计算机科学
COMPUTER SCIENCE

攻击图辅助下基于深度强化学习的服务功能链攻击恢复方法

周德强, 季新生, 游伟, 邱航, 杨杰

引用本文

周德强, 季新生, 游伟, 邱航, 杨杰. 攻击图辅助下基于深度强化学习的服务功能链攻击恢复方法[J]. 计算机科学, 2026, 53(1): 371-381.

ZHOU Deqiang, JI Xinsheng, YOU Wei, QIU Hang , YANG Jie. Attack Graph-assisted Deep Reinforcement Learning-based Service Function Chain AttackRecovery Method [J]. Computer Science, 2026, 53(1): 371-381.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.250300076

攻击图辅助下基于深度强化学习的服务功能链攻击恢复方法

周德强[1]　季新生[1,2]　游　伟[1]　邱　航[1]　杨　杰[1]
1 信息工程大学信息技术研究所　郑州 450002
2 紫金山实验室　南京 210000
(zhoudeqiang0518@163.com)

摘　要　服务功能链(SFC)凭借按需编排、灵活组网等优势为6G六大场景提供定制化服务,6G网络则对服务功能链性能提出更高要求。弹性首次在6G网络中受到关注,要求服务功能链具备确保基本功能持续稳定的能力,其中弹性恢复是关键阶段。现有恢复方法往往基于备份机制,导致资源浪费,同时忽略了攻击路径对恢复的影响,导致恢复效果难以保证。因此,充分考虑网络攻击特征,利用服务功能链攻击图确定服务功能链,定制化攻击恢复方案,包括VNF恢复范围及攻击恢复等级需求。为进一步求解符合定制化攻击恢复方案的放置方案,提出了一种基于深度强化学习的服务功能链攻击恢复算法DRL-SFCAR。仿真结果表明,与现有方法相比,DRL-SFCAR在保证恢复成功率的同时,在时延和恢复成本方面表现优异,能够保证攻击恢复效果,同时最小化长期恢复成本,为网络攻击场景下的SFC恢复提供可行方案。

关键词:服务功能链;弹性恢复;攻击图;深度强化学习;成本
中图分类号　TN915

Attack Graph-assisted Deep Reinforcement Learning-based Service Function Chain Attack Recovery Method

ZHOU Deqiang[1],JI Xinsheng[1,2],YOU Wei[1],QIU Hang[1] and YANG Jie[1]
1 Institute of Information Technology,Information Engineering University,Zhengzhou 450002,China
2 Purple Mountain Laboratories,Nanjing 210000,China

Abstract　SFC can provide customized services for the six scenarios of 6G with the advantages of on-demand orchestration,flexible networking,and other benefits,and 6G networks also put forward higher requirements for SFC. Resilience is receiving attention for the first time in 6G networks,requiring SFC to ensure stable and continuous service provision of fundamental function,with resilience recovery being a key stage. Existing recovery methods are often based on backup mechanisms leading to resource wastage,while ignoring the impact of network attack characteristics on recovery leading to difficulty in guaranteeing the recovery effect. Considering the characteristics of network attacks,this paper uses SFC attack graph to determine the customized attack recovery scheme for SFC,including the VNF recovery range and the demand of attack recovery level. To solve the placement scheme that conforms to the customized attack recovery scheme,a deep reinforcement learning-based SFC attack recovery method (DRL-SFCAR) is proposed. Extensive simulation results show that DRL-SFCAR performs better in terms of delay and recovery cost than the three comparison methods while ensuring recovery success rate. DRL-SFCAR can meet the attack recovery level requirement and minimize the long-term recovery cost,which achieves the customized recovery for SFC in network attack scenarios.

Keywords　Service function chain,Resilience recovery,Attack graph,Deep reinforcing learning,Cost

1　引言

随着移动通信技术的迅猛发展,第六代移动通信技术(6G)受到广泛关注[1]。2023年国际电信联盟(ITU-R)审议通过报告《Framework and overall objectives of the future development of IMT for 2030 and beyond》[2],定义了6G网络沉浸式通信、极高可靠低时延通信等六大增强和拓展场景,导致6G网络为不同业务场景提供差异化服务面临巨大挑战。得益于网络功能虚拟化[3]和软件定义网络[4],网络功能与传统专用硬件实现解耦,形成虚拟网络功能(Virtual Network Function,VNF),并根据特定链式顺序构成服务功能链(Service Function Chain,SFC)[5]。SFC具有按需编排、灵活组网

到稿日期:2025-03-14　返修日期:2025-05-22
基金项目:国家重点研发计划(2022YFB2902204);河南省重点研发专项项目(231111211000);河南省顶尖人才项目(244500510012)
This work was supported by the National Key Research and Development Program of China(2022YFB2902204), Key Research and Development Project of Henan Province(231111211000) and Top Talent Training Project of Henan Province(244500510012).
通信作者:季新生(ndscjxs@126.com)

等优势，能够作为有效方案灵活为 6G 不同业务场景按需提供定制化服务。与 5G 网络相比，除峰值速率、连接密度等传统能力指标提升外，弹性作为 6G 网络的关键能力指标首次在报告中被提出[1]。与传统的安全性、可靠性、隐私保护不同，弹性强调在部分网络资源受攻击时仍能确保基本功能运行的能力，具备对不利因素的预防、抵抗、恢复和适应能力[6-7]。

然而，基础设施虚拟化、资源共享等带来了更多漏洞，包括网络功能虚拟化自身存在的漏洞[8-9]以及与 SFC 相关的漏洞[10]。攻击者不断探索并利用中间节点（包括物理机、虚拟机和 VNF，如图 1 所示）的漏洞对 SFC 发起攻击，导致 SFC 面临大量安全风险，致使 SFC 故障瘫痪，难以保证基本功能持续稳定运行。因此，恢复作为弹性的一个关键阶段，可实现 SFC 从攻击故障状态到正常服务状态的转换，在网络攻击场景下对确保 SFC 基本功能运行起着至关重要的作用。但 6G 网络环境下的 SFC 攻击恢复面临巨大挑战，动态性导致网络资源状态频繁波动，攻击路径可能随网络动态实时变化，传统静态恢复策略难以精准定位攻击位置；多租户资源共享引发跨服务链资源抢占与隔离失效风险，恢复过程须在多租户竞争环境下保证服务完整性与资源公平性；复杂攻击链通过多节点漏洞渗透形成隐蔽攻击路径，攻击者利用虚拟化层与物理层耦合漏洞实施跨层渗透，单一节点恢复无法阻断攻击链传播。

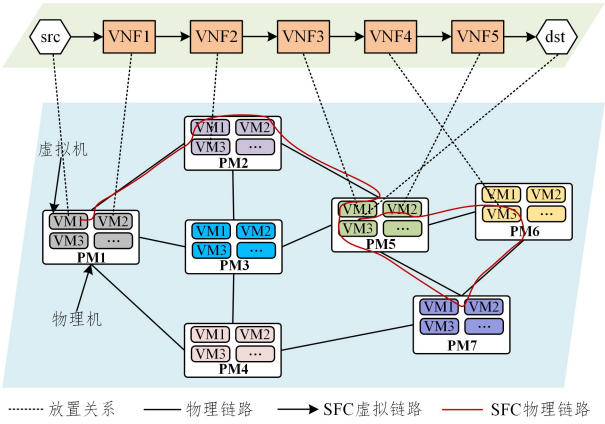


图 1 SFC 部署示意图

Fig. 1 SFC deployment figure

现有大量工作从响应恢复和主动恢复角度开展 SFC 恢复研究，但在应对网络攻击场景下的服务恢复时仍存在不足。一方面，主动恢复方法[11-16]大都基于静态备份机制，部署阶段为 VNF 预留静态备份资源以实现快速恢复，尤其是专用备份机制，这将导致极高的成本。响应恢复方法[17-19]则是在攻击故障发生后触发恢复操作，这将导致过长的服务中断时间。另一方面，现有恢复方法大都只对故障 VNF 执行恢复操作，然而现阶段网络攻击普遍演变为多阶段、多步骤形式，攻击者对目标 VNF 实施攻击需要攻破多个中间节点，即以攻击路径的形式对目标 VNF 发起攻击。由于攻击的隐蔽性，除目标 VNF 外，中间节点往往不会呈现故障状态，但中间节点已被攻击者所利用。此时，如果仅对目标 VNF 执行恢复操作，攻击路径仍然存在，极易对恢复的 VNF 再次发起攻击。因此，现有恢复方法不仅易造成资源浪费，更没有从网络攻击角度设计攻击恢复方法，难以保证攻击恢复效果。

我们以前的工作分析了在网络攻击场景下 SFC 恢复的特殊性，并提出 SFC 攻击图进行潜在攻击路径分析[20]，在此基础上，本文进一步解决攻击恢复等级约束的 SFC 攻击恢复问题。具体地，利用 SFC 攻击图分析 SFC 潜在攻击路径并进一步确定定制化恢复方案，包括 VNF 恢复范围及攻击恢复等级需求；然后采用深度强化学习算法求解满足攻击恢复等级需求的攻击恢复放置方法，以保证恢复效果。本文的主要贡献如下：

1）分析网络攻击对 SFC 恢复的影响，基于 SFC 攻击图和攻击成功阈值分析 SFC 攻击受损情况，并确定 SFC 的定制化恢复方案，包括被攻击 VNF 及攻击恢复等级需求；

2）建模攻击恢复等级约束的 SFC 攻击恢复问题，并将其转换为马尔可夫决策过程（Markov Decision Process，MDP），提出一种基于深度强化学习的 SFC 攻击恢复算法 DRL-SFCAR，其借助 Dueling DQN 为 SFC 求解满足最低攻击恢复等级的攻击放置方案；

