨域编排架构，为“三层三域”架构的核心层级，部署目

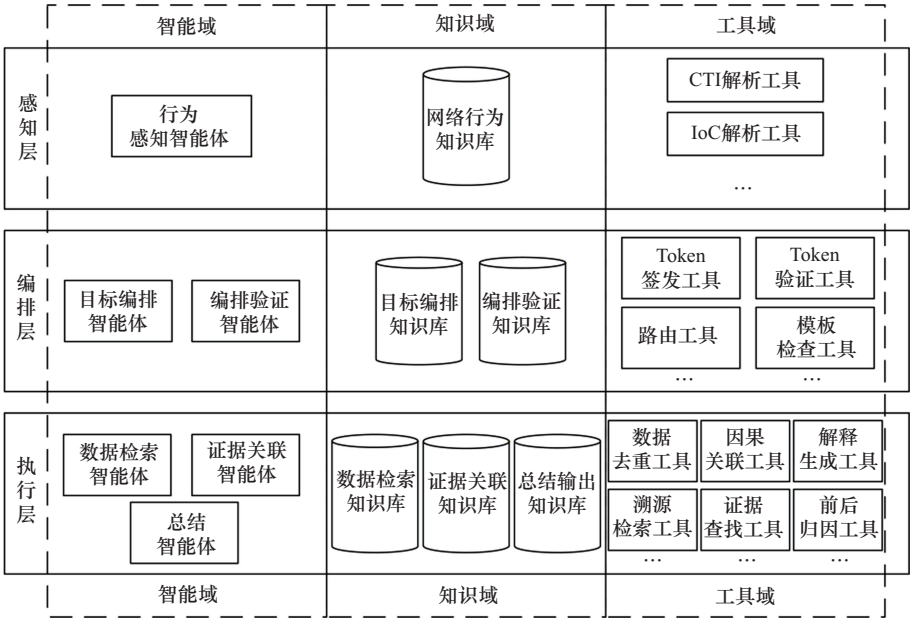


图4　面向6G智能体网络行为安全分析的“三层三域”网络架构

标编排智能体和编排验证智能体，以满足6G网络中任务意图驱动和跨域智能编排的业务需求。目标编排智能体根据上下文信息和行为分析目标，结合智能体功能进行调度和控制。编排验证智能体负责对编排方案进行可行性与安全性验证，保证执行层智能体能够满足预设编排目标。

执行层抽象于图1中的网络功能执行架构，部署数据检索智能体、证据关联智能体和总结智能体。该层级根据编排层下发的任务，基于因果推理能力检索关键证据并将其与行为进行关联，生成可核验的证据与关联结果，最终输出可解释的网络安全行为分析结论。

在横向维度上，智能域承载3层架构中的各类智能体，是网络行为安全分析的主体。知识域面向智能体任务提供知识增强服务，包括行为分析、推理与验证所需的结构化与非结构化知识，可分为任务知识和调用工具知识两类，以支撑可复用的分析与验证过程。工具域为智能域提供必要的工具，以完成智能体的目标任务。这些工具通过6G网络能力开放接口统一封装，使其调用过程不再局限于传统的函数接口或应用程序接口，而是作为网络原生能力，通过智能通信机制供智能体按需调用。

2.2　层协作方式

本节从层级协作视角，描述多智能体在协作过程中的交互方式和控制关系，主要涵盖意图生成、编排控制、证据生成、安全验证。首先将跨层交互抽象为6类消息，以此作为层间协作的统一接口语义。

意图：由网络行为感知智能体生成并上报至目标编排智能体，用于对可疑网络行为进行结构化表征并确定上下文边界，通常包含侵入指标（indicators of compromise，IoC）、候选战术、技术与流程（tactics, techniques, and procedure, TTP）及来源引用等。

计划：由目标编排智能体生成，为全局可执行方案的结构化描述，包括任务分解、依赖关系、终止条件等。

任务：由目标编排智能体完成任务拆解后下发至执行层智能体，并由编排验证智能体在执行前进行合规性与可行性校验，具备明确的输入输出模板和约束条件。

证据：由执行层智能体回传至目标编排智能体的结构化结果，需满足可追溯、可核验、可支撑证据关联与可解释复用的要求。

状态：执行层返回的运行状态与度量信息，如证据检索命中率、任务失败类型等，用于驱动编排层进行迭代修正或终止决策。

约束：由编排验证智能体提供，是用于计划、任务和证据验证的规则集合，包括限制检索范围、控制令牌长度、约束输出格式等。

各智能体以角色为边界实现分工协作：感知层负责提出可执行线索，但不开展全局推断；编排层拥有全局控制权并承担编排调度职能；执行层负责证据生成与表达，但不参与决策制定。6类智能体的层内角色分工见表1。

层级协作以意图交互、编排控制、执行反馈、迭代修正的顺序进行，其示意图如图5所示。所有的推理过程均需依托知识和证据完成，以保障多智能体协作的可靠性。意图交互阶段由网络行为感知智能体上报意图消息，该消息必须携带候选集与上下文证据边界，如IoC对应的语义证据与来源，确保编排层制定的计划具有可追溯性，避免在证据不足时开展过早推断。

目标编排智能体将整体计划拆解为子任务并下发至执行层，实现对多智能体的编排管控。下发任务需明确约束条件，如实体类型、检索字段等。编排验证智能体对任务输出进行合规校验，防止出现无界检索、越权调用与格式不兼容等情况。

执行层通过证据和状态反馈实现执行反馈。证据提供可核验的实体、安全事件与关联链段；状态报告资源消耗、任务失败原因等内容。编排层据此更新全局上下文与任务优先级，判断是否进入下一轮迭代。

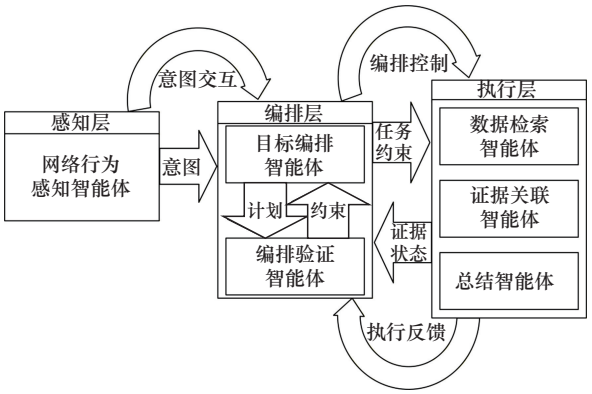


图5　层级协作方式示意图

当出现证据不全、验证驳回、命中率过低等情况时，由目标编排智能体进行迭代修正与策略调整，确保最终输出可信的网络行为安全分析结果。

2.3　多智能体协同协议

基于“三层三域”架构，以网络行为安全分析为目标，本文提出面向6G智能体网络行为安全分析的多智能体协同流程，如图6所示。该流程对多智能体在感知、编排与执行层级的交互过程进行统一规范；以第2.2节提出的6类消息作为统一语义接口，规定交互所需的通用字段，并依托A2A协议承载层间协作，使多智能体协同成为通信网络可直接支撑的内生能力。为保障语义可执行性，6类消息在5大阶段一一对应：意图生成阶段对应意图消息，计划编排与验证阶段对应

