5G核心网安全事故智能协同应急响应体系设计

Design of Intelligent Collaborative Emergency Response System for 5G Core Network Security Incidents

牛金乐[1,2]，曹　静[3]，孙　健[1,2]，郭新海[1,2]（1. 中国联通研究院，北京 100048；2. 下一代互联网宽带业务应用国家工程研究中心，北京 100048；3. 中国联合网络通信集团有限公司，北京 100033）

Niu Jinle[1,2]，Cao Jing[3]，Sun Jian[1,2]，Guo Xinhai[1,2]（1. China Unicom Research Institute，Beijing 100048，China；2. Next Generation Internet Broadband Service Application National Engineering Research Center，Beijing 100048，China；3. China United Network Communications Group Co.，Ltd.，Beijing 100033，China）

摘　要：

5G核心网已成为推动社会数字化转型的关键基础设施。网络切片、SDN/NFV和边缘计算等技术在提高网络灵活性的同时，也扩大了攻击面，带来了切片隔离失效、控制面洪泛、IMSI欺骗等复杂安全威胁，传统静态规则和人工响应方式难以满足时效性与智能化需求。提出一种基于多模型协同的智能应急响应体系，该体系覆盖从异常感知、事故分析、策略执行、闭环反馈与模型自适应优化的全流程，兼顾实时性与准确性，为5G核心网安全应急响应提供了理论支撑。

关键词：

5G核心网；网络切片；多模型协同；应急响应

doi：10.12045/j.issn.1007-3043.2025.09.016

文章编号：1007-3043（2025）09-0087-06

中图分类号：TN915.08

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

5G core network has become a key infrastructure driving social digital transformation. Technologies such as network slicing, SDN/NFV, and edge computing have improved network flexibility, but also significantly expanded the attack surface, introducing complex security threats like slicing isolation failure, control-plane flooding, and IMSI spoofing. Traditional static rules and manual response methods struggle to meet the timeliness and intelligence requirements. An intelligent emergency response system based on multi-model collaboration is proposed, covering the entire process from anomaly perception, event analysis, policy execution, closed-loop feedback, to model adaptive optimization. This system balances real-time performance and accuracy, providing theoretical support for security emergency response in 5G core networks.

Keywords：

5G core network；Network slicing；Multi-model collaboration；Emergency response

引用格式：牛金乐，曹静，孙健，等. 5G核心网安全事故智能协同应急响应体系设计[J]. 邮电设计技术，2025（9）：87-92.

0 引言

随着5G网络在全球范围内大规模部署，其高带宽、低时延和海量连接能力广泛渗透到工业互联网、智慧城市、车联网等关键应用场景。5G核心网采用了基于服务的架构（SBA），这种架构将网络功能分解为多个独立的服务，实现了网络功能的灵活编排和部署，提升了网络的可扩展性和灵活性。与此同时，网络功能虚拟化（NFV）和软件定义网络（SDN）等新技术[1-2]也被广泛应用，使得5G核心网能够基于通用硬件平台运行，降低了硬件成本，提高了网络的运维效率。

虽然5G核心网在技术和应用上取得了显著进展，采用了更开放、动态的技术架构，但这些特性也打破了传统网络的“物理隔离”和“硬件封闭”优势，使得攻击入口从“有限固定”变为“多元动态”，攻击面随之增大，其面临的安全威胁日益严峻[3]，安全事故频发，给社会和经济带来了较大的负面影响。

1 5G核心网安全风险分析

5G核心网是支撑数字社会运行的关键基础设施，其安全稳定运行关乎通信服务、社会民生与经济发展

收稿日期：2025-08-04

全局。随着5G网络部署规模扩大、业务场景持续拓展，其面临的安全风险日益增大，安全事故频发。

1.1 典型事故案例

2022年7月8日，加拿大电信巨头Rogers公司因核心网络配置错误发生全国性断网事故，故障持续约26 h，超过1 200万用户的无线、有线及互联网服务受到影响。这一故障不仅导致手机通话、短信和数据服务中断，还波及银行支付系统、自动取款机、政府机构热线及911紧急呼叫等关键基础设施，甚至造成加拿大全国最大公交系统瘫痪、入境管理系统ArriveCan无法访问。