3）评估分析了 DRL-SFCAR 算法的性能，结果表明其收敛速度快，能够在保证 SFC 攻击恢复效果的同时降低恢复成本。

本文第 2 章介绍了 SFC 恢复的相关研究；第 3 章回顾了网络攻击场景下 SFC 恢复的特殊性，并提出攻击恢复等级概念；第 4 章提出并建模攻击恢复等级约束的 SFC 攻击恢复问题；第 5 章提出了基于深度强化学习的 SFC 攻击恢复算法；第 6 章进行算法评估；最后总结全文。

2 相关工作

现有 SFC 恢复方法可以分为响应恢复和主动恢复两类。响应恢复是仅当网络攻击、随机性故障等原因造成服务故障后才触发恢复操作。Hu 等[17]提出一种 SFC 映射方法 Sur-SFC-E，以应对单节点故障造成的 SFC 故障。当网络中物理节点发生故障时，Sur-SFC-E 分析节点和链路资源情况，确定节点的优先级，并选择优先级最高的节点对故障节点上的 VNF 进行恢复。Cao 等[19]提出一种调度框架 Sec-SFC-Intell，以处理一个或多个网络节点发生故障的情况，能够确保已部署 SFC 恢复并持续提供服务。Soualah 等[18]提出一种链路恢复方法 R-SFC-MCTS，一旦基础设施链路发生中断，R-SFC-MCTS 立刻对受影响的虚拟链路进行重映射，以保证链路可达。然而，这些响应恢复方法只在故障发生后起效，资源准备、状态同步等过程将导致长时间的服务中断。为避免长时间的服务中断，主动恢复方法受到广泛关注，尽管其需要额外的成本和资源来提供备份。

主动恢复方法通过提前选择合适的放置和映射方案为 SFC 预留备份资源，以提供故障的快速恢复能力，具体可分为专用备份和共享备份。部分研究[11-13]通过 VNF 专用备份实现 SFC 快速恢复，一旦 VNF 发生故障，预留的专用备份 VNF 立刻上线替换故障 VNF 实现服务恢复。为了降低专用备份造成的大量资源预留问题，部分研究[14-16]推荐采用共享备份方式实现服务恢复。然而，共享备份方式导致多个 VNF

共享同一备份资源，一旦共享同一备份资源的多个 VNF 发生故障，仅能保证恢复其中一个 SFC，其余 SFC 故障仍难以解决。此外，为了尽可能缩短服务中断时间，部分研究[21-25]考虑基于故障预测的主动恢复方法。例如，Dong 等[23-24]提出的基于深度强化学习的异常流量感知方法可以实时监控网络传输，有效感知网络攻击。Fei 等[25]提出通过故障预测，在故障发生前进行虚拟机和流配置。Huang 等[21]则通过流量预测对可能过载的 VNF 提前准备实例，进而缩短配置造成的服务中断时间。尽管这些工作已经做出了很大努力，但基于备份的主动恢复方法所造成的资源浪费问题仍不容忽视。

总之，现有研究缺乏网络攻击场景下的 SFC 恢复能力。由于网络攻击的复杂性和隐蔽性，传统恢复方法不能从根本上消除 SFC 中的潜在攻击路径，难以保证网络攻击场景下的恢复效果。同时，资源备份导致的资源浪费问题也亟待解决。

3 攻击恢复模型

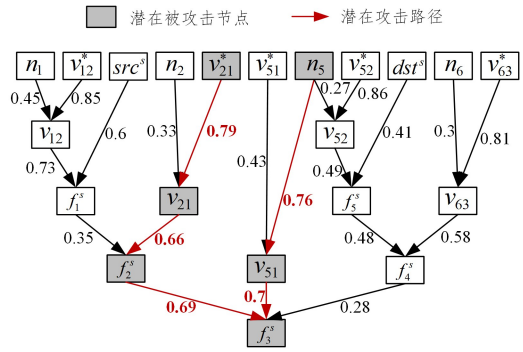
网络攻击具有隐蔽性，攻击者可以隐藏在任意物理机、虚拟机或 VNF 中，通过不断探索并利用 SFC 中间节点（包括物理机、虚拟机及 VNF）的漏洞对目标 VNF 发起攻击。目标 VNF 在受到网络攻击后呈现故障状态，中间节点虽未呈现故障状态，但已被攻击者所利用。如果恢复过程忽略攻击路径上的中间节点，攻击者则可以基于已有攻击条件快速对目标 VNF 再次发起攻击。我们先前的工作提出了 SFC 攻击图模型，其能够分析以任意 VNF 作为目标 VNF 时攻击者对 SFC 相关中间节点的攻击情况，实现对 SFC 中间节点的安全性分析。

假设 SFC s 中 VNFf_p^s 被攻击，潜在直连攻击路径包括：1）$f_{p-1}^s \rightarrow f_p^s$；2）$f_{p+1}^s \rightarrow f_p^s$；3）$pm_{f_p^s} \rightarrow vm_{f_p^s} \rightarrow f_p^s$；4）$vm_{f_p^s}^* \rightarrow vm_{f_p^s} \rightarrow f_p^s$。其中，$f_{p-1}^s$ 和 f_{p+1}^s 表示前后直连 VNF，$pm_{f_p^s}$ 和 $vm_{f_p^s}$ 分别表示放置 VNFf_p^s 的物理机和虚拟机，$vm_{f_p^s}^*$ 表示物理机 $pm_{f_p^s}$ 上除 $vm_{f_p^s}$ 之外的虚拟机。具体来看，潜在直连攻击路径包括：从前后相邻的 VNF 发起攻击，从所在物理机到所在虚拟机再到目标 VNF 发起攻击，以及从同驻虚拟机到所在虚拟机再到目标 VNF 发起攻击。因此，以受攻击 VNF 为根节点，沿 4 类潜在攻击路径进行反向查找，潜在攻击路径中的前后相邻 VNF 同样存在上述 4 类潜在攻击路径，依次反向查找，直至遍历完与 SFC 相关的所有 VNF、虚拟机和物理机。中间节点存在各类漏洞，攻击者可通过多漏洞结合和多方式选择对中间节点发起攻击，因此结合中间节点的漏洞分布情况、漏洞的通用漏洞评分系统（Common Vulnerability Scoring System，CVSS）评分和漏洞利用规则，可以得到潜在攻击路径的攻击概率[20]。基于此，SFC 攻击图被构建为一个权重为攻击概率的有向无环图。

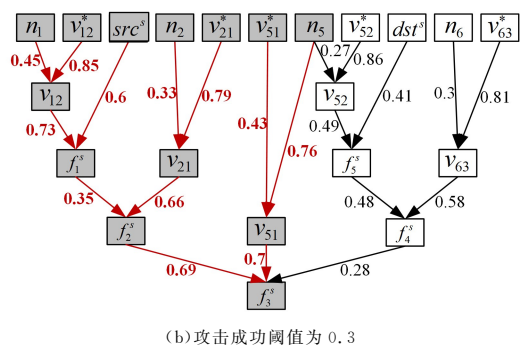
基于上述分析，SFC 攻击图可表示为加权有向无环图 $SFCAG=(S,A,P)$。其中，$S=S_{\text{ini}} \cup S_{\text{mid}} \cup S_{\text{end}}$ 表示与 SFC 相关的中间节点，包括 VNF、虚拟机和物理机。具体来看，$S_{\text{ini}}=\{src^s, dst^s, pm_{f_1^s}, \cdots, pm_{f_{|F^s|}^s}, vm_{f_1^s}^*, \cdots, vm_{f_{|F^s|}^s}^*\}$ 表示攻击图的初始节点，$S_{\text{mid}}=\{f_1^s, \cdots, f_{\text{attack}-1}^s, f_{\text{attack}+1}^s, \cdots, f_{|F^s|}^s, vm_{f_1^s}, \cdots, vm_{f_{|F^s|}^s}\}$ 表示攻击图的中间节点，$S_{\text{end}}=\{f_{\text{attack}}^s\}$ 表示被攻击的目标 VNF。$A \in S \times S$ 表示攻击图节点的有向边集合，方向表示攻击的因果关系。具体来看，对于任意有向边 $a_i \in A$，$a_i=pre(a_i) \rightarrow post(a_i)$，$pre(a_i)$ 表示有向边的起始节点，$post(a_i)$ 表示有向边的终止节点，即攻击者可以从节点 $pre(a_i)$ 发起对节点 $post(a_i)$ 的攻击。P 表示有向边的攻击转移概率，即攻击概率。对于任意有向边 $a_i \in A$，攻击转移概率 $P(a_i)$ 表示攻击者从 $pre(a_i)$ 发起对 $post(a_i)$ 攻击的成功概率。$P(a_i) \in [0,1]$，$P(a_i)$ 越小，攻击路径越难被利用。

SFC 攻击图能够直观呈现攻击者利用 SFC 中间节点探索攻击路径对目标 VNF 发起攻击的难易程度，但仅仅利用 SFC 攻击图确定 SFC 定制化攻击恢复方案是不够的。一方面，网络安全环境即攻击者的能力是能否探索并利用中间节点的关键，对于弱能力攻击者，只有攻击转移概率较大的有向边才能被利用，而强能力攻击者则可以利用攻击转移概率较小的有向边；另一方面，SFC 的安全需求也是影响恢复方案的关键因素，当安全需求较低时，只有攻击转移概率较大的有向边被视为潜在攻击路径，而当安全需求较高时，攻击转移概率较小的有向边也可被视为潜在攻击路径。因此，我们定义攻击成功阈值用于表示安全需求和攻击者能力，作为评判 SFC 有向边是否为潜在攻击路径的标准。当 SFC 攻击图中有向边的攻击转移概率大于攻击成功阈值时，该有向边被判定为潜在攻击路径。从目标 VNF 反推，即可得到所有潜在攻击路径，所有潜在攻击路径的起始节点和终止节点均被攻击者利用。