表1　6类智能体的层内角色分工

层级	智能体	角色	任务	输入	输出
感知层	网络行为感知智能体	意图提供者	将原始网络行为结构化	网络行为	意图
编排层	目标编排智能体	全局控制者	融合意图与证据形成全局计划，拆解并路由任务，决定迭代或终止	意图、证据、状态	计划、任务
	编排验证智能体	验证检查者	验证计划、任务、证据的安全性和合规性	计划、任务、证据	约束、验证结果
执行层	数据检索智能体	证据采集者	数据内检索事件并规范化，形成可用证据	任务	证据、状态
	证据关联智能体	行为关联者	在证据约束下组织行为因果结构	证据	证据、状态
	总结智能体	解释汇报者	输出行为安全分析结果	证据、上下文	状态，最终结果

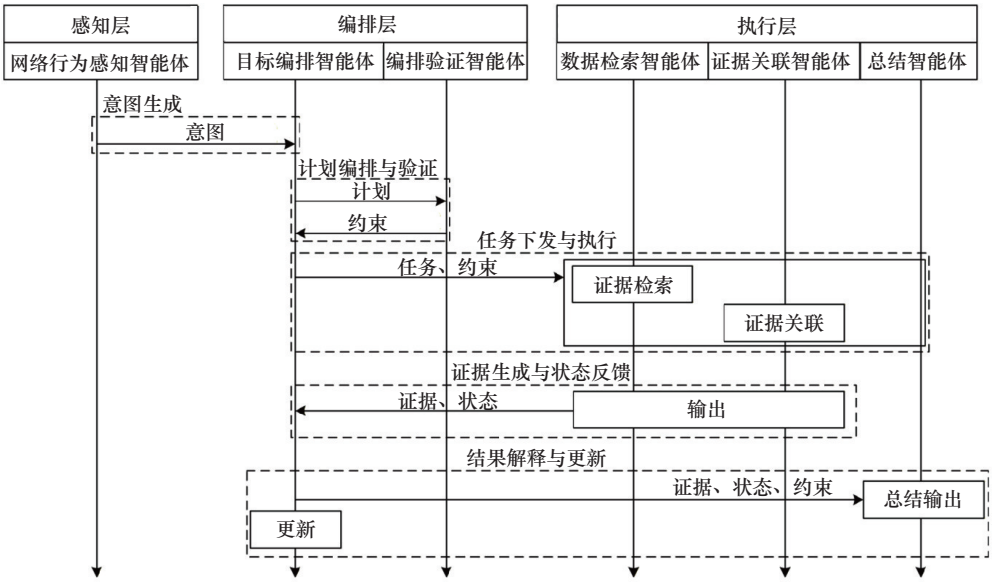


图6　网络行为安全分析的多智能体协同流程

计划消息与约束消息，任务下发执行阶段对应任务消息，证据生成与状态反馈阶段对应证据消息与状态消息，结果解释更新阶段对应证据、状态与约束消息。

单条协同消息由通用字段与任务载荷两部分组成。通用字段如下。

- 上下文：描述当前网络行为安全分析的上下文边界与来源信息，用于保证多智能体协同认知一致。
- 任务标识：标识当前协同任务的类型与所处阶段，用于驱动编排与控制逻辑。
- 溯源信息：记录消息来源、证据引用与处理路径，支撑安全核验与行为回溯。
- 运行状态：描述任务执行状态、资源消耗、失败原因等，为迭代修正与终止判断提供依据。

任务载荷用于承载特定行为安全任务所需的结构化数据，如查询模板、实体事件集合、推理中间结果等，不同任务可根据需要定义自身载荷结构。

多智能体协同流程共分为5个阶段，通过6类消息进行通信，并由编排验证智能体实施约束管控。

第一阶段：意图生成。部署于数据源近端的网络行为感知智能体对原始网络行为进行结构化分析，形成描述可疑行为的高层意图。意图需明确上下文边界、候选线索集合及来源引用，并通过A2A协议上报至目标编排智能体。这一阶段仅提出可执行线索，不开展全局推断。

第二阶段：计划编排与验证。目标编排智能体基于意图消息与全局上下文，生成可执行的分析计划，完成任务目标拆解、子任务规划与终止条件设定。生成的计划需提交编排验证智能体进行合规性与安全性校验，校验通过后方可进入执行阶段。

第三阶段：任务下发与执行。校验通过的计划下发至执行层智能体，明确任务输入输出规范与约束条件。编排验证智能体对下发任务进行必要的权限与资源检查，防范无界检索、越权调用或资源滥用等情况。

第四阶段：证据生成与状态反馈。执行层智能体按照任务要求生成结构化证据，并返回任务执行状态。证据须具备可追溯性，状态信息用于反映执行效果与异常情况。目标编排智能体据此更新全局上下文，判断是否进入下一轮迭代。

第五阶段：结果解释与更新。任务完成或终止后，由执行层与编排层共同完成结果解释与输出。生成的结构化结果写入知识域前，需经过编排验证智能体的合规性检查，验证通过后由编排层统一更新知识库，为后续行为安全分析提供持续支撑。

在上述协同流程中，A2A 协议主要用于智能体间的层间通信，承载意图、计划、任务、证据与状态等消息。

2.4 域通信协议

在上述多智能体协同流程中，智能体需要进行长时序推理协同，这不仅要求其具备工具调用能力，还需要实现对威胁情报、溯源证据、攻击模式，以及因果关系等知识的获取与更新。目前的主流智能体协议 MCP 提供了标准化的智能体工具调用范式，但未对知识对象的标准化描述、获取流程与更新约束作出规范，难以满足网络行为安全分析过程中的协同推理需求。本文在 MCP 的基础上，设计面向智能域－知识域－工具域的域间通信协议，在“三层三域”架构下对智能体、知识域与工具域进行协同组织。该协议将知识域中的网络行为知识作为独立对象进行编目与关联，便于检索、引用和更新，规范协同推理过程中知识获取与工具调用的统一流程与接口，便于知识增强与工具的组合，并在知识与工具引入过程中进行表示，保证过程可回溯与验证。该协议支持智能域、知识域和工具域之间的协同，为多智能体在 6G 网络中的协同提供基础通信能力。

智能域—知识域—工具域的域通信协议如图 7 所示，各组成部分定义如下。

- 知识域：专业知识集合，包括工具调用知识、网络行为库、攻击模式库等。
- 知识服务端：负责知识访问和增强的控制，包括知识检索、上下文增强等。
- 工具域：智能体可调用的工具集合，包括推理工具、检索工具、流量分析工具等。
- 工具服务端：负责工具的管理与调用，包括工具注册、权限授予等。
- 智能体客户端：部署于智能域，负责发起知识请求和工具调用。