2025年4月，韩国电信运营商SK电讯因遭受黑客组织攻击，导致约2 300万用户的USIM卡关键数据泄露，成为韩国电信史上最严重的数据泄露事件之一。泄露数据涉及2 695万个IMSI单元、9.82 GB USIM数据及29万条IMEI记录，这些数据可能被用于SIM卡克隆、身份伪造和金融欺诈。事件导致约25万用户转投其他运营商，SK电讯被迫为所有用户免费更换SIM卡，并暂停新用户服务以应对信任危机。

2025年6月，越南第二大电信运营商Vinaphone的核心网网元突发故障，导致全国63个省市的服务节点同时瘫痪，3 000万用户断网长达5 h16 min。医院、金融交易、交通系统等关键领域陷入混乱，这暴露了核心网元局部失效后引发的连锁反应。

这些安全事故表明，5G核心网一旦出现安全问题，其影响范围将远远超出通信领域，可能波及到社会的各个层面，导致交通瘫痪、金融交易中断、医疗救援受阻等严重后果，对社会的正常运转和经济的稳定发展构成巨大威胁。因此，如何有效应对5G核心网面临的安全挑战，已成为当前通信领域亟待解决的重要问题。

1.2 主要风险分析

5G核心网主要风险架构如图1所示。

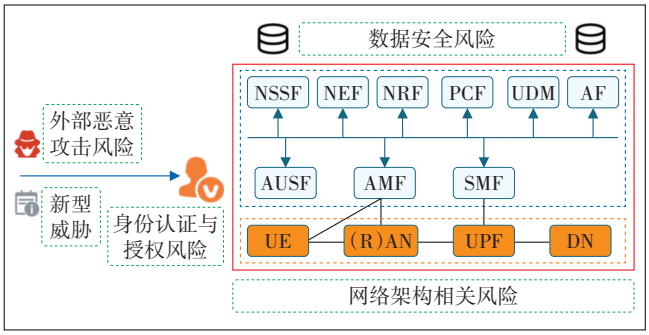

图1　5G核心网主要风险架构

1.2.1 网络架构相关风险

5G核心网采用SBA架构，网络功能（NF）以服务化形式部署，并通过标准化接口进行通信。这种架构虽然提高了网络的灵活性和可扩展性，但也带来了新的安全风险。在服务化架构方面，NF间接口缺乏有效的身份认证和访问控制机制，攻击者可能利用接口漏洞发起恶意调用，获取敏感信息或篡改网络配置；在网络切片方面，不同切片共享底层基础设施，若切片隔离机制存在缺陷，一个切片的安全漏洞可能扩散至其他切片，引发大规模网络故障。

1.2.2 数据安全风险

在5G核心网运行过程中，它无时无刻不在产生和处理海量用户数据与网络管理数据。用户数据涵盖个人身份信息、位置信息、通信内容等敏感信息，网络管理数据则包含网络拓扑、资源配置等关键信息。攻击者可通过中间人攻击、恶意软件感染等手段窃取、篡改或破坏这些数据。据IBM《2024年数据泄露成本报告》[4]，全球数据泄露事件的平均成本预计在2025年达到488万美元。一旦5G核心网数据泄露，不仅会损害用户隐私，还可能导致通信服务运营商面临法律诉讼和声誉损失。

1.2.3 身份认证与授权风险

5G网络支持多样化的应用场景和海量设备连接，传统的身份认证和授权机制难以满足其需求。部分物联网设备资源受限，无法运行复杂的认证协议，攻击者可能通过伪造身份凭证非法接入网络，获取网络资源或发动进一步攻击。同时，授权管理不当也会导致用户或设备获得超出自身权限的非法访问，从而对网络安全构成威胁。