以图 1 中的 SFC 为例，图 2 分别展示了当攻击成功阈值为 0.5 和 0.3 时 SFC 攻击图的分析结果。图中节点包括组成 SFC 的 VNF 及其所放置的物理机和虚拟机，分别表示为 f_p^s，n_i 和 v_{ik}。v_{ik}^* 表示物理机 n_i 上除 v_{ik} 外的虚拟机。例如，VNFf_3^s 被放置在物理机 PM5 及 PM5 上的虚拟机 VM1，则 $pm_{f_3^s}=n_5$ 且 $vm_{f_3^s}=v_{51}$。



（a）攻击成功阈值为 0.5



（b）攻击成功阈值为 0.3

图 2 不同攻击成功阈值下 SFC 的攻击情况

Fig. 2 Attack analysis under different attack success threshold

从图 2(a)可以看到，当攻击成功阈值为 0.5 时，被攻击节点包括 VNF f_2^s 和 f_3^s，虚拟机 v_{21} 和 v_{51}，以及物理机 n_5。分析攻击图可知，VNF f_2^s 及其所放置的虚拟机 v_{21} 被攻击，为保证攻击恢复效果，至少应在原物理机上新建虚拟机并运行 VNF f_2^s，或将其迁移至安全虚拟机；VNF f_3^s 及其所放置的虚拟机 v_{51} 和物理机 n_5 均被攻击，仅在原物理机上新建虚拟机并运行 VNF f_3^s 难以保证攻击的恢复效果，物理机 n_5 极有可能再次攻击新建虚拟机并影响 VNF f_3^s，因此应将 VNF 迁移至安全物理机。除此之外，VNF f_5^s 同样部署在被攻击物理机 n_5 上，虽然 VNF f_5^s 暂时未被攻击，为保证安全性，同样应考虑对其进行功能迁移。

从图 2(b)可以看到，当攻击成功阈值为 0.3 时，SFC 攻击情况有所不同。分析攻击图可知，被攻击节点包括 VNF f_1^s，f_2^s 和 f_3^s，虚拟机 v_{12}，v_{21} 和 v_{51}，以及物理机 n_1，n_2 和 n_5。受攻击节点范围增大，包括 f_1^s，v_{12}，n_1 和 n_2，这就导致 SFC 攻击恢复范围和攻击恢复等级存在差异。相比图 2(a)所示情况，VNF f_1^s 也需要被恢复；此外，由于 VNF f_2^s 所放置的物理机 n_2 被攻击，仅仅通过新建虚拟机难以保证 f_2^s 的攻击恢复效果，因此应将其迁移至安全物理机。

通过上述分析可以发现，除了恢复范围有差异，VNF 的攻击恢复等级也存在差异，因此存在 3 种不同攻击恢复等级的恢复策略。

1)VNF 重启：在原虚拟机中重启 VNF 以消除攻击路径，适用于放置 VNF 的虚拟机和物理机均为安全状态的情况。

2)虚拟机重建：在原物理机中新建虚拟机并运行 VNF 以消除攻击路径，适用于放置 VNF 的虚拟机被攻击但物理机为安全状态的情况。

3)功能迁移：将 VNF 迁移至安全物理机上以消除攻击路径，适用于放置 VNF 的虚拟机和物理机均被攻击的情况。

3 种恢复策略的攻击恢复等级由低到高，攻击恢复效果越来越好，因此低攻击恢复等级需求采用高攻击恢复等级恢复策略能够保证满足攻击恢复效果，反之则不成立。然而，攻击恢复等级越高，所对应恢复策略的恢复成本也越高。与等级最低的 VNF 重启相比，虚拟机重建需要额外消耗虚拟机实例成本，功能迁移则需要额外花费虚拟机实例成本和消耗状态同步成本(VNF 状态信息跨节点传输以保证服务同步所花费的成本)。因此，基于 SFC 攻击图和攻击成功阈值，可以确定 SFC 攻击恢复范围和攻击恢复等级需求，确定当前网络安全环境下的最优定制化攻击恢复方案。此时，通过合适算法求解符合定制化攻击恢复方案的放置方案，便可在保证攻击恢复效果的情况下尽可能降低恢复成本。

4 问题建模

4.1 符号定义

1)物理网络：物理网络是一个无向加权图 $G=(N,E)$，其中 N 表示物理机集合，E 表示连接物理机的物理链路集合。任意物理机 $n_i \in N$ 具有有限数量的 CPU 资源 $C_{n_i}^{\text{cpu}}$，每一物理链路 $(n_i,n_j) \in E$ 具有有限数量的链路带宽资源 $C_{n_i n_j}^{bw}$，$d_{n_i n_j}$ 表示物理链路 $(n_i,n_j) \in E$ 的传输时延。

2)SFC 部署模型：本文针对已在物理网络中部署运行的 SFC 进行攻击恢复，可以表示为 $s=\{F^s, L^s, src^s, dst^s, bw^s, PM^s, VM^s, PL^s, D^s, C_s^{\text{syn}}\}$。其中，$F^s$ 表示构成 SFC 的 VNF 集合，L^s 表示从源节点 src^s 到目的节点 dst^s 连接 VNF 的虚拟链路集合，放置 VNF $f_p^s \in F^s$ 要求一定数量的 CPU 资源 $cpu_{f_p^s}$，映射虚拟链路 $(f_p^s,f_q^s) \in L^s$ 要求一定数量的链路带宽资源 bw^s。PM^s 和 VM^s 表示在物理网络中放置 VNF F^s 的物理机集合和虚拟机集合，其中 $pm_{f_p^s}$ 和 $vm_{f_p^s}$ 分别表示放置 VNF f_p^s 的物理机和虚拟机。PL^s 表示虚拟链路 L^s 映射所占用的物理链路集合，一条虚拟链路可能被映射至多条物理链路，因此 $pl_{f_p^s f_q^s}$ 表示虚拟链路 (f_p^s,f_q^s) 映射所占用的物理链路集合，D^s 则表示 SFC 映射后的物理传输时延。为保证攻击恢复效果，VNF 状态信息应保持同步，尤其当恢复策略为功能迁移时，状态信息需要跨节点传输，因此 $c_{f_p^s}^{syn} \in C_s^{syn}$ 表示 VNF f_p^s 的状态同步成本。

3)SFC 恢复请求：恢复请求，即定制化攻击恢复方案，可以通过 SFC 攻击图和攻击成功阈值获得。SFC 恢复请求包括恢复范围和攻击恢复等级需求，可以表示为 $\{RF^s, RL^s, RM^s\}$。其中，RF^s 表示需要执行攻击恢复操作的 VNF 集合，且 $RF^s \subseteq F^s$；RL^s 表示 VNF 恢复导致需要重映射的虚拟链路集合，且 $RL^s \subseteq L^s$。不同 VNF $f_p^s \in RF^s$ 要求的攻击恢复等级是不同的，通过攻击恢复向量 $\boldsymbol{rm}_{f_p^s} \in RM^s$ 表示。攻击恢复向量 $\boldsymbol{rm}_{f_p^s}$ 是一个三维向量，分别对应低、中、高 3 种攻击恢复等级，低攻击恢复等级需求可以采用高攻击恢复等级策略，反之不成立。例如，当放置 VNF f_p^s 的虚拟机受损但物理机未受损时，其攻击恢复向量可以表示为[0,1,1]，即所要求的最低攻击恢复等级为虚拟机重建，更高攻击恢复等级的功能迁移同样可被采用。

另外，定义以下决策变量来表示已部署 SFC 在物理网络中的放置方案。

1)二进制变量 $\alpha_{f_p^s}^{n_i}$ 表示 VNF f_p^s 是否被放置在物理机 n_i 上，如式(1)所示。

$$\alpha_{f_p^s}^{n_i}=\begin{cases}1, & f_p^s \text{ 放置在 } n_i, \text{即 } pm_{f_p^s}=n_i\\ 0, & \text{其他}\end{cases} \tag{1}$$

2)二进制变量 $\beta_{f_p^s}^{v_{ik}}$ 表示 VNF f_p^s 是否被放置在虚拟机 v_{ik} 上，如式(2)所示。

$$\beta_{f_p^s}^{v_{ik}}=\begin{cases}1, & f_p^s \text{ 放置 } v_{ik}, \text{即 } vm_{f_p^s}=v_{ik}\\ 0, & \text{其他}\end{cases} \tag{2}$$

3)二进制变量 $\chi_{f_p^s f_q^s}^{n_i n_j}$ 表示虚拟链路 (f_p^s,f_p^s) 是否被映射到物理链路 (n_i,n_j)，$(n_i,n_j) \in pl_{f_p^s f_p^s}$ 上，如式(3)所示。

$$\chi_{f_p^s f_q^s}^{n_i n_j}=\begin{cases}1, & (f_p^s,f_p^s) \text{被映射到} (n_i,n_j)\\ 0, & \text{其他}\end{cases} \tag{3}$$

本文的目标是根据定制化攻击恢复方案求解放置方案，需要定义相关恢复决策变量表示攻击恢复放置方案，即恢复后 VNF 的放置方案和虚拟链路的映射方案，因此与 $\alpha_{f_p^s}^{n_i}$，$\beta_{f_p^s}^{v_{ik}}$ 和 $\chi_{f_p^s f_q^s}^{n_i n_j}$ 相对应，$\alpha_{f_p^s}^{n_i *}$，$\beta_{f_p^s}^{v_{ik} *}$ 和 $\chi_{f_p^s f_q^s}^{n_i n_j *}$ 分别表示攻击恢复放置方案的决策变量，在此不过多解释。