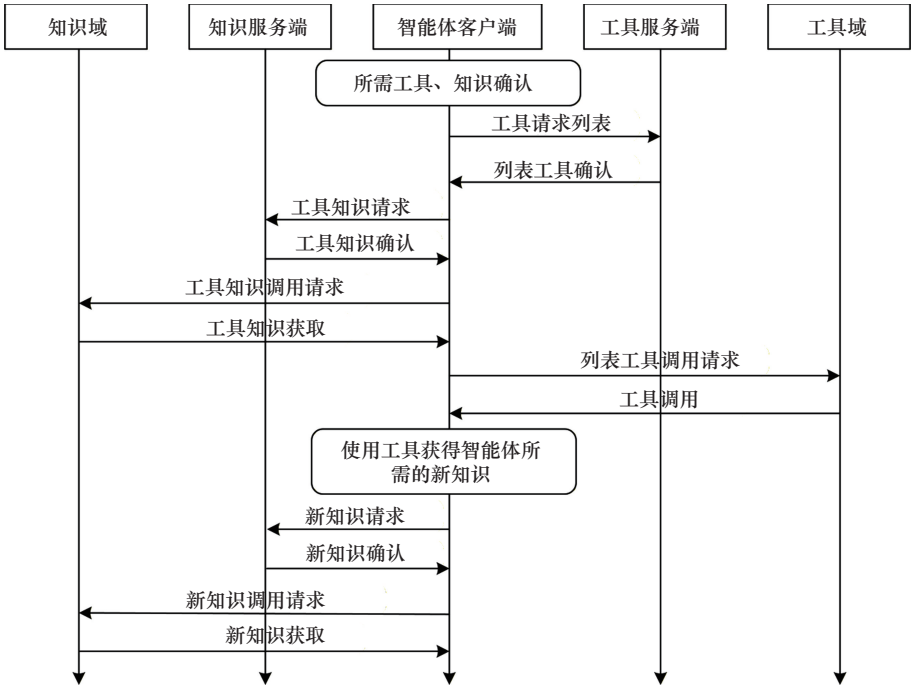


图 7　智能域—知识域—工具域的域通信协议

该协议整体可划分为工具准备和智能体执行两个阶段。在工具准备阶段，智能体客户端接收智能域内智能体的任务需求和知识需求，完成对知识域和工具域的资源调用。客户端先向工具服务端发送所需的工具请求列表；工具服务端维护工具列表、调用权限等关键信息，对调用行为开展合法校验与调用约束，并向客户端返回校验结果。客户端确认工具可正常调用后，向知识服务端发出工具所需的知识列表请求，包括提示词、上下文信息等，以帮助工具更好地发挥作用。客户端在收到知识列表请求的返回后，向知识域发出知识调用请求。在收到知识域的知识后，客户端基于工具列表向工具域发起工具调用。

在智能体执行阶段，客户端通过调用工具和知识增强机制为智能体补充执行所需知识，并向知识服务端发起新的知识请求；收到知识确认指令后，向知识域发起新知识的调用。至此，智能体已获取任务执行所需的工具和全部知识，可开展任务执行。该协议在知识和工具列表核验环节，对知识访问与工具调用进行细粒度约束，明确权限边界，确保整个通信过程可控。同时，为引入的知识和工具添加溯源标识，以保障网络行为安全分析流程可回溯、可验证。此外，通信过程可结合签名和完整性校验等机制，防止中间结果被篡改或伪造。

2.5　智能体工作范式

智能体作为网络行为安全分析中的基本执行单元，需在“三层三域”架构下与外部智能体、知识库和工具库进行交互，以完成自身任务。本节提出了适用于不同角色的单智能体工作范式，包括组成结构、功能模块和交互方式，如图 8 所示。将单智能体规范为以控制核心为中心、多个功能模块为辅助的内部结构，并基于域通信协议和 A2A 协议，完成与外部智能体的协同。

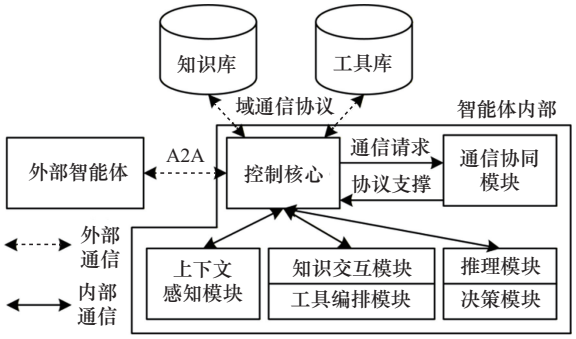


图 8　智能体工作范式

控制核心不参与具体推理与执行，主要承担状态协调、流程调度与协议封装职责，同时维护任务执行状态与阶段信息，管理上下文与中间推理结果，统筹智能体与知识库、工具库和外部智能体的协同时机，并完成内外部交互的协议适配，统一封装域通信协议与 A2A 消息。

上下文感知模块负责对异构、异步数据进行结构化处理与特征感知，数据来源包括网络日志、外部智能体传输数据等，为后续知识查询、工具调用和推理决策提供基础支持。

知识交互模块和工具编排模块不直接对接知识库和工具库，相关操作均由控制核心基于域通信协议进行统一控制。其中，知识交互模块负责知识需求生成和知识调用，工具编排模块则负责对工具进行规划、编排和约束。两类模块的输出结果均回传至控制核心，以支撑全局感知、协同与推理工作。

推理模块和决策模块负责综合上下文信息、知识反馈与工具执行结果，输出智能体的中间判断与决策内容。其输出结果可表现为网络行为假设、证据片段，或进一步的查询指令与协同请求。

通信协同模块作为智能体对外交互接口，按照控制核心的通信请求提供不同的协议支撑。A2A 协议用于实现智能体间的通信，域通信协议则用于实现智能体与知识库、工具库之间的通信。

3 以APT攻击链构建为实例的实验与评估

为验证本文所提架构在复杂行为安全分析场景下的有效性，本文选取代表性的网络行为安全任务开展实例验证。APT攻击是当前针对高敏感单位的主流攻击形式，如2025年国家互联网应急中心披露的一起境外针对中国国家授时中心的APT攻击事件[37]。这类攻击具备长期潜伏、多阶段演化、证据分散、跨域关联困难等特征[38]，是网络行为安全领域极具挑战的复杂攻击行为。APT攻击包含多个攻击阶段，关键行为线索分布在不同网络位置与时间尺度中，无法依靠单点检测实现有效识别[39]。构建APT行为攻击链能够刻画其攻击行为与演进过程，因此攻击链可作为网络行为安全分析的一种典型输出形式[40]。