1.2.4 外部恶意攻击风险

外部攻击者不断更新攻击手段，对5G核心网发起攻击。DDoS攻击仍是最常见的攻击方式之一，如攻击者通过模拟大量UE注册或恶意流量洪泛控制面网元，消耗其处理能力，导致核心网响应延时显著上升，最终影响多个切片业务的可用性与可靠性。漏洞利用攻击也是重要威胁之一，攻击者利用5G核心网系统、软件或协议中存在的漏洞，获取系统权限，实施破坏行为。随着5G与物联网、工业互联网的融合，来自这些领域的安全威胁也可能蔓延至5G核心网，形成复合型攻击。

1.2.5 新型风险挑战

随着技术发展，5G核心网面临的新型风险不断涌

现。人工智能驱动的自动化攻击工具愈发成熟，降低了黑客攻击的门槛。攻击者可以利用大模型，扫描网络漏洞、生成攻击策略，大幅提升攻击效率和隐蔽性。量子计算技术的发展对现有加密算法构成威胁，一旦量子计算机实用化，5G核心网采用的传统加密算法可能被破解，数据传输安全将面临严重挑战。

面对这些日益复杂的网络攻击，传统的静态规则和人工响应方式已难以在识别精度与响应速度方面有效应对，亟需构建一种全流程、闭环化、智能协同的安全应急响应体系，以保障5G核心网的稳定可靠运行。

2 智能协同应急响应体系设计

在应对日益复杂的5G核心网安全威胁时，防火墙和IDS等传统防护设备已经显得力不从心，难以有效应对。为此，本文结合人工智能算法，提出一种新的智能协同应急响应体系。该体系由监测预警层、智能分析层、决策执行层和反馈优化层4部分组成。

2.1 设计思路

监测预警层通过部署轻量化的Agent采集网络流量数据[5]，并依据专家经验对数据做初步判断；智能分析层采用专家规则、深度学习与图神经网络（GNN）协同工作的策略，形成“初步筛选→数据抽取→深入分析”3阶段多维智能识别机制，自动化地对网络事故信息做出准确判断；决策执行层依据智能分析层的分析结果，抉择并响应执行最优应对策略；反馈优化层通过综合分析网络中的多源数据，发现系统应对网络事故的不足，持续优化体系。

该体系通过监测预警层、智能分析层、决策执行层和反馈优化层4部分协同联动，形成“监测→分析→处置→优化”的闭环管理，确保其在实际应用中不断进化升级，持续筑牢5G核心网的安全防线[6]。5G核心网安全事故智能协同应急响应体系架构如图2所示。

2.2 监测预警层

监测预警层是5G核心网安全事故智能协同应急响应体系的第1道防线，其主要职责是通过部署多种先进的监测工具和技术，对5G核心网的运行状态进行全方位、实时的监测，及时发现潜在的安全事故，并发出准确的预警信息，为后续的应急响应工作提供及时、可靠的情报支持。

在5G核心网中，每天都有海量的网络数据产生，这些数据来自网元间通信交互的数据、网络设备的日志记录、用户的通信行为数据、网络流量数据等多个方面，这些海量数据的背后隐藏着大量有用信息，能最直观地反映当前的5G网络状态。

监测预警层采用分布式流量监测技术，在网络的关键节点，如核心网的边界、核心网内部的关键路由器和交换机以及关键网元（AMF、SMF、UPF及边缘MEC节点等）等位置，部署轻量级Agent监测探针，对网络流量进行实时采集和分析，用于捕获控制面和用户面的实时信令、流量和接口延迟等关键指标。Agent