4.2 攻击恢复等级约束的 SFC 攻击恢复问题

为保证攻击恢复放置方案的有效性，需要保证其满足攻

击恢复等级需求以及资源、性能等要求，因此定义以下约束。

1)攻击恢复等级约束。恢复方案应保证满足其最低攻击恢复级别需求。如果 VNF f_p^s 被放置到物理机 n_i 及其虚拟机 v_{ik}，即 $\alpha_{f_p^s}^{n_i\,*}=1$ 和 $\beta_{f_p^s}^{v_{ik}*}=1$，则可以通过与原部署方案进行比较，判断是否满足该约束。在攻击恢复向量约束下，只有当放置方案满足最低攻击恢复等级时，式(4)才成立，进而保证恢复效果。

$$\forall f_p^s\in RF^s,\text{if }\alpha_{f_p^s}^{n_i}=1\text{ and }\beta_{f_p^s}^{v_{ik}}=1,$$

$$\boldsymbol{rm}_{f_p^s}\cdot\begin{bmatrix}(\alpha_{f_p^s}^{n_i\,*}\cdot\alpha_{f_p^s}^{n_i})(\beta_{f_p^s}^{v_{ik}*}\cdot\beta_{f_p^s}^{v_{ik}})\\(\alpha_{f_p^s}^{n_i\,*}\cdot\alpha_{f_p^s}^{n_i})+(\beta_{f_p^s}^{v_{ik}*}\cdot\beta_{f_p^s}^{v_{ik}})\\1-(\alpha_{f_p^s}^{n_i\,*}\cdot\alpha_{f_p^s}^{n_i})-(\beta_{f_p^s}^{v_{ik}*}\cdot\beta_{f_p^s}^{v_{ik}})\end{bmatrix}=1\tag{4}$$

2)安全性约束。仅保证 VNF 满足恢复策略是不够的，还应保证 VNF 所放置的虚拟机和物理机是安全的。以一条由 3 个 VNF 组成的 SFC 为例，f_1^s 被放置在物理机 n_1 和虚拟机 v_{11}，f_2^s 被放置在物理机 n_2 和虚拟机 v_{21}，f_3^s 被放置在物理机 n_3 和虚拟机 v_{31}。通过分析其 SFC 攻击图，假设 f_1^s 和 f_2^s 的最低攻击恢复等级需求均为虚拟机迁移，即物理机 n_1 和 n_2 都存在安全风险，如果将 f_1^s 迁移到物理机 n_2 上，很明显满足攻击恢复等级约束，但是 f_1^s 仍被放置在风险物理机 n_2 上，这是不被允许的。因此，VNF 应避免放置到具有风险的虚拟机和物理机，如式(5)所示。

$$\forall s\in S,\forall f_p^s\in RF^s,\forall n_i\in N,\sum_{f_q^s\in RF^s}\boldsymbol{rm}_{f_p^s}(2)\beta_{f_p^s}^{v_{ik}*}\beta_{f_p^s}^{v_{ik}}=0\tag{5a}$$

$$\forall s\in S,\forall f_p^s\in RF^s,\forall n_i\in N,\sum_{f_q^s\in RF^s}\boldsymbol{rm}_{f_p^s}(3)\alpha_{f_p^s}^{n_i\,*}\alpha_{f_p^s}^{n_i}=0\tag{5b}$$

3)功能顺序约束。为保证攻击恢复后 SFC 功能正常运行，应保证数据从源节点按顺序流经各 VNF 直至目的节点。这种情况下，假设 f_p^s 和 f_{p+1}^s 被放置到物理机 n_i 和 n_j，那么虚拟链路 (f_p^s,f_{p+1}^s) 一定被映射到以物理机 n_i 为源节点的物理链路上和以物理机 n_j 为目的节点的物理链路上，如式(6)所示。

$$\begin{aligned}&\forall s\in S,\forall f_p^s\in RF^s,\\&\text{if }\alpha_{f_p^s}^{n_i\,*}=1,\sum_{n_k\in N}\chi_{f_p^sf_{p+1}^s}^{n_in_k\,*}=1\\&\text{if }\alpha_{f_{p+1}^s}^{n_j\,*}=1,\sum_{n_k\in N}\chi_{f_p^sf_{p+1}^s}^{n_kn_j\,*}=1\end{aligned}\tag{6}$$

4)流量守恒约束。流入任意物理机的流量和流出该物理机的流量应保持一致，如式(7)所示。

$$\begin{aligned}&\forall s\in S,\forall n_i\in N,\\&\sum_{(f_p^s,f_q^s)\in RL^s}\sum_{n_j\in N}\chi_{f_p^sf_q^s}^{n_in_j\,*}(+1\text{ if }n_i=src^s)=\\&\sum_{(f_p^s,f_q^s)\in RL^s}\sum_{n_j\in N}\chi_{f_p^sf_q^s}^{n_jn_i\,*}(+1\text{ if }n_i=dst^s)\end{aligned}\tag{7}$$

5)环路约束。任意虚拟链路映射到物理链路后不应形成环路，如式(8)所示。

$$\begin{aligned}&\forall s\in S,\forall(f_p^s,f_q^s)\in RL^s,\forall n_i\in N,\\&\sum_{n_j\in N}\chi_{f_p^sf_q^s}^{n_in_j\,*}\leqslant1\text{ and }\sum_{n_j\in N}\chi_{f_p^sf_q^s}^{n_jn_i\,*}\leqslant1\end{aligned}\tag{8}$$

6)时延约束。为保证服务质量，攻击恢复后 SFC 的时延应满足服务请求。文中只考虑传输时延，如式(9)所示。

$$\begin{aligned}&\forall s\in S,\sum_{(n_i,n_j)\in E}\sum_{(f_p^s,f_q^s)\in RL^s}\chi_{f_p^sf_q^s}^{n_in_j\,*}\cdot d_{n_i,n_j}+\\&\sum_{(n_i,n_j)\in E}\sum_{\substack{(f_p^s,f_q^s)\notin RL^s\\\text{and }(f_p^s,f_q^s)\in L^s}}\chi_{f_p^sf_q^s}^{n_in_j}\cdot d_{n_i,n_j}\leqslant D^s\end{aligned}\tag{9}$$

7)资源约束。所有 SFC 的 CPU 消耗不应超过物理机上的可用资源，同理，映射到物理链路上的流量不应超过链路的带宽容量，如式(10)所示。

$$\begin{aligned}&\forall n_i\in N,\sum_{s\in S}\sum_{f_p^s\in RF^s}\alpha_{f_p^s}^{n_i\,*}\cdot cpu_{f_p^s}+\sum_{s\in S}\sum_{\substack{f_p^s\notin RF^s\\\text{and }f_p^s\in F^s}}\alpha_{f_p^s}^{n_i}\cdot\\&cpu_{f_p^s}\leqslant C_{n_i}^{\text{cpu}}\end{aligned}\tag{10a}$$

$$\begin{aligned}&\forall(n_i,n_j)\in E,\sum_{s\in S}\sum_{(f_p^s,f_q^s)\in RL^s}\chi_{f_p^sf_q^s}^{n_in_j\,*}\cdot bw^s+\\&\sum_{s\in S}\sum_{(n_i,n_j)\in E}\sum_{\substack{(f_p^s,f_q^s)\notin RL^s\\\text{and }(f_p^s,f_q^s)\in L^s}}\chi_{f_p^sf_q^s}^{n_in_j}\cdot bw^s\leqslant C_{n_in_j}^{bw}\end{aligned}\tag{10b}$$

8)放置约束。任意需要恢复的 VNF 只能部署在一个物理机中的一个虚拟机上，不应重复部署，如式(11)所示。

$$\forall f_p^s\in RF^s,\sum_{n_i\in N}\alpha_{f_p^s}^{n_i\,*}=1\tag{11a}$$

$$\forall f_p^s\in RF^s,\sum_{v_{ik}\in n_i}\beta_{f_p^s}^{v_{ik}*}=1\tag{11b}$$

本文旨在保证 SFC 从网络攻击中恢复的同时降低攻击恢复所需要的成本，因此只考虑攻击恢复造成的成本。例如，无论采用何种攻击恢复等级，VNF 恢复占用的 CPU 资源是不变的，因此恢复成本不考虑 CPU 成本。首先，不同恢复策略所需要的恢复成本是不同的，相较于 VNF 重启，虚拟机重建会额外消耗虚拟机实例成本，功能迁移则额外消耗虚拟机实例成本和状态同步成本。此外，攻击恢复也会导致部分逻辑链路重映射，映射方案会影响带宽资源消耗的数量。因此，恢复成本考虑虚拟机实例成本、状态同步成本和链路成本 3 部分。

1)虚拟机实例成本。对于攻击恢复策略为虚拟机重建或功能迁移的 VNF，需要新建虚拟机运行 VNF，因此会消耗虚拟机实例成本。对于任意 SFC 恢复请求，虚拟机实例成本可以表示为：

$$C_{\text{vm}}=\sum_{f_p^s\in RF^s}[c_{\text{vm}}\cdot(\beta_{f_p^s}^{v_{ik}*}-\beta_{f_p^s}^{v_{ik}})(\text{if }\alpha_{f_p^s}^{n_i\,*}\beta_{f_p^s}^{v_{ik}*}=1)]\tag{12}$$