3.1 APT攻击链构建协同流程

在APT攻击链构建任务中，本文定义的通用协同流程与所提出的6类消息语义的映射关系见表2。

在上述映射关系下，多智能体在APT攻击链构建任务中的协同流程如图9所示。首先，网络行为感知智能体通过域通信协议获取威胁情报（cyber threat intelligence，CTI）解析规则、TTP分析知识等，调用工具提取IoC、候选TTP等关键线索，形成结构化意图。随后，通过A2A协议将意图传输给目标编排智能体。

目标编排智能体融合意图与全局上下文，基于域通信协议获取攻击阶段模型、步骤映射规则与历史攻击模板，将IoC/TTP映射为候选攻击步骤序列，并生成用于证据核验的候选查询任务，再借助A2A协议将候选任务提交至编排验证智能体进行校验。

编排验证智能体通过域通信协议调用安全策略、查询白名单等，结合分析工具完成包括Token授权合法、查询模板安全等检查。若验证失败，将通过A2A协议反馈原因并触发重新编排；若验证通过，则将任务下发至数据检索智能体，同时回传状态信息至目标编排智能体，用于状态同步。

数据检索智能体在接到查询任务后，对网络日志、溯源数据进行检索，提取与攻击步骤相关的实体及事件信息，完成攻击步骤的映射。检索结果经由A2A协议同时发送给证据关联智能体和目标编排智能体，用于同步当前构建进度。

证据关联智能体收到候选查询和检索结果后，通过域通信协议获取历史攻击模式和因果关联知识，调用证据关联工具和推理工具，完成时序与逻辑关联，生成候选攻击链。随后，通过A2A协议将关联结果返回给目标编排智能体，为全局决策提供依据。

目标编排智能体融合检索证据与关联结果，形成攻击链描述，并提交至编排验证智能体进行一致性与存在性验证。若验证不通过，将返回改进建议并触发迭代；若验证通过，则将结果同步发送至目标编排智能体与总结智能体。

总结智能体将各类攻击证据转换为可解释的攻击链叙事。在生成过程中，若需补全上下文，可通过A2A协议请求目标编排智能体发起补充查询。该请求经编排验证智能体校验后，由数据检

表2 协同流程与消息在APT攻击链构建任务中的映射关系

协同阶段	6类语义消息	APT攻击链构建中的实际载荷
意图生成与上报	意图	初始IoC、候选TTP、行为摘要、来源引用
计划编排与验证	计划+约束	攻击阶段划分、查询策略、终止条件、模板白名单
任务下发与执行	任务+约束	查询模板、字段类型、时间范围、关联约束
证据生成与状态反馈	证据+状态	实体事件集合、攻击阶段映射、命中率、失败原因
结果解释与更新	证据+状态+约束	攻击链结构化描述、证据引用、可写入知识条目

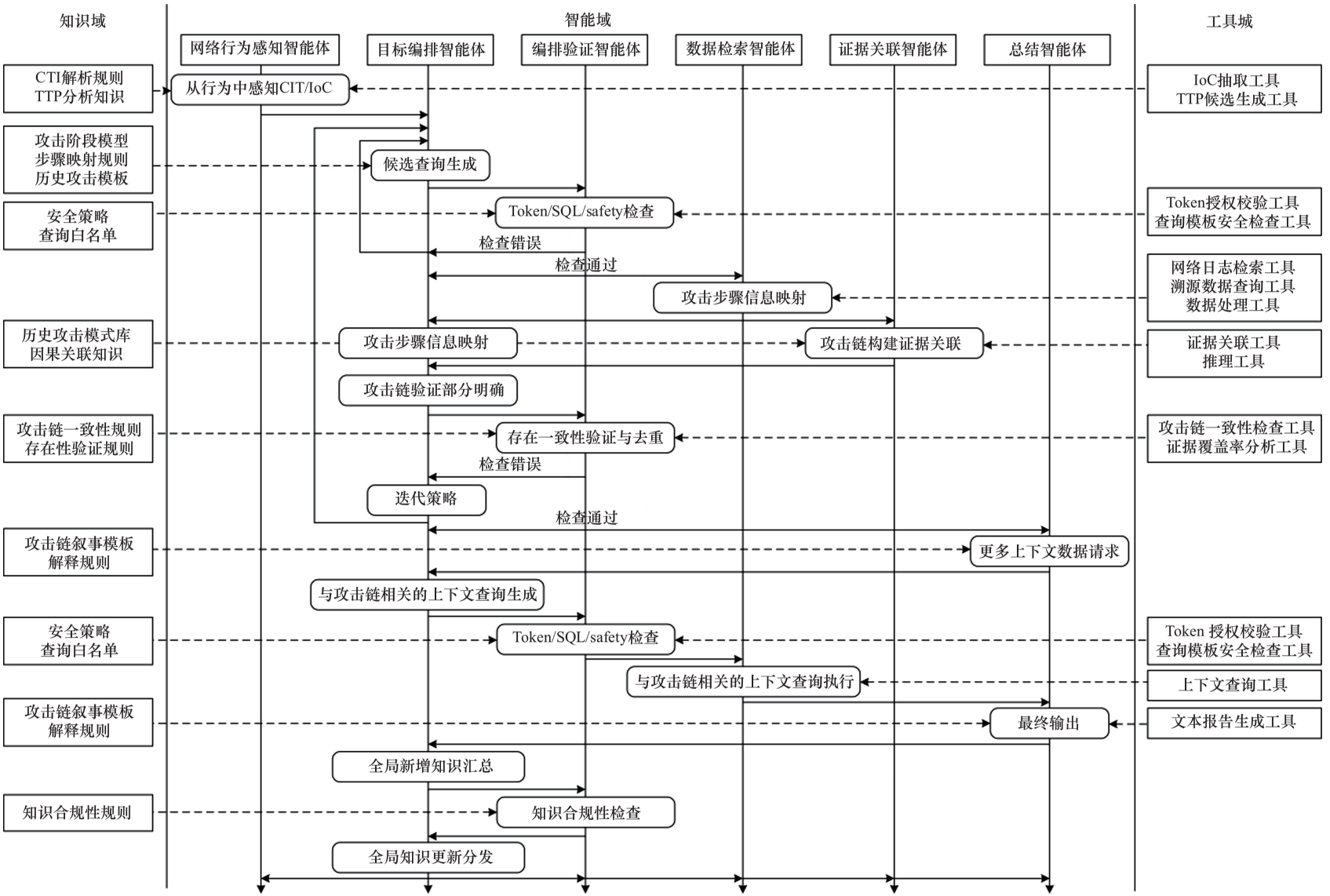


图9　以APT攻击链为例的智能体协同流程

索智能体执行并交付至总结智能体，最终生成完整的攻击链描述。

最终输出结果回传至目标编排智能体，用于触发全局新增知识的汇总。新增知识在写入前须通过编排验证智能体的合规性检查。审查通过后，由目标编排智能体统一分发至各智能体对应的知识域，实现对知识的更新。

