缓解嵌套 GTP 攻击：面向第五代移动通信及未来网络的闭环 eBPF 防御

征求反馈的作者稿——2026年11月24日

AbdulAziz AbdulGhaffar卡尔顿大学系统与计算机工程系，加拿大渥太华

Ashraf Matrawy卡尔顿大学信息技术学院，加拿大渥太华

arXiv:2611.29756v1 [cs.CR] 22 Nov 2026

摘要——**不断发展的蜂窝网络仍依赖传统的通用分组无线业务隧道协议用户面（GTP-U），以便在数据平面上封装并路由用户数据流量。近期安全研究表明，嵌套 GTP-U（GTP-in-GTP）载荷漏洞会使针对受害用户的多种攻击成为可能。为应对这一漏洞，本文提出一种基于扩展伯克利包过滤器（eBPF）和快速数据路径（XDP）的闭环防御方案，用于检测和缓解第五代移动通信及未来网络中的嵌套 GTP-U 攻击。该框架包含三个组件：内核中的 XDP检测与丢弃模块（XDP-DDM）、用户空间的用户面遥测代理（UP-TA），以及多线程控制平面缓解编排器（CP-MO）。**

我们在一个集成了 Free5GC、UERANSIM 和 Containerlab 的切片化第五代移动通信测试平台上实现并评估了拟议防御机制。实验结果表明，XDP-DDM 能够以线速检测并丢弃恶意嵌套 GTP-U 数据包，而 UP-TA 和 CP-MO 则分别异步报告并撤销攻击者的网络访问权限。在每秒 10,000 个数据包的跨切片嵌套GTP用户面洪泛攻击下，拟议解决方案在引入极小开销的同时，保持了受害切片的基线性能。我们还表明，拟议解决方案对用户吞吐量和往返时间的影响极小。

索引词—**第五代移动通信和第六代移动通信安全、闭环缓解、扩展伯克利包过滤器、XDP、GTP-U 封装、网络切片。**

1. 引言

随着蜂窝网络从第五代移动通信（第五代移动通信）迈向第六代移动通信（第六代移动通信），近期 3GPP 第20版标准化研究（6G系统架构，3GPP TR 23.801-1 [1],）指出，第六代移动通信将沿用现有的 5G 基于服务的架构（SBA）、控制面与用户面分离（CUPS）以及网络切片作为基线起点 [1]。然而，蜂窝网络的数据平面（DP）仍依赖传统的通用分组无线业务隧道协议用户面（GTP-U） [2]。

最近，Shaik 等人 [3], [4]在 2025 年 ACM 计算机与通信安全会议（CCS）上证明，仅使用一部智能手机和有效用户身份识别模块（SIM）的受控用户设备（UE），即可利用用户面功能（UPF）中 GTP-U 数据包处理的漏洞，跨六个第五代移动通信核心网（包括商用网络）实施严重的协议隧道和网络边界桥接攻击。由于新兴的第六代移动通信架构预计将保留 GTP-U 隧道，以便通过 N3 和 N9接口进行用户面转发 [1],，除非建立自动化的数据平面防御机制，否则这些底层协议漏洞将持续构成威胁，并直接遗留至第六代移动通信网络。

1.1. 问题陈述

GTP-U 最初在 2.5G/3G 网络中实现标准化，其设计目标是高吞吐量转发，而非抵御对抗性攻击 [3], [5]。在标准的第五代移动通信部署中，上行用户流量由服务 gNodeB（gNB）封装到外层 GTP-U报头中，该报头包含目标用户面功能的互联网协议（IP）地址以及用于用户设备（UE）的 32 位隧道端点标识符（TEID） [2], [3]。由于 GTP-U 缺乏源身份认证或递归载荷验证，标准的用户面功能实现仅验证最外层 GTP-U 报头，并将内部封装的载荷视为不透明的字节流 [3], [4]。

正如Shaik等人 [3]所证明的，已认证攻击者可通过向其合法上行隧道注入包含嵌套GTP-U报头（GTP-in-GTP）的精心构造数据包，滥用这种盲目解封装。当用户面功能剥离合法的外层GTP-U报头时，它未能检查内层协议层，并盲目地将内层伪造的GTP-U数据包路由回内部用户面或控制面接口。尽管Shaik 等人 [3]在未切片核心网中证明了这些利用，但该威胁在多租户5G/6G网络切片环境中会被进一步放大 [6]。