2)状态同步成本。对于攻击恢复策略为功能迁移的 VNF，还需额外消耗状态信息同步成本：

$$C_{\text{vm}}=\sum_{f_p^s\in RF^s}[c_{f_p^s}^{\text{syn}}\cdot(\alpha_{f_p^s}^{n_i\,*}-\alpha_{f_p^s}^{n_i})(\text{if }\alpha_{f_p^s}^{n_i\,*}=1)]\tag{13}$$

3)链路成本。对于攻击恢复等级为 VNF 迁移的 VNF，其所放置的物理机发生变化将导致物理链路相应变化，因此带宽成本也被纳入恢复成本，如式(14)所示。

$$C_{\text{bw}}=\sum_{(f_p^s,f_q^s)\in RL^s}\sum_{(n_i,n_j)\in E}(\chi_{f_p^sf_q^s}^{n_in_j\,*}\cdot bw_{f_p^sf_q^s})\tag{14}$$

综上，任意 SFC 攻击恢复请求的恢复成本可以表示为：

$$C=C_{\text{vm}}+C_{\text{syn}}+C_{\text{bw}}\tag{15}$$

基于上述分析，SFC 攻击恢复问题可以建模为 ILP 模型：

$$\begin{aligned}&\min C\\&\text{s. t. 式(4)}-\text{式(11)}\end{aligned}\tag{16}$$

5 DRL-SFCAR

为求解上述攻击恢复等级约束的 SFC 攻击恢复问题，获得放置方案，将 SFC 攻击恢复问题进一步建模为马尔可夫决策过程，并提出一种基于深度强化学习的 SFC 攻击恢复算法

DRL-SFCAR。DRL-SFCAR 基于 Dueling DQN 算法，通过分离状态价值和动作优势，能更稳定地学习攻击恢复策略，为恢复请求提供高质量攻击恢复放置方案。图 3 展示了 DRL-SFCAR 算法的整体框架。

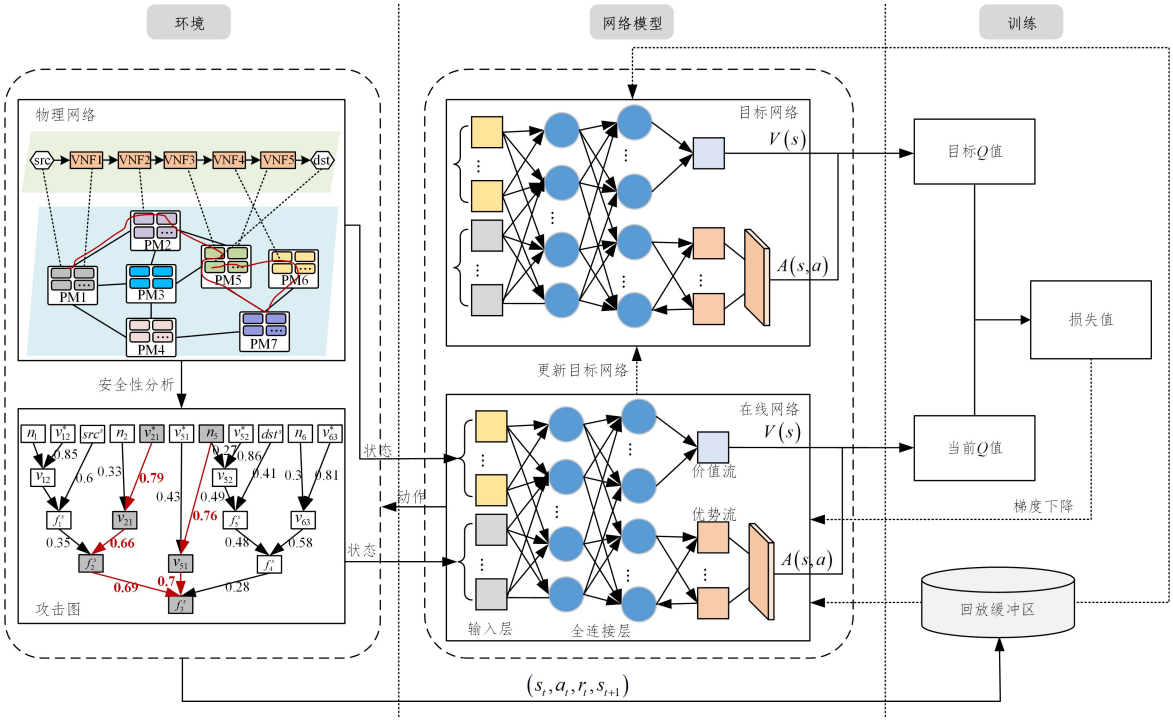


图 3 DRL-SFCAR 整体框架

Fig. 3 Framework of DRL-SFCAR

5.1 马尔可夫决策过程

DRL-SFCAR 在每一时间步为一个 VNF 求解放置方案，根据当前环境状态选择动作，环境通过执行选择的动作获得收益，并转换为下一状态，重复执行并学习上述过程，从而获得最大收益。首先将恢复问题转换为马尔可夫决策过程，包括状态、动作、收益。

状态：状态包括物理网络状态和恢复请求状态。其中，物理网络状态包括节点 CPU 资源 $C_{n_i}^{\text{cpu}}$ 和链路带宽资源 $C_{n_i n_j}^{\text{bw}}$，恢复请求状态包括 CPU 需求 cpu^t、带宽需求 bw^t、源节点 src^t、目的节点 dst^t 和攻击恢复等级需求 rm^t。因此，状态可以表示为：

$$s_t=\{C_{n_1}^{\text{cpu},t},\cdots,C_{n_{|N|}}^{\text{cpu},t},C_{n_1n_2}^{\text{bw},t},\cdots C_{n_1n_{2|E|}}^{\text{bw},t},cpu^t,bw^t,src^t,dst^t,\boldsymbol{rm}^t\} \tag{17}$$

其中，状态向量长度为 $|N|+|E|+7$。

对状态中的物理网络部分进行预处理，从而更准确地学习状态信息。具体来看，将网络资源情况与当前 VNF 资源需求进行比较，满足资源需求则对应状态位取 1，否则状态位取 0。状态中的 CPU 需求 cpu^t、带宽需求 bw^t、目的节点 dst^t 和攻击恢复等级 $\boldsymbol{rm}^t$ 可以直接从恢复请求中获得，而源节点 src^t 则与前一 VNF 放置方案相关，当前状态中的源节点 src^t 应为前一 VNF 所放置的物理机。

动作：动作应体现出 VNF 放置方案，包括是否 VNF 重启、是否虚拟机重建以及是否功能迁移及迁移到哪。动作可以表示为：

$$a_t=\{action\} \tag{18}$$

其中，$action\in[-1,|N|]$。$action=-1$ 表示 VNF 放置在原虚拟机实施 VNF 重启，$action=0$ 表示 VNF 放置在原物理机但新建虚拟机运行 VNF，$action\in[1,|N|]$表示 VNF 迁移至新物理机 $action$。

收益：为在保证 SFC 攻击恢复效果的情况下最小化恢复成本，收益应与恢复成本直接相关。恢复成本越小，收益越高；反之，收益越低。因此，将收益表示为成本的负数，并将失败动作（不满足攻击恢复等级或其他约束的放置方案）的收益值取 −20。收益可以表示为：

$$r_t=r(s_t,a_t)=\begin{cases}(C|s_t,a_t), & \text{恢复成功}\\ -20, & \text{恢复失败}\end{cases} \tag{19}$$

基于此，SFC 攻击恢复问题能够表示为马尔可夫决策过程，即$\{s_t,a_t,r,s_{t+1}\}$。

5.2 算法描述

DRL-SFCAR 采用 Dueling DQN 算法，DuelingDDQN 包括两个结构相同的网络，分别表示为在线网络 θ 和目标网络 θ^-，如图 3 所示。区别于传统 DQN 网络，Dueling DQN 将网络分为价值流和优势流，分别表示状态值函数 $V(s_t)$和优势函数，它们共享在线网络和目标网络的部分参数，只是在末端被分为价值流和优势流，其分别表示为 θ_v 和 θ_v^- 以及 θ_a 和 θ_a^-。状态函数表示状态的优劣，优势函数表示动作相较于其他动作的平均优势。优势函数可以表示为：

$$A(s_t,a_t;\theta,\theta_a)-\frac{1}{|A|}\sum_{a_t'\in A}A(s_t,a_t';\theta,\theta_a) \tag{20}$$

其中，$\frac{1}{|A|}\sum_{a_t'\in A}A(s_t,a_t';\theta,\theta_a)$表示当前状态所有动作的平均值。把价值函数和优势函数结合，可以得到代理在当前状态下执行动作的收益，即 Q 值，如式(21)所示。

$$Q(s_t,a_t;\theta,\theta_v,\theta_a)=V(s_t;\theta,\theta_v)+(A(s_t,a_t;\theta,\theta_a)-\frac{1}{|A|}\sum_{a_t'\in A}A(s_t,a_t';\theta,\theta_a)) \tag{21}$$

Dueling DQN 代理在与环境交互时进行观察。当有状态输入时，代理计算所有动作 $a_t\in A$ 的 Q 值，采用 ε-greedy 策略选择 Q 值最大化的动作，并得到其奖励值。然而，Q 值会在每次迭代中实时更新进行重置，因此目标网络的 Q 值可以表示为：

$$Q_t=r_t+\gamma\max_{a_{t+1}}Q(s_{t+1},a_{t+1};\theta^-,\theta_v^-,\theta_a^-) \tag{22}$$

其中，$\max_{a_{t+1}}Q(s_{t+1},a_{t+1};\theta^-,\theta_v^-,\theta_a^-)$ 表示状态 s_{t+1} 时最佳动作的收益，γ 表示收益的折扣因子。