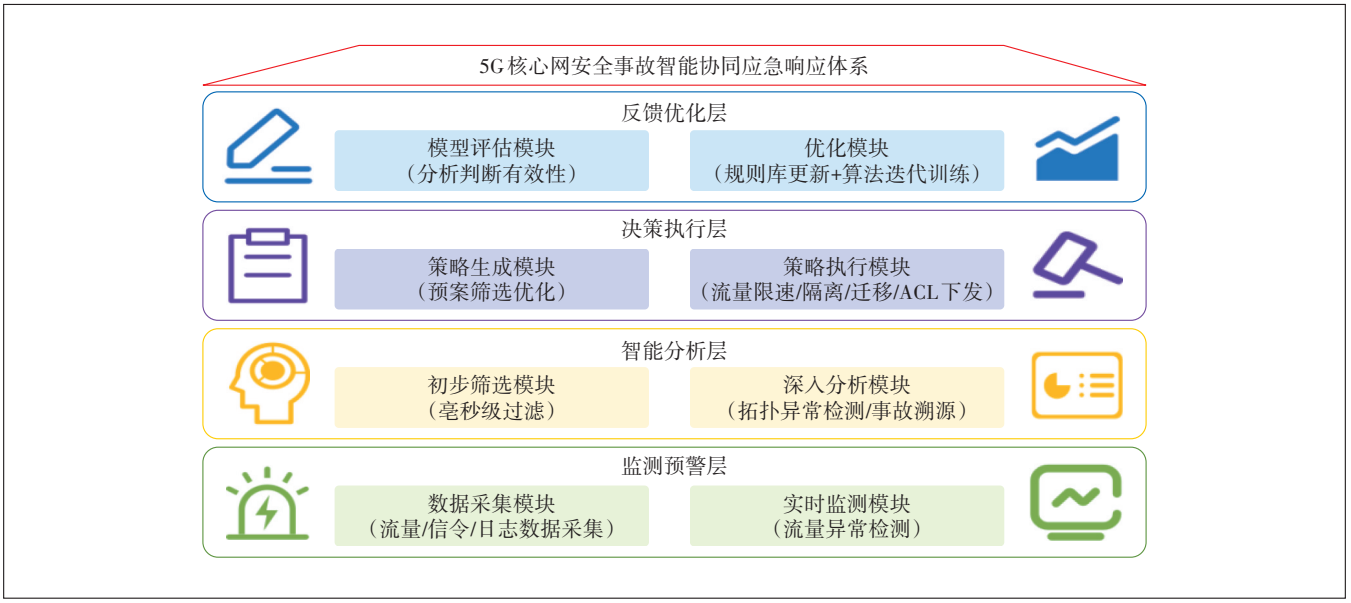

图2　5G核心网安全事故智能协同应急响应体系架构

可以对流量进行实时快照采集，当网络事故发生时，Agent可以检测到异常数据，并向系统发出告警信息，同时将采集到的数据下发给上层的智能分析模块，以便系统根据数据迅速分析网络状态，在网络事故发生时，快速做出响应。在应急通信场景中，轻量5G核心网通过分布式Agent实现快速部署与实时监测，确保网络状态的实时感知。监测预警流程如图3所示。

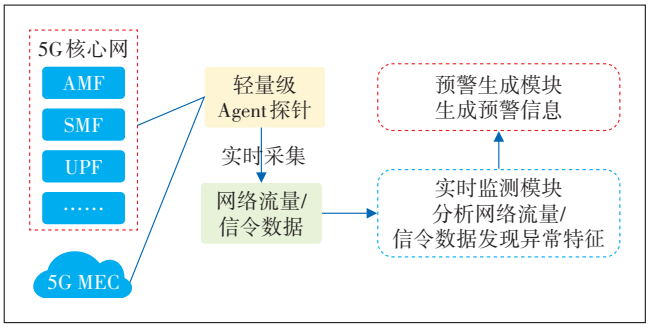

图3　监测预警流程

2.3 智能分析层

智能分析层在5G核心网安全事故智能协同应急响应体系中起着核心的分析判断作用。该层利用人工智能算法结合专家经验，对监测预警层采集的网络事故相关信息进行深入、全面的评估和分析，准确判断网络事故的类型、严重程度和影响范围，并制定出科学合理的应急响应策略，为决策执行层提供明确的行动指导。