1.2. 研究动机

缓解嵌套 GTP-U 攻击至关重要，因其对合法用户的影响严重，且存在多向量利用 [7]。嵌套GTP-U封装并非导致单一攻击，而是作为“协议隧道”的一种高度可利用机制，这是MITRE FiGHT 框架正式认可的关键威胁类别 [8]。通过改变内层封装载荷，攻击者可以执行： ① 隧道端点标识符和会话端点标识符（*SEID*）枚举 [3]， ②直接用户设备到用户设备数据包注入 [3]， ③ 控制平面边界桥接（分组转发控制协议（PFCP）-in-GTP） [3],[9]， ④ 放大反射攻击 从而导致计费欺诈和配额耗尽 [3], [5], 以及 ⑤ 跨切片注入 [6]。因此，在UPF入口消除嵌套GTP-U封装对于消除这些攻击向量至关重要。

在本研究中，我们重点关注在 UPF 入口处消除 GTP-U 中嵌套 GTP-U 封装，同时指出，同一快速数据路径（XDP）解析流水线可直接扩展用于检测控制平面边界桥接，例如 GTP 中封装 PFCP。

1.3. 研究问题

本研究探讨如何直接在 UPF 数据面和 5G 核心网控制平面（CP）中构建自主、闭环、零信任防御。具体而言，我们针对三个核心研究问题（RQ）展开研究，它们直接指导我们的架构设计目标和实验评估：

RQ1（数据平面强制执行）： 如何在不显著影响合法流量性能的情况下，在 *UPF* 内以线速确定性地检测并丢弃嵌套 *GTP-U* 封装攻击？

- 我们通过第 4.2 节中的内核 XDP 检测与丢弃模块（XDP-DDM），以“轻量级处理”和“即插即用集成”设计目标应对这一问题，并在第 6.2 节和第 6.3 节中进行验证。

RQ2（非阻塞跨平面遥测）： 在容量洪泛期间，如何将内核中的高容量攻击检测结果传递到用户空间并跨越 *N4* 接口，同时避免引发告警风暴或造成 *CPU* 瓶颈？

- 通过我们的“高可靠性”设计目标予以解决：采用 10 秒 BPF最近最少使用（LRU）映射去抖机制，并结合第 4.2 节和第 4.3 节中的用户面遥测代理（UP-TA），相关效果已在第 6.3 节中量化评估。

RQ3（自动闭环会话撤销）： 在主动洪泛攻击期间，如何使第五代移动通信/第六代移动通信控制平面自主地将数据面威胁遥测数据转化为同步、永久的用户设备会话终止，并在 *3GPP* 基于服务的架构功能之间执行列入黑名单，同时保持受害切片韧性？

- 由多线程控制平面缓解编排器（CP-MO）与第五代移动通信在第 4.4 节中与控制平面网络功能（NF）交互，并在第 6.1 节中针对每秒 10,000 个数据包（包/秒）的洪泛攻击进行了评估。

1.4. 贡献

本文的主要贡献总结如下：

1）**闭环 eBPF/XDP 安全防御：**我们提出了一种新颖的闭环防御框架，能够实现内核空间数据面威胁缓解，并结合自动控制平面攻击者撤销，以抵御嵌套 GTP-U 攻击。a◯ **线速检测与遥测：**我们开发了附加在用户面功能 N3 入站接口上的内核 eBPF/XDP 程序（XDP-DDM），用于检查嵌套 GTP 头部，并在 $< 0.4\ \mu$ 秒内丢弃恶意数据包。借助 BPF LRU 映射执行 10 秒逐攻击者告警去抖，用户空间代理 UP-TA 将轻量级 JSON 告警分发至控制平面，在 ~ 1 毫秒内完成，同时不会造成用户面功能 CPU 瓶颈。b◯**自动控制平面撤销：**我们设计了一个多线程控制平面—移动性管理编排器（CP-MO）代理，将恶意内部 IP 地址解析为其 SUPI，并通过 SMF、接入和移动性管理功能以及统一数据存储库执行 3GPP REST API拆除，从而将攻击者永久列入黑名单。