Dueling DQN 的损失函数为均方误差，如式(23)所示。

$$L(\theta)=\mathbb{E}[(Q_t-Q(s_t,a_t;\theta,\theta_v,\theta_a))^2] \tag{23}$$

其中，$\mathbb{E}$表示取期望。基于损失函数，通过梯度下降法不断优化网络参数，并定期复制在线网络参数 θ 用于更新目标网络参数 θ^-。

DRL-SFCAR 的具体训练过程如算法 1 所示。算法输入包括学习率 LR、回放缓冲区容量 Z、奖励折扣因子 γ、目标网络更新频率 ω、训练批次 K、批大小 m 和探索率 ε，用于学习训练；输出是目标网络，求解攻击恢复放置方案。首先，初始在线网络、目标网络、回放缓冲区和环境，并根据环境和恢复请求确定初始状态 s_1（第 1－3 行）。然后，算法开始迭代训练，直至达到最大训练批次 K。在每次迭代中，代理根据ε-greedy 策略确定当前状态的动作 a_t，如果小于探索率 ε，则随机选择动作 a_t；否则利用在线网络选择具有最大收益的动作 $a_t=\max_{a_t}Q(s_t,a_t;\theta,\theta_v,\theta_a)$（第 6－7 行）。环境执行动作 a_t，计算当前状态 s_t 下选择动作 a_t 的收益 r_t，并转为下一状态 s_{t+1}，接着将四元组数据 (s_t,a_t,r_t,s_{t+1}) 更新到回放缓冲区（第 8－9 行）。如果缓冲区数据数量达到训练要求，则从缓冲区中随机选择 m 个四元组数据，根据式(22)分别计算各个数据的 Q 值，根据式(23)计算损失，并采用梯度下降法更新在线网络 θ（第 10－13 行）。更新探索率，并根据更新频率 ω 定期更新目标网络 $\theta^-\leftarrow\theta$（第 14－15 行）。至此，一个时间步完成，当完成所有迭代的所有时间步后，得到目标网络 θ^-，目标网络 θ^- 即可用于求解攻击恢复放置方案。

算法 1 DRL-SFCAR 训练过程

输入：学习率 LR，回放缓冲区容量 Z，奖励折扣因子 γ，目标网络更新频率 ω，训练批次 K，批大小 m，探索率衰减因子 d

输出：目标网络 θ^-

1. 初始化在线网络 θ 和目标网络 θ^-；
2. 初始化容量为 Z 的回放缓冲区 D；
3. 初始化环境并获取状态 s_1；
4. while episode=1,2,…,K do
5. for t=1,2,…,T do
6. 根据 ε-greedy 策略随机选择动作 a_t；
7. 否则选择动作 $a_t=\max_{a_t}Q(s_t,a_t;\theta,\theta_v,\theta_a)$；
8. 环境执行动作 a_t 并返回下一状态 s_{t+1} 和收益 r_t；
9. 将四元组 (s_t,a_t,r_t,s_{t+1}) 更新到回放缓冲区 D；
10. 从缓冲区 D 中随机采样 m 个数据 (s_i,a_i,r_i,s_{i+1})，i=1,2,…,m；
11. 根据式(22)计算 y_i，$y_i=r_i+\gamma\max_{a_{t+1}}Q(s_i,a_i;\theta^-,\theta_v^-,\theta_a^-)$；
12. 根据式(23)计算损失值；
13. 使用梯度下降法更新在线网络参数 θ；
14. 更新 ε-greedy 策略探索率 ε=ε·d；
15. 定期更新目标网络 $\theta^-\leftarrow\theta$；
16. end for
17. end for

5.3 复杂度分析

DRL-SFCAR 基于 Dueling DQN 算法，通过独立的价值函数和优势函数解耦状态与动作的共线。前向时间复杂度由 3 部分构成：共享层的矩阵运算（计算复杂度 $O(L_s\cdot M^2)$）、价值分支的标量输出（$O(M)$）以及优势分支的归一化操作（$O(M\cdot(|N|+2))$）。其中，L_s 为共享层数，M 为隐藏层维度，$|N|+2$ 为动作空间规模。因此，前向传播时间复杂度为 $O(L_s\cdot M^2+M\cdot(|N|+3))$。反向传播过程中，梯度须沿共享层和双分支回传，其时间复杂度与前向传播呈线性正比。空间复杂度则体现为双分支结构的参数量：价值函数分支的全连接层参数量为 M，优势函数分支参数量为 $M\cdot(|N|+2)$，结合共享层的 $L_s\cdot M^2$ 参数，总参数量为 $L_s\cdot M^2+M\cdot(|N|+3)$。经验回放缓冲区的存储需求为 $O(Z\cdot d)$，其中，Z 为缓冲区容量，d 为状态-动作对数据维度。

6 性能评估

6.1 实验设置

为验证 DRL-SFCAR 算法的性能，采用与文献[20]相同的实验环境和设置进行实验。具体地，在 Germany50 网络中部署 100 条 SFC，并随机选择 SFC 的 VNF 作为攻击目标 VNF，然后利用 SFC 攻击图生成在不同攻击成功阈值下的 SFC 恢复请求。其中，Germany50 拓扑由 50 个节点和 88 条边组成，每个节点的 CPU 资源为 48 核，每条边的带宽容量为 40 Gbps[26]，边的传输时延服从[2,4]ms 的均匀分布。每条 SFC 由 3 到 7 个 VNF 组成，其 CPU 需求服从[1,4]上的均匀分布，带宽需求从[100,150,200,250,300] Mbps 中随机选择[27]。不同 VNF 实现状态同步所传输的数据量存在差异，因此状态同步成本服从[1,4]的均匀分布，虚拟机实例成本设置为 2。Dueling DQN 的具体网络参数和其他参数设置详见表 1。

基于上述设置，本实验在 Intel Core i7-7740@3.60 GHz 和 64 GB 内存的 Windows 上进行，实验结果使用 PyCharm 获得。

表 1 参数设置

Table 1 Parameter setup

实验参数	值
物理节点 CPU 资源	48
物理链路带宽资源	40
物理链路传输时延	[2,4]
攻击成功阈值	[0,1]
服务功能链 VNF 数量	[3,7]
VNF 的 CPU 资源需求	[1,4]
服务功能链带宽需求	[100,150,200,250,300]
状态同步成本	[1,4]
虚拟机实例成本	2
学习率	0.005
回放缓冲区容量	5000
奖励折扣因子	0.5
训练批次	1000
批大小	64
探索率衰减因子	0.995

6.2 实验结果

6.2.1 收敛性分析

首先，对 DRL-SFCAR 算法的收敛性展开分析。在攻击成功阈值为 0.5 的情况下得到 100 个攻击恢复请求，网络参数设置详见表 1，在此实验设置下，模型共进行 1000 轮训练。图 4 给出了累计收益的变化趋势。由图 4 可见，随着训练轮数的持续增加，每一轮的累计收益亦相应增长，且在训练至 500 轮之后，累计收益趋于稳定。结果充分表明，DRL-SFCAR 算法具备出色的稳定性与收敛性。

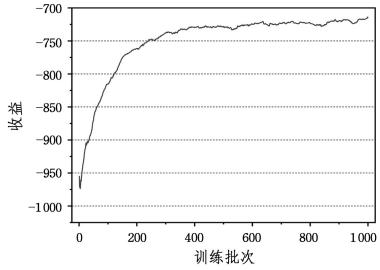
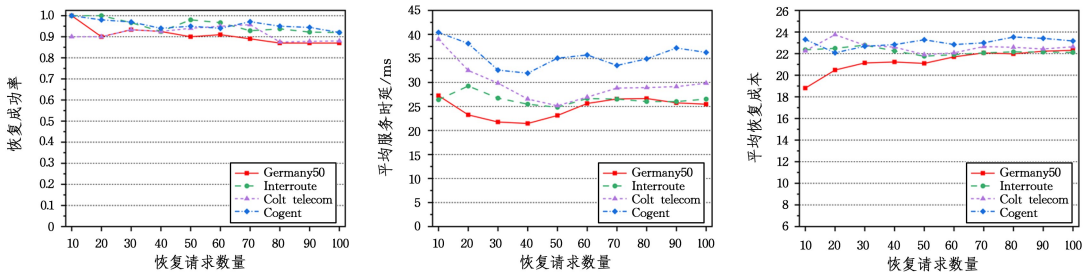


图 4 收益变化趋势

Fig. 4 Reward trend

6.2.2 性能分析

首先分析 DRL-SFCAR 算法在不同规模网络环境中的性能表现。实验选取了 4 个具有不同规模的网络，除 Germany50 网络外，还包括 Interroute 网络(110 个节点，147 条边)、Colt Telecom 网络(153 个节点，177 条边)以及 Cogent 网络(197 个节点，243 条边)。4 个网络中均部署了 100 条 SFC，并在攻击成功阈值为 0 的情况下分别得到 100 个攻击恢复请求。图 5 详细展示了 DRL-SFCAR 算法在不同规模网络下的性能情况。由图 5(a)可知，在上述所有测试网络中，DRL-SFCAR 算法均能够稳定地维持 90%的恢复成功率，这充分表明算法在不同网络拓扑中都具有很好的适应性。如图 5(b)所示，随着网络拓扑规模的增大，服务时延呈现出相应增大的趋势。这是由于网络规模增大使得数据传输过程中需要经过更多的物理链路，从而导致了时延的增加。然而，即便在这种情况下，DRL-SFCAR 算法依然能够确保恢复后的时延满足服务时延约束需求，体现了其在时延方面的优异性能。同理，随着网络拓扑规模的增大，链路映射过程中会占用更多的物理链路资源，从而带来更高的成本消耗。但如图 5(c)所示，无论何种测试网络，算法所产生的成本均能有效控制在 24 以下，这有力地证明了 DRL-SFCAR 算法在成本控制方面的优势。综上所述，DRL-SFCAR 算法展现出了良好的可拓展性和普适性，能够在不同规模的网络中为攻击恢复请求提供高效的恢复方案，有效应对网络规模变化所带来的挑战。