智能分析层通过预设的专家规则库，利用AMF/SMF/UPF等网元的流量阈值、注册失败率和异常接口调用等规则进行初步判定，实现毫秒级的快速过滤，剔除误报流量。随后，将符合规则预警条件的事故流量输入训练好的CNN-LSTM深度学习模型，提取其空间特征和时序特征，捕捉流量间的隐藏信息；利用图神经网络（GNN）构建5G核心网功能拓扑图[7]，通过节点间关系捕捉跨切片、横向传播或API绕过类威胁，实现高维结构异常检测；系统通过专家规则库和多模型协同分析，共同发掘异常网络事故的类型，精确定位事故的源头，为后续应急决策的选择与执行提供重要依据。同时，系统可依据安全事故的影响范围、持续时间、造成的损失等因素，对安全事故进行量化评估，确定其严重程度等级，如Ⅰ级（特别重大）、Ⅱ级（重大）、Ⅲ级（较大）、Ⅳ级（一般）等。智能分析流程如图4所示。

2.4 决策执行层

决策执行层是5G核心网安全事故智能协同应急响应体系的具体行动实施者，负责迅速、准确地制定并执行应急响应策略。它通过采取一系列相应的技术手段和措施，对安全事故进行及时、有效的处置，尽快恢复5G核心网的正常运行，降低安全事故造成的损失和影响。

当安全事故发生时，系统基于智能分析层输出的安全事故评估结果，结合专家经验和预先建立的应急策略库，从应急策略库中筛选出相应的预案，并根据实际情况进行优化和调整。决策执行层结合零信任和最小权限原则，通过SDN控制器与切片Orchestrator协同作用[8]，将决策下发至相关NF，实现流量限速、资