3.2 实验设置

3.2.1 数据集设置

本次实验选择APT数据集中难度较高的Clearscope-e3和Clearscope-e5数据集[41]开展性能评估。其中，Clearscope-e3数据集贯穿全部实验，全面验证本文所提架构的性能；Clearscope-e5作为补充数据集，用于验证本文所提架构在不同APT场景下的泛化能力。两个数据集均以日志形式记录主机、进程、文件、网络连接等多类系统行为事件，完整覆盖APT攻击从初始入侵、持久化建立、横向移动到目标达成的多阶段攻击过程。数据集未标注单个事件或阶段标签，仅以提供的攻击场景描述来反映攻击的特征。为评估攻击链构建的性能，实验先将原始数据转换为全局溯源图，再依据描述确定攻击事件集合。需要注意的是，溯源图与攻击事件集合仅用于性能评估，不参与攻击链构建流程，避免信息提前泄露对实验结果造成干扰。

3.2.2 智能体设置

感知智能体对日志中主机、进程、文件和网络连接等多类事件进行规范化处理，将其表示为“实体—事件—上下文”的结构化片段，并抽取IoC与候选TTP，形成分析意图上报至编排层。目标编排智能体基于攻击阶段生成受约束的查询任务，任务核验通过后下发至执行层。数据检索智能体从日志与溯源数据中检索证据；证据关联智能体对证据进行因果关联分析，生成候选攻击链；再由总结智能体输出结构化的攻击链分析结果。在本文所提方案中，目标编排智能体与总结智能体采用LLM驱动，以支持语义推理，其余智能体以逻辑代码为主，仅将LLM作为工具模块接入使用。

3.2.3 知识设置

实验所用知识主要包括攻击链构建知识和工具运行知识。前者包括攻击技术表、IoC映射规则、编排合法性规则等；后者包括字段名称、节点结构等。

3.2.4 评估指标设置

将构建得到的攻击链映射到ATT&CK框架对应的攻击阶段，并通过语义一致性校验合并语义攻击的攻击步骤。以映射后的攻击阶段集合与人工划定的攻击事件集合进行对比，计算精准率、召回率和F1分数。其中，精准率用于衡量攻击链中行为判定的准确性；召回率用于衡量攻击链对关键攻击步骤的覆盖能力；F1分数用于综合评价攻击链构建结果的准确性和完整性。

3.2.5 基线设置

实验选择3类方案作为对比基线：（1）传统AI溯源方案Flash[10]，该方案基于图神经网络（graph neural network，GNN）和word2vec技术实现APT检测；（2）单智能体检测架构ProvSeek[39]，该架构依托单个LLM驱动多模块实现APT检测。（3）多智能体检测架构TAL[36]，该架构部署3个智能体，并结合上下文推荐系统开展APT检测。

3.3 APT攻击链的网络行为安全分析示例

实验选取3类典型APT攻击链进行网络行为安全分析，攻击链示意图如图10所示，不同方法的检测性能见表3。这些攻击链由多个低可观测、分散的网络行为构成，可充分验证“三层三域”架构针对长期潜伏、多阶段演化及多路径特征的复杂网络行为的分析能力。

典型潜伏型APT攻击链的攻击从系统与进程探测开始，逐步转为信息收集、隐蔽通信以及后续的执行与驻留，单个阶段中的网络行为呈现低

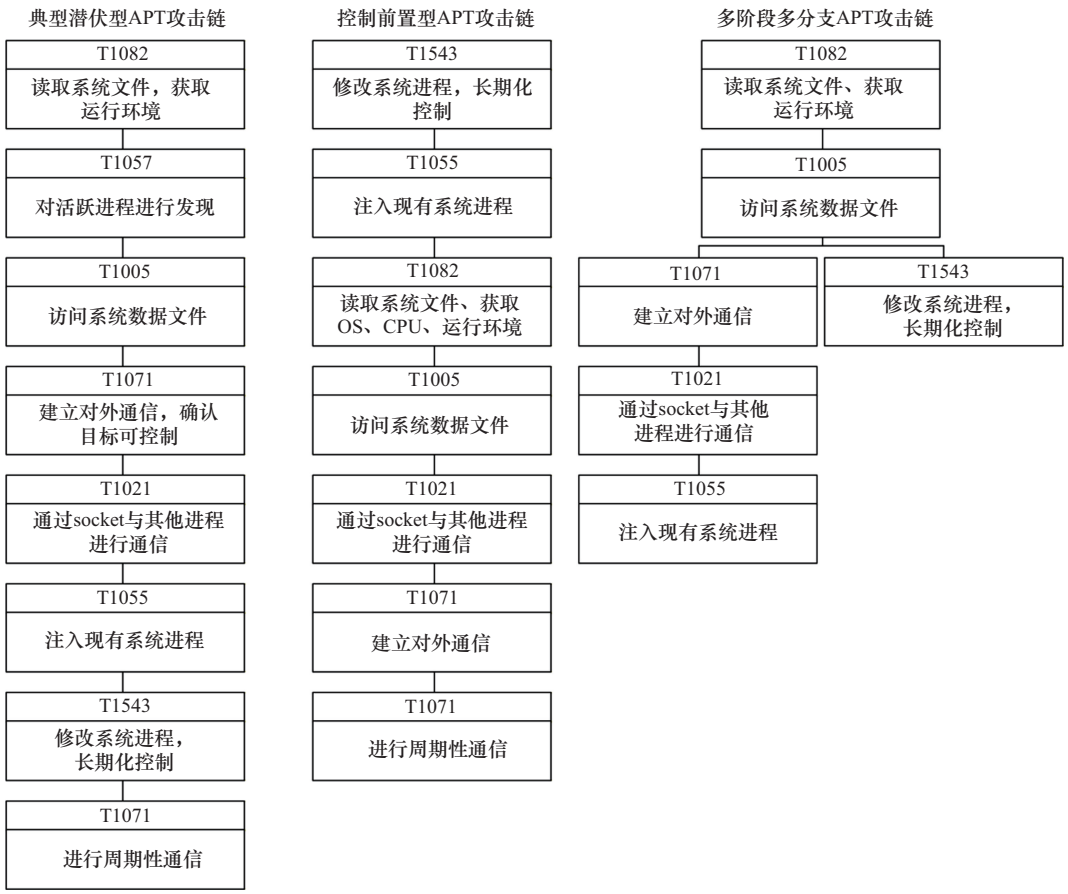


图10　3种典型APT攻击链示意图

表3　不同方法在3类APT攻击链上的检测性能

方法	典型潜伏型APT攻击链			控制前置型APT攻击链			多阶段多分支APT攻击链		
	精准率	召回率	F1分数	精准率	召回率	F1分数	精准率	召回率	F1分数
Flash	68%	86%	77%	62%	80%	71%	67%	83%	75%
ProvSeek	72%	76%	74%	73%	77%	75%	63%	69%	66%
TAL	80%	82%	79%	81%	84%	82%	78%	80%	79%
“三层三域”	**89%**	**93%**	**91%**	**86%**	**90%**	**88%**	**86%**	**86%**	**86%**