(a)恢复成功率 (b)服务时延 (c)恢复成本

图 5 不同网络下 DRL-AFCAG 的性能

Fig. 5 Performance of DRL-SFCAR in different networks

接着分析攻击成功阈值对 DRL-SFCAR 算法攻击恢复效果的影响。在攻击成功阈值从 0 至 1 的不同取值情况下，分别得到 100 个攻击恢复请求。图 6 直观呈现了不同攻击成功阈值下 100 条 SFC 所需恢复 VNF 的总数，以及对应 3 种攻击恢复等级的 VNF 数量分布情况。

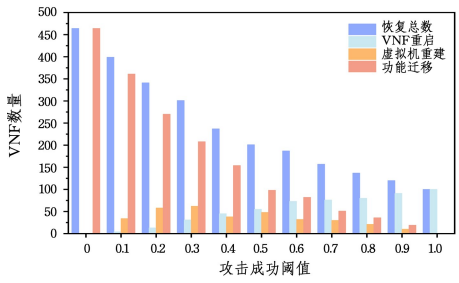


图 6 攻击成功阈值对攻击恢复等级的影响

Fig. 6 Impact of attack success threshold on attack recovery level

由图 6 可见，随着攻击成功阈值的增大，需要恢复的 VNF 数量呈现出递减趋势，整体上对攻击恢复等级的需求也降低。因为攻击成功阈值反映了安全需求以及攻击者能力，当攻击成功阈值增大时，在相同的网络环境中，攻击者对网络节点发起攻击的难度显著增加，受攻击影响的 VNF、虚拟机以及物理机的范围和数量均会相应减小，进而致使需要恢复的 VNF 范围缩小，较低的攻击恢复等级便足以保障攻击恢复效果。

图 7 和图 8 分别展示了不同攻击成功阈值下 SFC 的平均时延和平均恢复成本。图 7 呈现了不同攻击成功阈值下 SFC 的平均时延变化情况。从中可清晰看出，随着攻击成功阈值的持续增大，恢复后 SFC 的平均时延呈现出逐渐上升的态势。结合上述对图 6 的分析，攻击成功阈值越大，高攻击恢复级别需求的 VNF 数量越少。DRL-SFCAR 算法旨在降低恢复成本以获取更大的恢复收益，因而更倾向于采用满足最低攻击恢复等级的恢复策略。在此情形下，通常无需实施功能迁移方案，即放置 VNF 的物理机保持不变，这就使得攻击成功阈值越大，SFC 的时延越趋近于 SFC 初始部署时的时延；反之，服务时延则与 DRL-SFCAR 算法所求解的放置方案的性能紧密相关。因此，图 7 中 SFC 时延随攻击成功阈值的这种变化趋势，不仅充分体现了 DRL-SFCAR 算法对时延具备优化能力，也从侧面有力验证了该算法在时延方面的卓越性能。

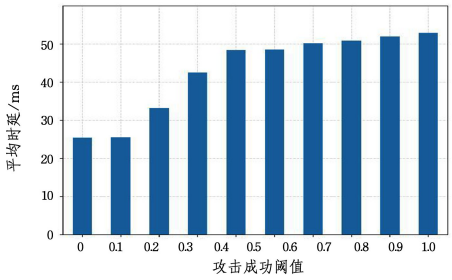


图 7 攻击成功阈值对时延的影响

Fig. 7 Impact of attack success threshold on delay

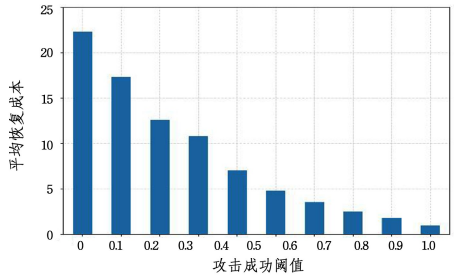


图 8 攻击成功阈值对恢复成本的影响

Fig. 8 Impact of attack success threshold on recovery cost

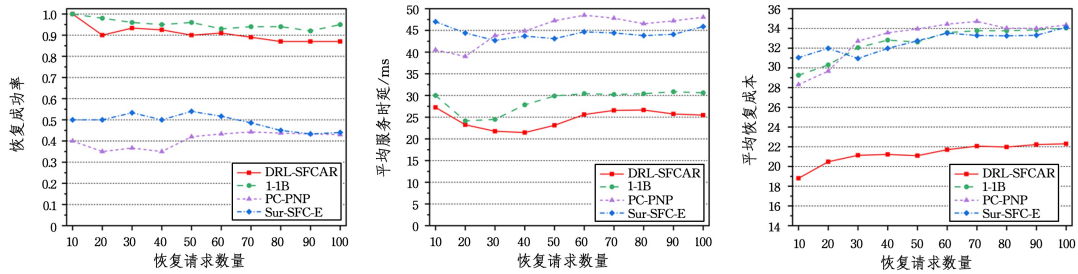
图 8 呈现了不同攻击成功阈值下 SFC 的平均恢复成本情况。由图 8 可见，随着攻击成功阈值的增大，SFC 的平均恢复成本呈现出逐渐降低的趋势。这主要归因于以下两个方面：一是当攻击成功阈值增大时，需要恢复的 VNF 数量显著减少，且高攻击恢复级别需求的 VNF 数量也随之降低。需同步状态的 VNF 数量减少，创建和维护虚拟机实例的数量亦相应减少，直接导致了状态同步成本以及虚拟机实例成本的降低。二是依据前文对时延的分析结果可知，随着攻击阈值的不断增大，恢复后 SFC 的平均时延逐渐减小，而时延与所占用链路的数量密切相关，平均时延减小意味着所占用链路数量相应减少，进而在一定程度上降低了带宽资源的消耗，最终促使恢复成本降低。

然而，需要特别注意的是，增大攻击成功阈值虽然能够有效降低攻击恢复成本，但同时也可能会忽略部分潜在攻击路径。因此，应综合权衡安全需求以及网络安全环境审慎确定攻击成功阈值，以实现攻击恢复成本与恢复效果之间的最优平衡，在保障网络安全的前提下，最大限度地优化资源利用和成本效益。

6.2.3 性能比较

为证明所提算法的优越性，选择了 3 种恢复方案进行性能对比，包括 PC-PNP[15]，1-1B[13] 和 Sur-SFC-E[17]。其中，PC-PNP 是一种基于共享备份的主动恢复方法，通过物理节点对方式为节点上的 VNF 提供备份恢复，但一个物理节点可能是多个物理节点的备份节点。1-1B 是一种基于专用备份的主动恢复方法，即为每一 VNF 预留备份。Sur-SFC-E 是一种被动恢复方案，当 VNF 发生故障后，Sur-SFC-E 通过分析节点和链路资源等情况确定节点的优先级，并选择优先级最高的节点实现 VNF 恢复。为保证结果的一般性和有效性，恢复请求在攻击成功阈值为 0 时分析 100 条 SFC 的攻击图生成，此时，所有 VNF 都需要被恢复且要求最高攻击恢复等级。

4 种算法的性能比较结果如图 9 所示。



(a)恢复成功率 (b)服务时延 (c)恢复成本

图 9 4 种算法的性能比较

Fig 9 Performance comparison of four recovery algorithms

图 9(a)展示了 4 种方法的恢复成功率。可以看到，DRL-SFCAR 和 1-1B 的成功率显著高于 PC-PNP 和 Sur-SFC-E。其中，DRL-SFCAR 的成功率可达 95%，1-1B 的成功率为 87%。DRL-SFCAR 通过持续与环境进行交互，选择可获取最高累积收益的动作，以此确保恢复方案的有效性；并且，借助神经网络的强大计算能力，该算法在求解攻击恢复放置方案时具备极快的运算速度。反观 1-1B，通过遍历所有满足时延条件的路径来挑选合适的恢复方案，这使得其在服务接受率方面表现出色，然而，遍历操作耗时巨大，导致难以在短时间内完成恢复方案的求解。PC-PNP 作为一种共享备份方法，在面对多个占用相同备份资源的 VNF 同时恢复的复杂情况时，应对能力不足，从而导致恢复成功率较低。Sur-SFC-E 则依据节点和链路的资源状况选择最优恢复方案，但该方法难以保证恢复后的 SFC 时延满足既定需求，致使恢复成功率较低。

图 9(b)展示了 4 种方法的平均时延情况。总体而言，DRL-SFCAR 在时延控制方面表现最优，1-1B 次之，PC-PNP 和 Sur-SFC-E 表现较差。DRL-SFCAR 的平均服务时延集中在 20～27 ms 区间，而 PC-PNP 和 Sur-SFC-E 的平均时延大多超过 40 ms。即使 1-1B 将时延作为遍历条件求解恢复方案，其服务时延也集中在 24～31 ms。相较于其他 3 种方法，DRL-SFCAR 的平均服务时延降低幅度约为 17%～48%。

图 9(c)对比了 4 种方法的平均恢复成本。显然，DRL-SFCAR 的恢复成本远低于其他 3 种方法。这主要源于 DRL-SFCAR 摒弃了主动式恢复方法中的资源备份模式，同时依据网络安全环境确定攻击恢复等级，有效避免了因盲目追求恢复效果而造成的成本浪费。1-1B 和 PC-PNP 均采用主动预备份方式，不可避免地会占用大量资源，进而导致恢复成本居