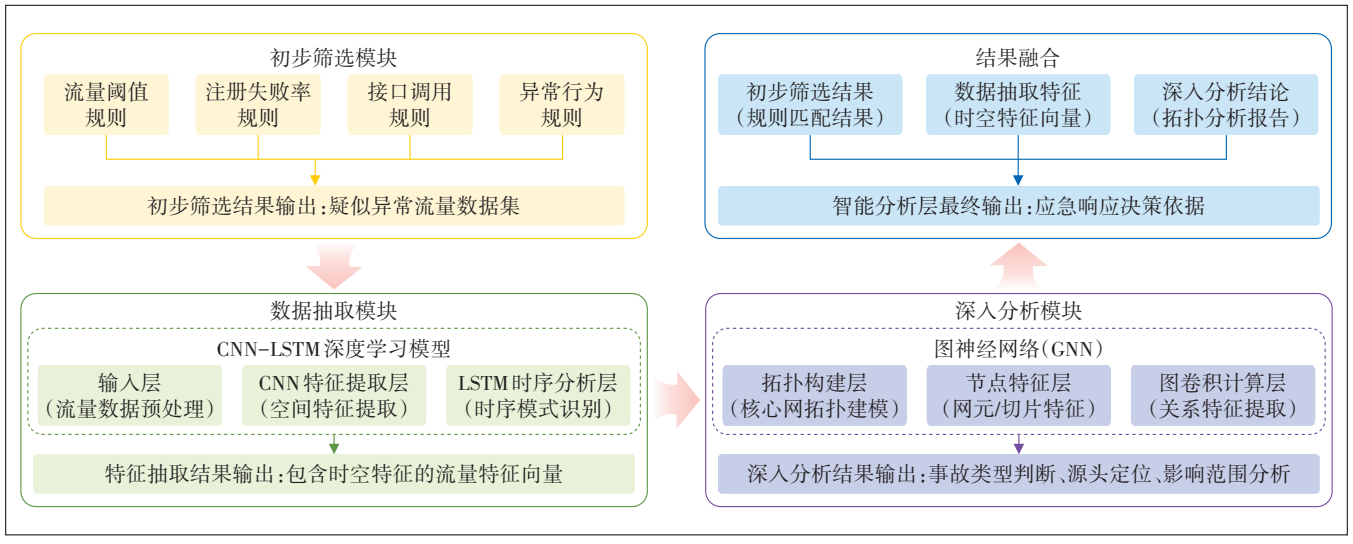

图4　智能分析流程

源隔离、跨切片迁移、ACL策略下发或边缘过滤等功能。切片Orchestrator负责对切片生命周期进行管理，当安全事故发生时，系统将攻击切片资源进行冻结或降权，将高优先级切片资源重分配以最大化业务可用性；对于高敏感业务，系统会智能化调度资源，实施跨切片迁移，将业务转入已知安全的切片，从而将事故影响最小化。

同时，系统还会考虑到应急响应过程中的风险和成本，在保障安全的前提下，选择最经济、最有效的应急响应策略。决策执行流程如图5所示。

2.5 反馈优化层

反馈优化层承担着“闭环学习”与对系统“持续优化”的重任。在每次安全事故处置过程中，系统会同时在监测预警层和决策执行层采集数据，这些数据包括Agent抓取的流量特征、决策执行层下发的策略版本、切片隔离与边缘拦截记录、执行结果及关键性能指标（如响应时延、误报率、业务恢复时间等）等。这些多源数据会被统一汇聚到日志中心，进行汇总分析。通过将5G核心网中的运行数据与模型判断输出进行关联，反馈优化层能够评估本体系的模型判断分析、决策策略制定和执行流程的有效性，为下一轮的规则调整与模型训练提供准确信息，这些信息可用于优化专家规则库、深度学习算法模型和应急策略库。反馈优化流程如图6所示。