2) **面向 5G/6G 的即插即用兼容性：**我们的 XDP-DDM 解决方案原生运行于 Linux 网络驱动程序中，在数据包到达 UPF 应用程序之前进行处理；它与底层 UPF 实现完全解耦。无需修改现有 VNF 源代码，即可将其无缝部署为安全层，适用于当前第五代移动通信和未来第六代移动通信架构中的任何基于 Linux 的 UPF。

3) **在切片式 5G 测试平台上进行实证验证：**我们在一个集成了 Free5GC、UERANSIM 和 Containerlab 的 5G 网络切片测试平台上部署并评估了拟议防御机制。在大规模跨切片嵌套GTP用户面洪泛攻击下，我们的防御机制成功抵御了攻击，并保护受害者的合法流量免受基线 UPF 所遭受的严重影响。为促进结果的可复现性，我们将核心 eBPF/XDP 模块、遥测/编排代理及部署脚本作为开源制品发布[1]。

本文其余部分安排如下。第 2 节回顾相关工作并明确研究空白。第 3 节定义系统假设与威胁模型，并说明攻击；第 4 节详细介绍所提出的闭环扩展伯克利包过滤器（扩展伯克利包过滤器）/XDP 防御。第 5 节概述第五代移动通信测试平台环境和评估方法，随后在第 6 节全面分析实验结果。

1. 源代码将在论文发表后公开，网址为: https://github.com/abdulazizag/Nested-GTP-Mitigation

本文的局限性将在第 7 节讨论，第 8 节概述本文的伦理考量。第9节总结全文。

2. 相关工作

本节综述与我们工作相关的三个领域的最新研究。表1总结了最密切相关的研究，并重点说明我们所提出的闭环 eBPF/XDP 防御如何推进该领域的最新水平。

2.1. GTP-U 协议漏洞与封装攻击

通用分组无线业务（GPRS）隧道协议用户面（GTP-U）是二十多年前为可信电信回程设计的，它仅依据 IP 地址和隧道端点标识符优先转发数据包，缺乏原生的源身份认证、完整性验证或递归载荷检查 [4]。近期进攻性安全研究表明，5G 用户面功能继承了这些根本性协议缺陷 [3]。

来自趋势科技研究的行业威胁情报 [10] 首次警告，专用5G网络中被攻陷的用户设备可注入畸形或嵌套GTP-U载荷，从而触发数据包反射并使未修补的用户平面功能崩溃，并建议采用具备蜂窝技术（CT）感知能力的深度包检测（DPI）防火墙进行缓解。在全球互联网范围内，Zhang 等人 [5] 扫描了公开暴露的GTP节点，并在众多提供商和国家中识别出约749,000台暴露主机。作者证明，攻击者可以利用这些漏洞实施各种攻击。与我们的工作不同，Zhang等人关注外部面向互联网的 GTP 暴露，并建议采用基于身份认证的协议替代方案，而不是防御内部 N3 用户面，以抵御经过身份认证的内部用户设备发起的跨切片嵌套 GTP-U 攻击。

Kwon等人 [9] 聚焦于源自已认证 UE 的内部威胁，证明了将 PFCP（GTP 中封装 PFCP）和 ICMPv6 封装在 GTP 载荷中，能够使恶意用户设备绕过数据平面隔离，并访问运营中的 5G 网络内的会话管理功能（SMF）和 UPF 节点。然而，尽管作者讨论了高层次的路由和访问控制列表（ACL）加固建议，但并未设计或通过实证评估可实施的反制措施来缓解这些攻击。

最近，Shaik 等人 [3], [4]在四个开源和两个商用第五代移动通信核心网中，评估了通过 GTP-U 中嵌套 GTP-U 数据包实现的协议隧道。通过利用可预测的隧道端点标识符分配和宽松的用户面功能路由，作者实施了多种攻击，包括直接的用户设备到用户设备的数据包注入和反射式计费欺诈。尽管 Shaik 等人概述了高层次的加固指南，但他们仅评估了未进行网络切片的核心网，既未设计或实证评估内核内防御，也未设计或实证评估自动化的闭环会话撤销框架。