高不下。尽管 PC-PNP 采用共享备份方式，在一定程度上降低了备份成本，但其共享备份 VNF 的位置需兼顾多个 VNF，导致大量带宽资源的消耗。Sur-SFC-E 仅依据资源情况选择恢复位置，虽避免了备份成本，但与 PC-PNP 类似，恢复位置的选择同样会消耗大量带宽资源。此外，攻击成功阈值会根据安全需求和网络安全环境而动态变化。通过上述对图 8 的分析可知，当攻击成功阈值大于 0 时，攻击恢复成本会进一步降低。因此，DRL-SFCAR 在攻击恢复成本方面具有更为显著的优势。

综上所述，DRL-SFCAR 能够在确保高恢复成功率的基础上，在服务时延和恢复成本方面展现出最优性能，尤其是在恢复成本控制上优势明显。故而，DRL-SFCAR 作为一种高效的 SFC 攻击恢复算法，能够在 SFC 攻击图的辅助下，紧密结合安全需求和网络安全环境，为 SFC 提供切实有效的攻击恢复放置方案。

结束语 本文考虑了网络攻击场景下的 SFC 攻击恢复问题，结合安全需求和网络环境，利用 SFC 攻击图和攻击成功阈值识别 SFC 中所有潜在攻击路径，实现潜在攻击路径上中间节点的攻击恢复。进一步，通过不同攻击恢复等级适应 VNF 的不同受攻击情况，以保证攻击恢复效果，同时避免盲目恢复造成的资源和成本浪费问题。为了求解符合攻击恢复方案的放置方案，提出了基于深度强化学习的 SFC 攻击恢复算法 DRL-SFCAR，该算法能够在符合攻击恢复等级的基础上显著降低攻击恢复成本，保证攻击恢复效果。仿真结果证明了 DRL-SFCAR 的性能。

参 考 文 献

[1] NA M, LEE J, CHOI G, et al. Operator's Perspective on 6G: 6G Services, Vision, and Spectrum[J]. IEEE Communications Magazine, 2024, 62(8): 178-184.

[2] ITU. Framework and overall objectives of the future development of IMT for 2030 and beyond[EB/OL]. https://www.itu.int/md/R19-WP5D/new/en.

[3] HERRERA J G, BOTERO J F. Resource allocation in NFV: A comprehensive survey[J]. IEEE Transactions on Network and Service Management, 2016, 13(3): 518-532.

[4] HALEPLIDIS E, PENTIKOUSIS K, DENAZIS S, et al. Software-defined networking(SDN): Layers and architecture terminology[R]. 2015.

[5] QUINN P, NADEAU T. Problem statement for service function chaining[R]. 2015.

[6] MOGYOROSI F, BABARCZI P, ZERWAS J, et al. Resilient control plane design for virtualized 6g core networks[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2453-2467.

[7] SARKAR S, VITTAL S. Locomotive 5g core for 6g ready resilient and highly available network slices and sfcs[C]// 2022 18th International Conference on Network and Service Management (CNSM). IEEE, 2022: 367-373.

[8] HE G, LIAO X, LIU C. A security survey of NFV: from causes to practices[C]// 2023 3rd International Conference on Consumer Electronics and Computer Engineering (ICCECE). IEEE, 2023: 624-628.

[9] MALEH Y, QASMAOUI Y, El GHOLAMI K, et al. A comprehensive survey on SDN security: threats, mitigations, and future directions[J]. Journal of Reliable Intelligent Environments, 2023, 9(2): 201-239.

[10] PATTARANTAKUL M, VORAKULPIPAT C, TAKAHASHI T. Service Function Chaining security survey: Addressing security challenges and threats[J]. Computer Networks, 2023, 221: 109484.

[11] WANG M, CHENG B, WANG S, et al. Availability-and traffic-aware placement of parallelized SFC in data center networks[J]. IEEE Transactions on Network and Service Management, 2021, 18(1): 182-194.

[12] QU L, ASSI C, SHABAN K, et al. A reliability-aware network service chain provisioning with delay guarantees in NFV-enabled enterprise datacenter networks[J]. IEEE Transactions on Network and Service Management, 2017, 14(3): 554-568.

[13] ZHAO J H, MA J, LI Q W, et al. Service Function Chain Deployment Method Based on VNF Divided Backup Mechanisms [J]. Computer Science, 2025, 52(7): 287-294.

[14] ALOMARI Z, ZHANI M F, ALOQAILY M, et al. On ensuring full yet cost-efficient survivability of service function chains in NFV environments[J]. Journal of Network and Systems Management, 2023, 31(3): 45.

[15] PENG C, ZHENG D, PHILIP S, et al. Latency-bounded off-site virtual node protection in NFV[J]. IEEE Transactions on Network and Service Management, 2021, 18(3): 2545-2556.

[16] TANG H B, QIU H, YOU W, et al. A Reliability-guarantee Method for Service Function Chain Deployment Based on Joint Backup[J]. Journal of Electronics & Information Technology, 2019, 41(12): 3006-3013.

[17] HU Y, GUO Y. Survivable service function chain mapping in NFV-enabled 5G networks[C]// 2021 IEEE 7th International Conference on Network Softwarization (NetSoft). IEEE, 2021: 375-380.

[18] SOUALAH O, MECHTRI M, GHRIBI C, et al. A link failure recovery algorithm for virtual network function chaining[C]// 2017 IFIP/IEEE Symposium on Integrated Network and Service Management (IM). IEEE, 2017: 213-221.

[19] CAO H, JINDAL A, HU H, et al. Secure and intelligent service function chain for sustainable services in healthcare cyber physical systems[J]. IEEE Transactions on Network Science and Engineering, 2022, 10(5): 2674-2684.

[20] ZHOU D Q, JI X S, YOU W, et al. DDQN-SFCAG: A service function chain recovery method against network attacks in 6G networks[J]. Computer Networks, 2024, 254: 110748.

[21] HUANG Z, HUANG H. Proactive failure recovery for stateful NFV[C]// 2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). IEEE, 2020: 536-543.

[22] ZHANG P，SHU S，ZHOU M C. Adaptive and dynamic adjustment of fault detection cycles in cloud computing[J]. IEEE Transactions on Industrial Informatics，2019，17(1)：20-30.

[23] DONG S，XIA Y，PENG T. Network abnormal traffic detection model based on semi-supervised deep reinforcement learning[J]. IEEE Transactions on Network and Service Management，2021，18(4)：4197-4212.

[24] DONG S，XIA Y，WANG T. Network abnormal traffic detection framework based on deep reinforcement learning[J]. IEEE Wireless Communications，2024，31(3)：9.

[25] FEI X，LIU F，XU H，et al. Adaptive VNF scaling and flow routing with proactive demand prediction[C]// IEEE INFOCOM 2018－IEEE Conference on Computer Communications. IEEE，2018：486-494.

[26] ERAMO V，MIUCCI E，AMMAR M，et al. An approach for service function chain routing and virtual function network instance migration in network function virtualization architectures[J]. IEEE/ACM Transactions on Networking，2017，25(4)：2008-2025.

[27] KIKUCHI H，TAKAHASHI K. Zipf distribution model for quantifying risk of re-identification from trajectory data[J]. Journal of Information Processing，2016，24(5)：816-823.

ZHOU Deqiang，born in 1998，postgraduate. His main research interests include 5G/6G network，network slicing and cyberspace security.

JI Xinsheng，born in 1968，Ph.D，professor. His main research interests include next-generation mobile communication，network architecture and cyberspace security.

（责任编辑：柯颖）

2025 年“CCF 博士学位论文激励计划”评选结果公告

CCF 博士学位论文激励计划为推动中国计算机领域的科技进步，鼓励创新性研究，激励计算机领域的博士研究生潜心钻研，务实创新，解决计算机领域中需要解决的理论和实际问题，表彰做出优秀成果的年轻学者而设立。

经评选，最终 10 篇论文（名单见附 1）入选 2025 年“CCF 博士学位论文激励计划”、5 篇论文（名单见附 2）获得 2025 年“CCF 博士学位论文激励计划”提名。

附 1：2025 年“CCF 博士学位论文激励计划”入选名单

姓名	论文题目	培养单位	导师
崔炜暄	低延迟高吞吐的神经网络推理系统研究	上海交通大学	陈全
方维	深度脉冲神经网络的学习算法研究	北京大学	田永鸿
国孟昊	基于注意力机制的视觉骨干网络	清华大学	胡事民
王登豹	机器学习中的置信度校准方法研究	东南大学	张敏灵
王浩天	因果启发的可信机器学习研究	中国人民解放军国防科技大学	杨学军
徐冬竹	运营化5G网络全程测量与关键性能优化技术研究	北京邮电大学	马华东
张凯羿	基于对称密码的后量子数字签名	上海交通大学	郁昱
周昆	基于预训练语言模型的文本表示学习方法研究与应用	中国人民大学	文继荣
陈小羽	临界条件下的快速吉布斯采样	南京大学	尹一通
李泽南	神经符号系统的非确定性管理研究	南京大学	吕建

附 2：2025 年“CCF 博士学位论文激励计划”提名名单

姓名	论文题目	培养单位	导师
唐楚哲	面向Web应用的可扩展事务型数据库关键技术研究	上海交通大学	陈海波
张铭	高性能内存事务处理系统关键技术研究	华中科技大学	华宇
王天佐	基于受限信息的因果推断理论与方法	南京大学	周志华
束俊	模拟学习方法论：理论，算法和应用	西安交通大学	徐宗本
高尚华	复杂场景的自适应视觉感知	南开大学	程明明