2.6 协同机制

智能协同应急响应体系的核心优势在于各层、各组件之间的高效协同联动，通过跨层数据交互、技术组件联动及动态策略调整，该体系能够在复杂网络环

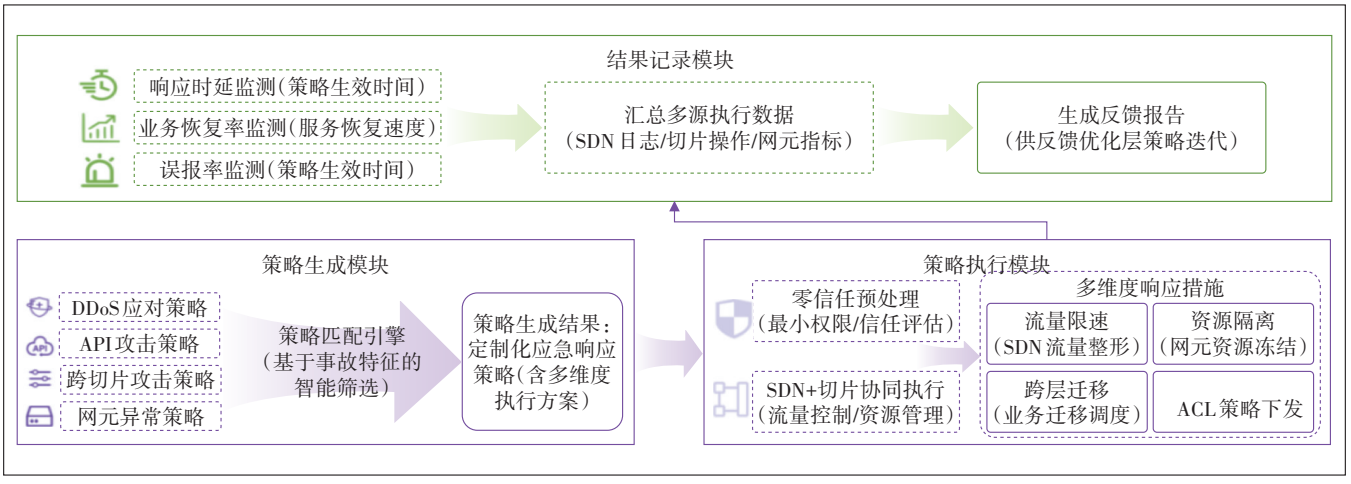

图5　决策执行流程

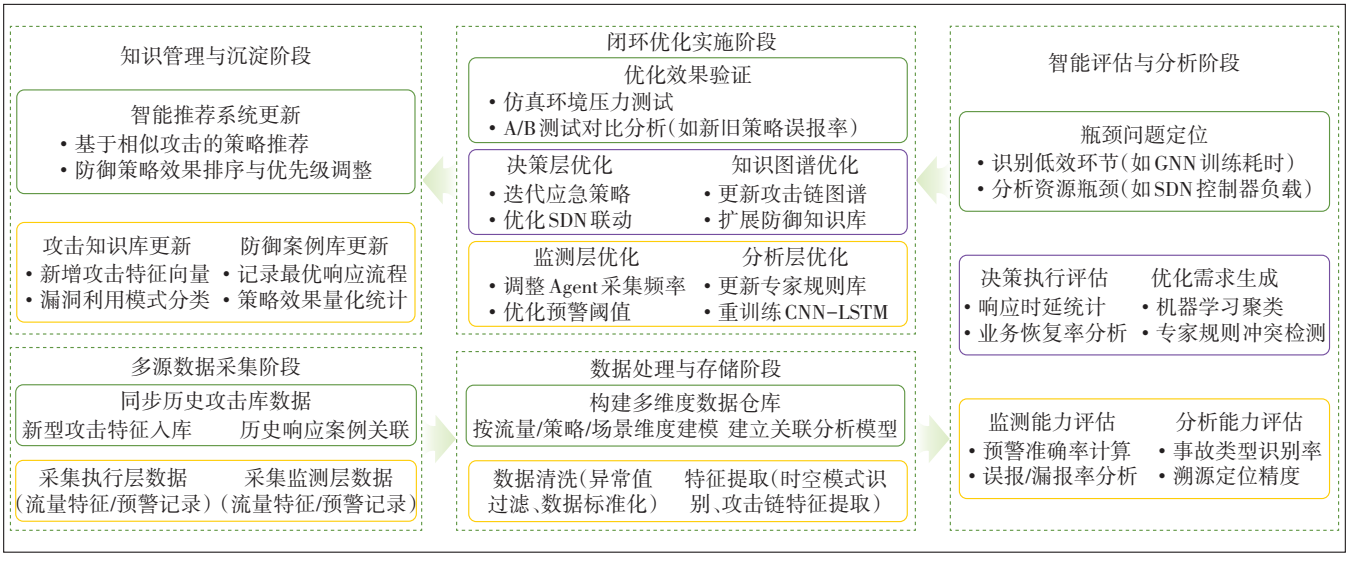

图6　反馈优化流程

境中实现快速响应与持续进化。

2.6.1 跨层协同机制

a）数据驱动的层间联动。监测预警层实时采集的流量，信令数据直接作为智能分析层的输入，经AI模型与专家规则分析后，将事故类型、源头定位等结果传递至决策执行层；决策执行层的策略效果通过反馈优化层进行汇总，反向优化监测规则、分析模型及策略库，形成数据闭环。

b）应急响应流程协同。各层以“事件驱动”模式协同工作。监测预警层触发异常告警后，智能分析层启动多模型联动分析机制，决策执行层根据分析结果自动匹配应急策略库，并通过SDN与切片管理组件执行响应措施，反馈优化层同步记录执行数据，以优化后续流程。