2.2. 主动式与反应式 5G 网络切片防御

为防止一个网络切片中的攻击者降低共托管切片的性能，现有的网络切片安全文献大体遵循两种范式：通过数学优化实现主动式拓扑隔离，以及通过机器学习（ML）实现反应式异常检测。

在主动优化领域，Sattar等人 [11]提出了一种混合整数线性规划（MILP）模型，通过实施切片间硬件隔离（ISI）、切片内虚拟网络功能（VNF）分布以及专用安全虚拟机监控器区域，来缓解分布式拒绝服务（DDoS）洪泛攻击和切片发起的 CPU 耗尽攻击。基于 VNF 共享的数学建模，Mahyoub 等人 [12] 提出了一种 CP 过程级混合整数非线性规划（MINLP）模型，该模型利用最大 VNF 流量和外部暴露约束，限制 3GPP 流程之间的 VNF 共享。

Bolourian等人 [13] 提出了*5Guard*，这是一种端到端（E2E）隔离感知网络切片框架，旨在最大化基础设施提供商利润。然而，*5Guard*仅通过数值仿真评估资源开销，并未让切片经受真实网络攻击。AbdulGhaffar 和 Matrawy [6] 提出了跨多 UPF 数据路径的切片隔离即服务混合整数非线性规划（MINLP）框架，并在由 10 台虚拟机（VM）组成的 Free5GC 和诺基亚 Containerlab 测试平台上部署生成的拓扑，从而衔接了数学优化与实证验证。在流量型洪泛攻击和跨切片 GTP-in-GTP 反射攻击下进行的实证评估证明，在共享物理主机上仅采用逻辑 VNF 隔离、而不进行物理硬件隔离，会导致显著的性能下降。与我们的运行时数据平面防御不同，这些研究依赖离线数学模型，以主动式隔离切片并缩小攻击面。

另一方面，反应式切片防御依赖机器学习和深度学习（DL）异常检测器，例如 Khan 等人提出的*SliceSecure* [14]，、Javadpour 等人提出的基于强化学习的 DDoS 切片隔离 [20]，，以及 Yarkina 等人提出的无线接入网（RAN）性能隔离 [21]。这些反应式机器学习方法基于常规传输层洪泛数据集评估流级特征，而这些数据集不包含 GTP-in-GTP 协议漏洞利用；此外，它们的特征聚合和推理延迟过高，无法在高速率流量型洪泛攻击期间及时阻止 Linux 内核队列饱和。

2.3. 内核级 eBPF/XDP 与可编程 UPF 防御

近期研究还利用了第五代移动通信用户面功能（5G UPF）中的可编程数据平面（P4 和 eBPF/XDP）。Parola等人 [15]利用 Polycube 框架进行流量分类和服务质量（QoS）管理，展示了一个基于 eBPF/XDP 的早期 5G 移动网关概念验证。为将这一范式扩展至符合运营商级3GPP标准，