频且看似合法的特性。Flash在该类APT攻击链检测上的召回率为86%，但精准率仅为68%，说明其能够覆盖较多潜在恶意行为，但误报相对较多；ProvSeek的精准率和召回率分别为72%和76%，表现相对稳定；TAL提升至80%的精准率和82%的召回率，表现出较好的综合能力。相比之下，本文所提“三层三域”架构取得了89%的精准率、93%的召回率和91%的F1分数，均为最优。实验结果表明，“三层三域”架构能够持续关联分散的网络行为，关联不同阶段的语义一致性，完整还原攻击流程，有效识别具备长期潜伏、逐步渗透特征的网络行为。

控制前置型APT攻击链在攻击初期即建立长期控制能力，而非传统“先发现，再利用，最后控制”的顺序。由于其行为阶段具有不确定性，网络行为安全分析不能严格依赖时间顺序。Flash在该类攻击检测中的精准率降至62%，召回率为80%，表明其在顺序异常场景时误判增多；Prov-

Seek取得了较均衡的效果，精准率为73%、召回率为77%；TAL的精准率和召回率进一步提升至81%和84%，证明了多智能体协同对非典型顺序攻击具有较强适应性。本文所提的“三层三域”架构取得了86%的精准率、90%的召回率和88%的F1分数，显著优于各基线方法，表明该架构能够识别非典型顺序的攻击行为，并基于行为语义进行整体分析，从而能够适应复杂网络环境下的多样化攻击策略。

多阶段多分支APT攻击链由多个并行开展的攻击阶段构成，形成多条相互关联的攻击链，共同服务于整体攻击目标。对其分析不能只关注局部行为而忽略分支层面的行为意图：考虑更多的分支可能会导致精准率下降，而忽略分支则会导致召回率下降。Flash在攻击检测上仍表现出高召回、低精准的特点，其精准率和召回率分别为67%和83%；ProvSeek的检测性能下降更为明显，精准率、召回率和F1分数分别为63%、69%和66%，说明其在复杂并行分支场景下覆盖不足；TAL取得了78%的精准率、80%的召回率和79%的F1分数，表现相对均衡。相比之下，“三层三域”架构的精准率、召回率和F1分数均达到86%，说明其能够同时关注多分支局部行为特征与全局攻击意图，捕捉网络行为中的非线性与并行化特征，并做出综合决策，与6G智能体网络中多实体协同、行为化的特征高度契合。

3.4 对比实验

Flash、ProvSeek、TAL与“三层三域”架构在Clearscope-e3和Clearscope-e5数据集上的APT攻击链构建性能对比见表4。在两个数据集上，“三层三域”架构的3项指标均取得了最优性能，说明其不仅在单一数据集上有效，而且具备较稳定的跨数据集表现。从Clearscope-e3到Clearscope-e5的变化来说，“三层三域”与TAL表现一致，但“三层三域”的绝对性能始终更高。与ProvSeek和Flash相比，“三层三域”架构无论是性能的相对提升还是绝对值都具有明显优势，这表明“三层三域”架构在保证覆盖能力的同时，能够显著降低误报率，从而在不同数据分布下取得更优性能。

表4 不同方法在Clearscope-e3和Clearscope-e5数据集上的APT攻击链构建性能对比

方法	Clearscope-e3			Clearscope-e5		
	精准率	召回率	F1分数	精准率	召回率	F1分数
Flash	65%	83%	74%	67%	83%	75%
ProvSeek	70%	74%	72%	71%	75%	73%
TAL	80%	82%	81%	82%	84%	83%
“三层三域”	**87%**	**89%**	**88%**	**89%**	**91%**	**90%**

Flash在召回率上表现较好，但精准率较差，说明其能够覆盖较多真实攻击，但因依赖异常行为特征，缺乏对不同攻击阶段的关联，产生较多误报。ProvSeek在精准率上有所提升，但召回率下降，表明单智能体方法在攻击阶段碎片化和弱证据场景下，存在一定漏检。TAL在两个数据集和不同的性能指标上的表现都相对均衡，表明多智能体协同构建APT攻击链的优势，但构建过程缺乏分层约束与明确分工，整体性能仍受限。

相比之下，“三层三域”架构通过感知层、编排层和执行层的分工协同，将攻击链构建过程拆解为多个可控阶段。各智能体分别负责行为感知、攻击语义映射、因果关联和推断，并在协同过程中引入知识增强，在降低误报率的同时高效覆盖攻击阶段，实现了精准率与召回率的同步提升。这表明“三层三域”架构不仅能够提升攻击链覆盖能力，也提升了构建结果的可靠性与一致性。

不同LLM对“三层三域”架构、ProvSeek和TAL的性能影响见表5。“三层三域”架构的F1分数均值为86.49%，标准差为1.28；ProvSeek的F1分数均值为69.70%，标准差为2.63；TAL的F1分数均值为78.82%，标准差为1.92。由此可

见，“三层三域”架构对 LLM 的敏感性更低，且在小参数模型下，仍能保持较高的精准率和召回率。这说明其能力主要来源于多智能体协同机制与结构化推理流程，而非单一 LLM 的参数规模。

表 5　不同 LLM 对 APT 攻击链构建性能的影响

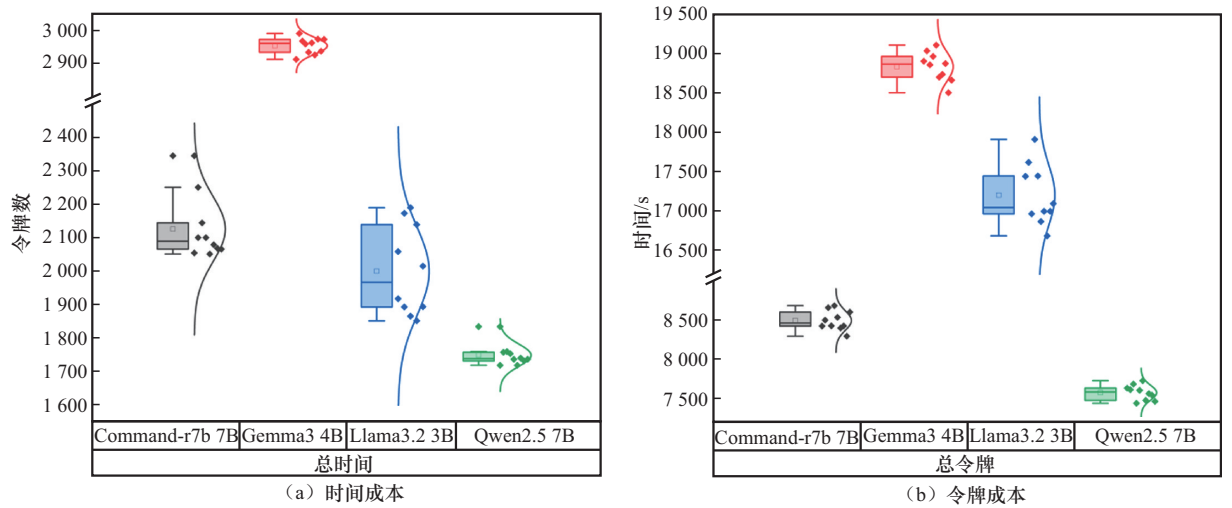
LLM	“三层三域”		ProvSeek		TAL	
	精准率	召回率	精准率	召回率	精准率	召回率
Llama3.2 3B	84%	87%	63%	68%	75%	79%
Qwen2.5 7B	**87%**	**89%**	**70%**	**74%**	**80%**	**82%**
Gemma3 4B	84%	86%	65%	69%	74%	80%
Command-r7b 7B	**87%**	88%	**70%**	71%	79%	**82%**