2.6.2 技术组件协同策略

a）AI模型与专家知识协同。智能分析层采用“专家规则+深度学习模型+图神经网络模型”的三模型协同架构。专家规则库实现毫秒级异常流量初筛，剔除误报流量数据；CNN-LSTM模型提取流量时空特征，捕捉隐蔽异常模式；GNN模型构建核心网拓扑图，识别跨切片、横向传播等复杂威胁。三者优势互补，既保证了响应速度，又提升了复杂攻击的检测精度。

b）网络控制与切片管理协同。决策执行层通过SDN控制器与切片Orchestrator的协同实现精细化响应。SDN负责用户面流量调度与控制面信令过滤，切片Orchestrator管理切片资源重分配。当面对DDoS攻击时，SDN实时限速并清洗恶意流量，同时切片Orchestrator将核心业务迁移至备用切片，确保服务的连续性。

2.6.3 动态反馈优化协同

反馈优化层通过多源数据聚合实现全体系协同进化。

a）监测与分析协同优化。基于历史攻击数据优化监测预警层的Agent采集策略，并调整智能分析层的模型参数。

b）决策与执行协同优化。根据策略执行效果，迭代应急策略库的响应模板，完善SDN与切片管理的联动逻辑。

3 体系运行成效

在实际运行中，体系通过监测预警、智能分析、决策执行与反馈优化这4层的协同运作，不仅能够对潜在风险进行前置感知与预警，还能借助人工智能与专家知识实现对网络事故的精准分析与溯源，并通过策略下发与切片调度，对突发安全事件进行快速响应与处置。同时，反馈优化机制确保系统在每一次安全事件后都能实现自我迭代与能力进化。

体系的落地与实践，能够有效提升5G核心网的攻击检测精度与响应速度。在应对DDoS攻击、APT攻击、信令风暴、跨切片渗透、0-day漏洞利用等多类型威胁时，该体系可大幅缩短应急响应时间，大大降低业务中断风险和经济损失，更好地保障5G网络的高可用性和可信性。

4 结束语

本文通过剖析5G核心网中的典型事故案例，深入分析了5G核心网面临的安全风险，基于此，构建了一套面向5G核心网的智能协同应急响应体系。该体系采用“边缘感知→多模型智能分析→零信任决策→自适应优化”的逻辑来实现，覆盖从异常感知、事故分析、响应决策、策略执行，到反馈优化的全流程，有效提升了5G核心网应对网络事故的实时性、准确性与智能化演进性，为5G核心网稳定运行提供了保障。

参考文献：

[1] 邱勤，刘胜兰，韩晓露，等. 5G应用安全参考架构与解决方案研究[J]. 信息安全研究，2020，6(8)：680-687.
[2] 郭威，欣娜，常艳生，等. 云化架构下的5G核心网灰度升级策略应用研究[J]. 邮电设计技术，2025(4)：19-24.
[3] 马宇威，杜海涛，粟栗，等. 基于数字孪生的5G网络安全推演[J]. 计算机工程与应用，2024，60(5)：291-298.
[4] IBM，Ponemon Institute. 2024年数据泄露成本报告（第19版）[R/OL]. [2025-07-04]. https://www.ibm.com/downloads/documents/cn-zh/107a02e94948f4ec.
[5] 洪生，王俊松. 基于实时大数据分析的流量异常检测研究[J]. 信息化研究，2023，49(4)：26-31.
[6] 殷炜. 基于多智能体的云网融合编排与调度研究[J]. 邮电设计技术，2025(4)：25-31.
[7] 韩建兴，李卓桐，井音吉，等. 联合网络拓扑与知识图谱的光网络多故障定位[J]. 光通信研究，2022(4)：27-30.
[8] 赵鹏，段晓东. SDN/NFV发展中的关键：编排器的发展与挑战[J]. 电信科学，2017，33(4)：18-25.

作者简介：
牛金乐，工程师，硕士，主要从事网络与信息安全研究工作；曹静，工程师，硕士，主要从事网络与信息安全管理工作；孙健，工程师，硕士，主要从事网络与信息安全研究工作；郭新海，工程师，硕士，主要从事网络与信息安全研究工作。