表1：相关工作在 第五代移动通信用户面安全、切片隔离和可编程数据平面方面的比较 es

参考文献	主要范围	防御范式	嵌套GTP-U检查	线速丢弃（μs级 XDP）	自动化3GPP UE撤销	实证5G攻击测试平台
Salim（趋势科技） [10]	5G 用户面（N3）	CT 感知深度包检测	✓	×	×	×
Zhang 等人 [5]	暴露的 4G/5G GPRS隧道协议	协议认证 / 审计	×	×	×	✓(Open5GS/Free5GC)
Kwon等人 [9]	5G 独立组网核心网（N3/N4）	路由 / 访问控制列表加固	✓(GTP 中封装 PFCP)	×	×	✓(运营商 / 5G 独立组网)
Shaik 等人 [3]	5G 独立组网核心网 (N2/N3/N4)	虚拟电厂/电池储能系统 规则 & 深度限制	✓	×	×	✓（6 个核心 +SDR）
Sattar 等 [11]	5G核心网切片	主动式 MILP 主机隔离	×	×	×	✓（OpenVZ虚拟演进分组核心网）
Mahyoub 等 [12]	5G 控制平面流程	主动式 混合整数非线性规划 VNF 共享	×	×	×	× (仿真)
Bolourian等（*5Guard*） [13]	端到端 5G 切片	在线 MIP 集成（L0–L2）	×	×	×	× （仿真）
AbdulGhaffar 与 Matrawy [6]	多 UPF 切片	主动式 物理/虚拟网络功能层级 混合整数非线性规划	× （拓扑的）	×	×	✓(Free5GC +Clab)
Khan等人（*SliceSecure*） [14]	5G 切片数据平面	反应式 DL 异常检测	×	×	×	✓(Free5GC)
Parola 等人 [15]	5G 移动网关	eBPF/XDP 转发与流量监管	×	× (仅流量监管)	×	✓(Polycube 概念验证)
Messaoudi等 [16]	5G UPF (N3/N6)	eBPF/XDP + tc HTB QoS	×	× (服务质量实施)	×	✓(100G OAI-UPF)
Akem & Fiore [17]	5G UPF数据平面	交换机内 P4 树机器学习 决策	×	✓(P4)	×	✓(Tofino交换机)
Repetto 等人（*ASTRID*） [18]	网络功能虚拟化 / 5G UPF边缘	eBPF边车 +ARIMA 控制器	×	∼ (∼ 2.4 s负载)	×	✓(Open5GS + Kubernetes)
Loureiro 等人 [19]	第五代移动通信控制平面（网络存储库功能）	XDP 固定窗口 SYN 过滤器	×	✓（仅 TCP SYN）	× (临时阻止)	✓(Open5GS)
拟议防御机制	**5G/6G 切片用户面功能**	**闭环 eBPF/XDP + UP-TA + CP-MO**	✓	✓（< 0.4 μ秒）	✓（会话管理功能/接入和移动性管理功能/统一数据存储库）	✓（**Free5GC +Clab**）

Messaoudi等人 [16]设计了一种高性能的 OAI-UPF，将 XDP、Linux流量控制（tc-bpf）和分层令牌桶（HTB）排队机制相结合，以实现服务质量实施、流量分类和转发。然而，Parola等人 [15] 和 Messaoudi等人 [16] 均严格聚焦于正常的 GPRS隧道协议数据包；其上行链路XDP解析器仅剥离单个外层 GTP-U报头，既不检查载荷中是否存在嵌套的GTP-in-GTP攻击，也不执行安全缓解。

多项研究已将可编程数据平面应用于第五代移动通信安全和DDoS缓解。Akem和Fiore [17]将训练好的基于树的机器学习分类器嵌入P4可编程用户面功能中，以亚微秒级线速对恶意5G流量进行分类。与运行于通用Linux用户面功能上的内核原生eBPF/XDP解决方案不同，Akem和Fiore的方案需要专用且昂贵的P4交换机，并且作为开环分类器运行，不具备自动化的3GPP控制面会话撤销功能。Repetto等人 [18]开发了一个eBPF框架，用于检测和缓解域名系统（DNS）放大攻击。

Loureiro等人 [19] 在Open5GS测试平台中实现了一个eBPF/XDP程序，以保护网络存储库功能免受传输控制协议（TCP）SYN洪水攻击。尽管该方案能有效保护网络存储库功能，但它只检查未封装的传输层TCP SYN标志，并临时限制连接速率，而不会解析N3 GTP-U用户面隧道，也不会永久终止遭到入侵的用户设备会话。

总结与研究空白：如表 1 所示，在保护第五代移动通信及未来第六代移动通信的用户面免受跨切片封装攻击方面，显然存在研究空白。

进攻性安全研究 [3], [5], [9], [10] 揭示了嵌套 GTP-in-GTP 和协议隧道攻击的严重性。主动式数学切片隔离模型 [6], [11]–[13] 只有通过配置专用物理服务器，才能防止跨切片泄漏。与此同时，现有的 eBPF/XDP 和可编程用户面功能研究要么只关注正常转发 [15], [16] ，要么不支持检查嵌套GTP-U 流量 [15]–[19]。