相比之下，ProvSeek 的性能受 LLM 影响更为明显，使用小参数模型的精准率和召回率均显著下降。这表明，单智能体架构对推理能力依赖较强，缺乏足够的结构化约束，难以在复杂攻击场景下保持稳定性能。TAL 的多智能体方法相较于单智能体方法的 LLM 依赖性有所降低，但由于其粗粒度分工及缺少知识和工具的引入，LLM 仍需负责大量工作，其 LLM 依赖性仍高于“三层三域”架构。

在 4 种不同 LLM 下，本文所提方案在处理 10 000 条事件的时间成本和令牌成本箱线图如图 11 所示。从图 11 可知，本文所提方案的整体运行时间与生成令牌数均保持较小波动。其中，Qwen2.5 7B 与 Gemma3 4B 的运行时间标准差分别为 35.43 和 22.86，表现出较高的时间稳定性。

在令牌成本方面，“三层三域”架构在不同 LLM 下未出现异常的令牌生成现象。其中，Qwen2.5 7B 的平均令牌成本为 7 545、标准差为 89.4，为最低且最稳定，具有较高的推理效率。可以看出，本文所提方法的整体开销对 LLM 的选择具有较强鲁棒性，其运行稳定性主要由多智能体协同流程与任务编排机制所决定，而非单一模型的规模或推理策略。

接下来，使用 Qwen2.5 作为基础 LLM，对 ProvSeek、TAL 与“三层三域”的时间成本和令牌成本进行对比，结果见表 6。“三层三域”在时间成本和令牌成本上均显著低于对比方法，在重复实验中具有最小的标准差。以上结果表明，“三层三域”在保证攻击链构建性能的同时，有效减少了对 LLM 推理资源的依赖，且具有优秀的稳定性。这主要源于多智能体协同架构对攻击链构建任务的合理拆解及对知识和工具的合理使用，使其不需要像 ProvSeek 那样依赖 LLM 进行频繁的长上下文构建和推理，也不需要如 TAL 那样让 LLM 参与所有决策过程。



（a）时间成本　　（b）令牌成本

图 11　本文所提方案在 4 种不同 LLM 下运行成本的箱线图

表6　基于Qwen2.5，3种方案的时间成本与令牌成本

方法	时间成本/s	时间成本标准差/s	令牌成本	令牌成本标准差
ProvSeek	2 837.31	92.07	15 209	231.2
TAL	2 433.29	51.24	9 731	134.5
“三层三域”	**1 754.77**	**35.43**	**7 545**	**89.4**

4　结束语

在6G网络原生智能的演进趋势下，智能体逐步成为网络中承担感知、编排与执行功能的基本单元。这一趋势在提升网络智能水平的同时，也使网络行为呈现碎片化、跨域化和长期潜伏等特征，传统的单点检测难以满足网络行为安全分析的需求。为此，本文面向6G智能体网络中的网络行为安全需求，提出了“三层三域”多智能体协同网络架构，通过分层分域协同，将行为感知、全局编排与智能执行融入网络。在此基础上，结合层间协作方式和域间通信协议，设计了完整的网络行为安全分析的多智能体协同机制与流程。以APT攻击链构建作为网络行为安全分析实例进行验证，结果表明，“三层三域”架构能够有效支撑复杂、长期网络行为的安全分析。

参考文献：

[1] Chai J J, Zhao Z J, Zhu Y H, et al. A survey of cooperative multi-agent reinforcement learning for multi-task scenarios[J]. Artificial Intelligence Science and Engineering, 2025, 1(2): 98-121.

[2] Wang C X, You X H, Gao X Q, et al. On the road to 6G: visions, requirements, key technologies, and testbeds[J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 905-974.

[3] Li Y H, Wang H Z, Min G Y, et al. A flexible and scalable multi-agent learning framework for dynamic RAN slicing in 6G native-AI networks[J]. IEEE Transactions on Mobile Computing, 2026, 25(5): 7258-7273.

[4] Yang L, Naser S, Shami A, et al. Toward zero touch networks: cross-layer automated security solutions for 6G wireless networks[J]. IEEE Transactions on Communications, 2025, 73(9): 7650-7679.

[5] TR 22.870: 2025 Study on 6G use cases and service requirements[S].

[6] TR 38.914: 2025 Study on 6G scenarios and requirements[S].

[7] Aly A, Iqbal S, Youssef A, et al. MEGR-APT: a memory-efficient APT hunting system based on attack representation learning[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 5257-5271.

[8] Li T, Liu X M, Qiao W, et al. T-trace: constructing the APTs provenance graphs through multiple syslogs correlation[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(3): 1179-1195.

[9] Zhao J, Yan Q B, Liu X D, et al. Cyber threat intelligence modeling based on heterogeneous graph convolutional network[C]// Proceedings of the 23rd International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2020). 2020: 241-256.

[10] Ur Rehman M, Ahmadi H, Ul Hassan W. Flash: a comprehensive approach to intrusion detection via provenance graph representation learning[C]//Proceedings of the 2024 IEEE Symposium on Security and Privacy (SP). Piscataway: IEEE Press, 2024: 3552-3570.

[11] Golec M, Khamayseh Y, Melhem S B, et al. LLM-driven APT detection for 6G wireless networks: a systematic review and taxonomy[PP]. V2. arXiv (2025-06-23) [2026-02-04]. arXiv: 2505.18846.

[12] Dai C, Wang Y Z, Wu T Y, et al. Robust multi-agent reinforcement learning for physical layer security communication in RIS-assisted UAV-enabled ISAC networks[J]. IEEE Transactions on Network Science and Engineering, 2025, 13: 4969-4984.

[13] Zakir Khan M, Ge Y, Mollel M, et al. RFSensingGPT: a multimodal RAG-enhanced framework for integrated sensing and communications intelligence in 6G networks[J]. IEEE Transactions on Cognitive Communications and Networking, 2026, 12: 298-311.

[14] Wang Y, Yang C G, Li T, et al. A survey on intent-driven end-to-end 6G mobile communication system[J]. IEEE Communications Surveys & Tutorials, 2026, 28: 882-915.