据我们所知，本研究首次设计、实现并通过实证验证了一种闭环 eBPF/XDP 安全防御，将亚微秒级（< 0.4 μ秒）嵌套 GTP-U 数据包丢弃、内核级去抖遥测，以及异步 3GPP 控制面会话撤销和恶意用户设备列入黑名单整合起来，以在共享用户面功能基础设施上保障跨切片服务质量。

3. 系统假设与威胁模型

为评估所提出的闭环防御，我们通过说明系统假设、对手能力和嵌套 GTP 攻击来界定威胁态势。

3.1. 系统假设

- **基础设施安全：**第五代移动通信核心网采用虚拟化架构，通过共享或隔离的虚拟化网络功能实现多个网络切片的部署。我们假设底层裸机硬件和虚拟机监控程序配置在物理上安全且不可篡改 [6], [22]。
- **控制平面隔离：**攻击面严格局限于数据面。控制平面网络功能（例如会话管理功能

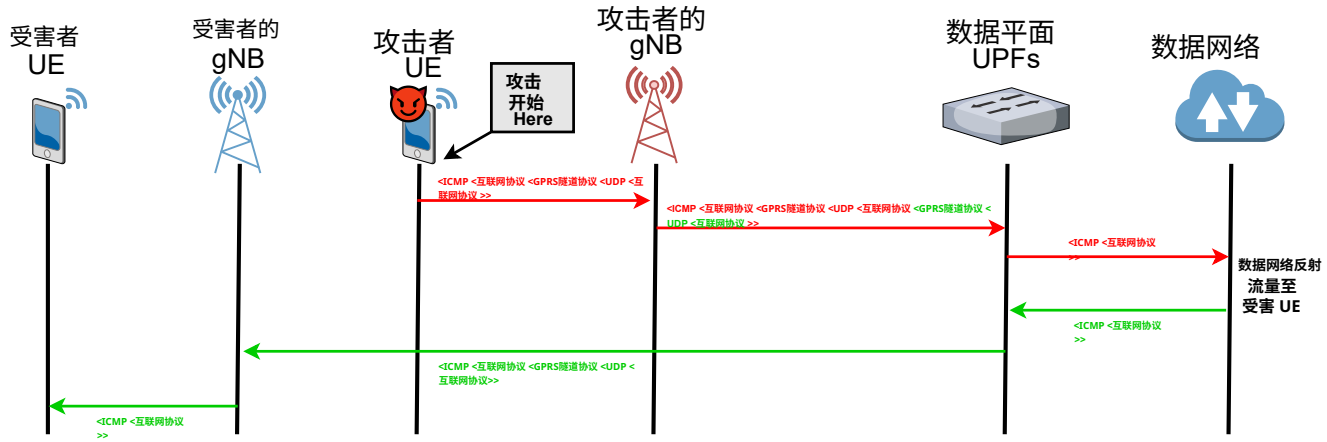


图 1：反射攻击序列图。红色箭头表示攻击流量。绿色表示合法流量，但会成为攻击的一部分。**注意：**攻击者的下一代基站不受攻击者控制，而是为攻击者（恶意用户）提供服务的合法下一代基站 [3]。（为节省空间，数据包头部按从内层到外层的简写顺序显示。）

和接入和移动性管理功能（AMF））彼此隔离，并受到保护，不受攻击 [6]。

- **对手接入：**攻击者被视为网络中的合法用户设备，但其行为具有恶意。用户设备成功完成初始身份验证和会话建立流程，获取合法的 IP 地址并接入网络切片 [3], [6]。

- **可信无线接入网与源 IP 绑定：**假设服务中的下一代基站是合法且未遭入侵的网络节点，能够使用有效的外层 GTP-U 头部和隧道端点标识符封装上行用户设备流量。此外，对于本文提出的控制面撤销机制，我们假设遭入侵的用户设备发送上行数据包时，在非嵌套内层 IP 头部中使用其合法分配的协议数据单元（PDU）会话 IP 地址，同时在嵌套 GTP-U 载荷中伪造受害者标识符。第 7 节讨论了放宽这一内层源 IP 假设，并将撤销机制扩展至外层 TEID 关联的影响。

3.2. 对手能力

- **协议操纵：**攻击者全面了解 3GPP 规范，因此能够以编程方式构造符合协议规范的互联网协议数据包 [3], [6]。
- **隧道注入：**攻击者将定制载荷直接注入上行数据流。服务中的下一代基站会盲目地将恶意载荷封装在合法的 GTP-U 头部中，并将其转发至用户面功能 [3], [6]。

- **侦察与欺骗：**攻击者通过探测、枚举或查阅文档，可以识别关键核心网组件。利用这些侦察结果，攻击者在嵌套载荷中伪造内部 IP 地址和隧道端点标识符，以利用 UPF 的解封装逻辑 [3], [6]。
- **流量型资源耗尽：**攻击者可以通过单个遭到入侵的 UE 生成泛洪流量。攻击者将此类流量型洪泛攻击与 GTP-U 协议隧道传输相结合，旨在中断受害 UE 的服务并实施计费欺诈 [6]。

3.3. 嵌套 GTP 攻击

Shaik 等人最近在 ACM CCS 上展示了这一针对 5G 网络的攻击 2025 [3]。由于用户面功能缺少嵌套 GTP 头部验证和路由逻辑强制执行机制，攻击者可以通过向受害者的上行 GTP 隧道注入流量来利用这一漏洞 [2], [23]。恶意行为者会构造一个针对受害者的非法 GTP-in-GTP 嵌套数据包，在伪造的内层 IP 和 GTP 头部中设置受害 UE 的 IP 地址和隧道端点标识符。此外，攻击者将内层目的 IP 地址设为受害者所连接的用户面功能，并将内层载荷（DNS 或互联网控制消息协议（ICMP）请求等）发送至公共服务器。

随后，攻击者将这一构造的数据包发送至各自的下一代基站。作为正常运行的一部分，下一代基站会添加外层 IP 头部（其中包含服务下一代基站和用户面功能的 N3 IP 地址）以及包含攻击者上行 TEID 的外层 GTP-U 报头，并将其转发至用户面功能。由于用户面功能缺乏嵌套 GTP 头部验证，它会解封装外层 GTP 报头，并根据内部格式错误的 GTP 报头对内层载荷进行路由。由于攻击者使用受害者的信息构造了内层报头，用户面功能会通过受害者的上行隧道路由该数据包，使其看起来像是源自受害 UE。由此，公共服务器的