[15] Cheng S, Wang Z Y, Feng F Z, et al. IFresher: information freshening for mobile augmented reality with multi-agent reinforcement learning in edge computing[J]. IEEE Transactions on Mobile Computing, 2025, 24(11): 11703-11716.

[16] Liang Y Z, Jiang R H, Wei B S, et al. MAMoE: a multi-agent mixture-of-experts framework for LLM-assisted 3D object re-

construction and transmission[J]. IEEE Transactions on Network Science and Engineering, 2026, 13: 3862-3878.

[17] Gui J S, Li Z Y, Zhang J J, et al. Multi-heterogeneous-agent DRL for efficient congestion control with reward redistribution in space-air-ground integrated networks[J]. IEEE Transactions on Network Science and Engineering, 2026, 13: 3035-3052.

[18] Batool I, Fouda M M, Ismail M, et al. AMADRL: privacy-aware attention-based multiagent deep reinforcement learning for optimizing spectral allocation in 6G vehicular networks[J]. IEEE Internet of Things Journal, 2026, 13(3): 4792-4808.

[19] Chatzistefanidis I, Leone A, Nikaein N. Maestro: LLM-driven collaborative automation of intent-based 6G networks[J]. IEEE Networking Letters, 2024, 6(4): 227-231.

[20] Mekrache A, Ksentini A, Verikoukis C. Intent-based management of next-generation networks: an LLM-centric approach[J]. IEEE Network, 2024, 38(5): 29-36.

[21] Yao Z, Tang Z Q, Yang W M, et al. Enhancing LLM QoS through cloud-edge collaboration: a diffusion-based multi-agent reinforcement learning approach[J]. IEEE Transactions on Services Computing, 2025, 18(3): 1412-1427.

[22] Zhou L, Deng X F, Wang Z, et al. Semantic information extraction and multi-agent communication optimization based on generative pre-trained transformer[J]. IEEE Transactions on Cognitive Communications and Networking, 2025, 11(2): 725-737.

[23] Liu J L, Chen K Q, Liu R Y, et al. Alice-SLAM: accurate and lite-communication collaborative SLAM for resource-constrained multi-agent[J]. IEEE Journal on Selected Areas in Communications, 2025, 43(12): 4076-4090.

[24] Chang H G, Liu Y M, Sheng Z G. Distributed multi-agent reinforcement learning for collaborative path planning and scheduling in blockchain-based cognitive Internet of vehicles[J]. IEEE Transactions on Vehicular Technology, 2024, 73(5): 6301-6317.

[25] Yan S M, Shi L, Bu X H, et al. Barycentric coordination-based flocking behavior for nonlinear multi-agent systems with cooperation-competition interactions[J]. IEEE Control Systems Letters, 2025, 9: 2351-2356.

[26] Liu J D, Li T, Wang Q Y, et al. Unleashing collaborative potentials: multifaceted collaboration among agents in multitask Internet of things networks[J]. IEEE Internet of Things Journal, 2025, 12(14): 28121-28135.

[27] Lai J Y, Liu H S, Xu G Y, et al. Joint computation offloading and resource allocation for LEO satellite networks using hierarchical multi-agent reinforcement learning[J]. IEEE Transactions on Cognitive Communications and Networking, 2025, 11(4): 2554-2567.

[28] Chen X, Xiao B H, Lin X Y, et al. Multi-agent collaboration for vehicular task offloading using federated deep reinforcement learning[J]. IEEE Transactions on Mobile Computing, 2025, 24(9): 8856-8871.

[29] Yang T T, Feng P, Guo Q X, et al. AutoHMA-LLM: efficient task coordination and execution in heterogeneous multi-agent systems using hybrid large language models[J]. IEEE Transactions on Cognitive Communications and Networking, 2025, 11(2): 987-998.

[30] Matsumoto D, Watarai K, Okada S, et al. A2A routing service with MCP integration: bridging security, auditability, and governance in AI agent systems[C]//Proceedings of the 2025 IEEE International Conference on Computing (ICOCO). Piscataway: IEEE Press, 2025: 60-65.

[31] Feng H F, Zhang W T, Liu Y, et al. GNN-enabled multi-agent DRL for adaptive path selection in multi-network domains[J]. IEEE Transactions on Network Science and Engineering, 2026, 13: 130-145.

[32] Huang A R, Yan J F, Fan X J, et al. Multi-scenario cloud–edge collaborative DDoS detection in LLM-enabled AIoT[J]. IEEE Transactions on Network Science and Engineering, 2026, 13: 3790-3809.

[33] Huo X, Liu M X. Encrypted decentralized multi-agent optimization for privacy preservation in cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2023, 19(1): 750-761.

[34] Wen X R, Wen J B, Xiao M, et al. Defending against network attacks for secure AI agent migration in vehicular metaverses[J]. IEEE Internet of Things Journal, 2026, 13(3): 4153-4166.

[35] Chen J L, Lan X L, Zhang Q Q, et al. Defending against APT attacks in cloud computing environments using grouped multiagent deep reinforcement learning[J]. IEEE Internet of Things Journal, 2025, 12(12): 19459-19470.

[36] Hmimou Y, Tabaa M, Khiat A, et al. A multi-agent system for cybersecurity threat detection and correlation using large language models[J]. IEEE Access, 2025, 13: 150199-150215.

[37] 国家互联网应急中心. 关于国家授时中心遭受美国国家安全局网络攻击事件的技术分析报告[R]. 2025.
CNCERT. Technical analysis report on the cyberattack against the National Time Service Center by the U.S. National Security Agency[R]. 2025.

[38] Nour B, Pourzandi M, Debbabi M. Threatify: APT threat variant generation using graph-based machine learning[J]. IEEE Transactions on Network and Service Management, 2025, 22(5): 3978-3994.

[39] Mukherjee K, Kantarcioglu M. LLM-driven provenance forensics for threat investigation and detection[PP]. V2. arXiv (2025-11-17)[2026-02-04]. arXiv: 2508.21323.

[40] Siriwardhana Y, Porambage P, Liyanage M, et al. AI and 6G security: opportunities and challenges[C]//Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit). Piscataway: IEEE Press, 2021: 616-621.

[41] Hossain M N, Milajerdi S M, Wang J A, et al. SLEUTH: real-time attack scenario reconstruction from COTS audit data[C]// Proceedings of the 26th USENIX Security Symposium (USENIX Security 17). 2017: 487-504.

[作者简介]

黄奥然（1999– ），男，北京交通大学电子信息工程学院博士生，主要研究方向为智能体网络、网络安全。

周华春（1965– ），男，博士，北京交通大学电子信息工程学院副院长、博士生导师，主要研究方向为智能通信、移动互联网、大模型技术、网络安全与卫星网络。

闫竟夫（1996– ），男，北京交通大学电子信息工程学院博士生，主要研究方向为网络安全、智能通信。

范晓静（1999– ），女，北京交通大学电子信息工程学院博士生，主要研究方向为网络安全、卫星网络。