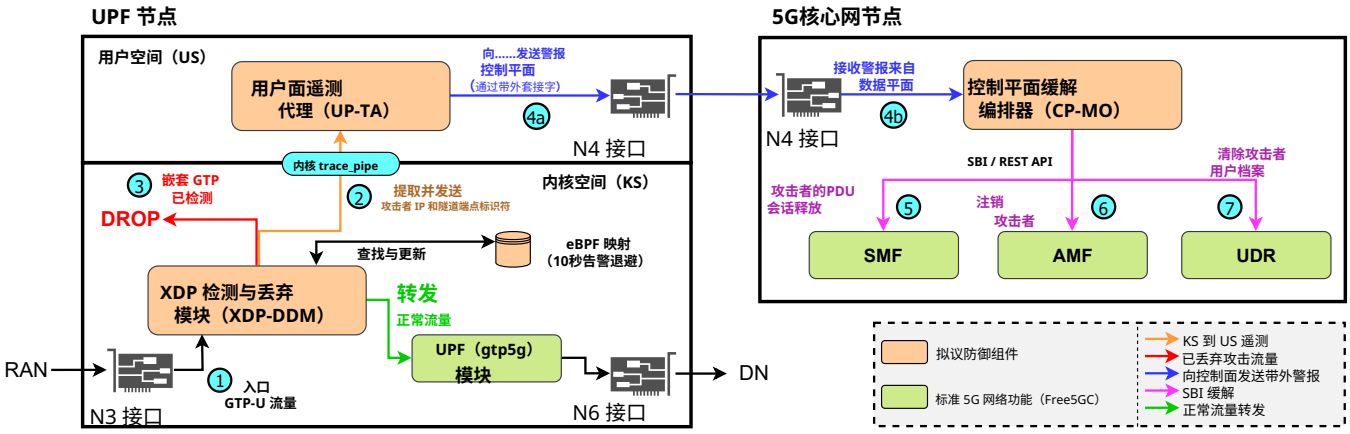


图 2：所提出的闭环 eBPF/XDP 检测与自动化第五代移动通信/5G/6G 控制面缓解防御方案：（1）入口 N3 GTP-U 检查；（2）通过 trace_pipe 异步发送遥测，由 10 秒 eBPF 退避映射控制；（3）以内联线速丢弃数据包（XDP_丢弃）；（4a–4b）向 5G 核心网带外转发警报；以及（5–7）分别跨 SMF、AMF 和 UDR 依次执行 SBI/REST 会话拆除、UE 注销和用户配置文件撤销。绿色模块代表 Free5GC 网络功能（NFs）/组件，而橙色模块展示了我们提出的闭环 eBPF/XDP 检测与自动化缓解组件。

响应会通过受害者的下行隧道发送至受害 UE。该攻击导致受害者的上行和下行隧道充满攻击流量，从而造成配额耗尽、计费欺诈和反射攻击。图 1 展示了嵌套 GTP 攻击的流程。

4. 提出的闭环 eBPF 防御

4.1. 概述与设计原则

为在不影响合法用户流量性能的情况下消除嵌套 GTP-U 攻击的威胁，我们提出了一种闭环检测与缓解防御方案。该方案跨越第五代移动通信数据平面和控制平面边界运行，并利用扩展伯克利包过滤器。

之所以选择扩展伯克利包过滤器作为该防御方案的基础技术，是因为它在现代云原生环境中具备独特能力。扩展伯克利包过滤器作为抽象虚拟机运行，可在 Linux 内核中的安全沙箱内执行用户定义的程序，使开发人员能够扩展内核行为，而无需修改内核源代码或冒系统崩溃的风险 [24]。为满足 5G/6G 数据平面的严格低时延要求，该防御方案具体依赖 XDP。XDP 是一种直接集成到 Linux 内核中的高性能、可编程网络数据路径 [25]。它在网络设备驱动程序上下文中，为自定义数据包处理应用提供了安全的执行环境 [25]。通过将数据处理转移到尽可能早的阶段，即在内核分配内存或启用标准网络协议栈之前，XDP 可实现线速数据包操纵和丢弃 [25],[26]。

借助这些能力，拟议防御机制基于三项核心设计原则构建：1) **轻量级处理：**采用极小的资源占用，确保以线速进行低延迟数据包处理。2) **高可靠性：**确保快速、准确地检测恶意嵌套GTP-U 流量。3) **即插即用集成：**旨在与当前第五代移动通信或未来第六代移动通信网络中的任何基于 Linux 的 UPF 部署完全兼容。

如图 2 和图 3 的调用流程所示，拟议防御机制由三个专用组件构成：XDP 检测与丢弃模块（XDP-DDM）、用户面遥测代理（UP-TA）和控制平面缓解编排器（CP-MO）。

4.2. XDP 检测与丢弃模块（XDP-DDM）

XDP 检测与丢弃模块（XDP-DDM）是一个轻量级的内核空间执行模块，附加在用户面功能的 N3 入口接口上（算法 1）。它在 XDP 挂钩处运行，可在网络协议栈中尽可能早地拦截流量。

为保持最高处理速度，XDP-DDM 将操作限制为纯粹的线速报头解析和丢弃数据包。 ① XDP-DDM 拦截来自无线接入网的到达帧，检查外层 GPRS隧道协议-U 报头并解析封装载荷。合法的用户面数据包会立即返回 XDP_PASS，并转发至 UPF（gtp5g）模块 [27], [28], 以便通过 N6 接口向数据网络（DN）进行标准解封装。 ② 如果检测到目标端口为 2152 的嵌套用户数据报协议（UDP）数据包，XDP-DDM 会查询以攻击者 IP 为索引的 eBPF 映射，以执行 10 秒的警报退避计时器。这可以防止在海量洪泛攻击期间耗尽 CPU 资源。

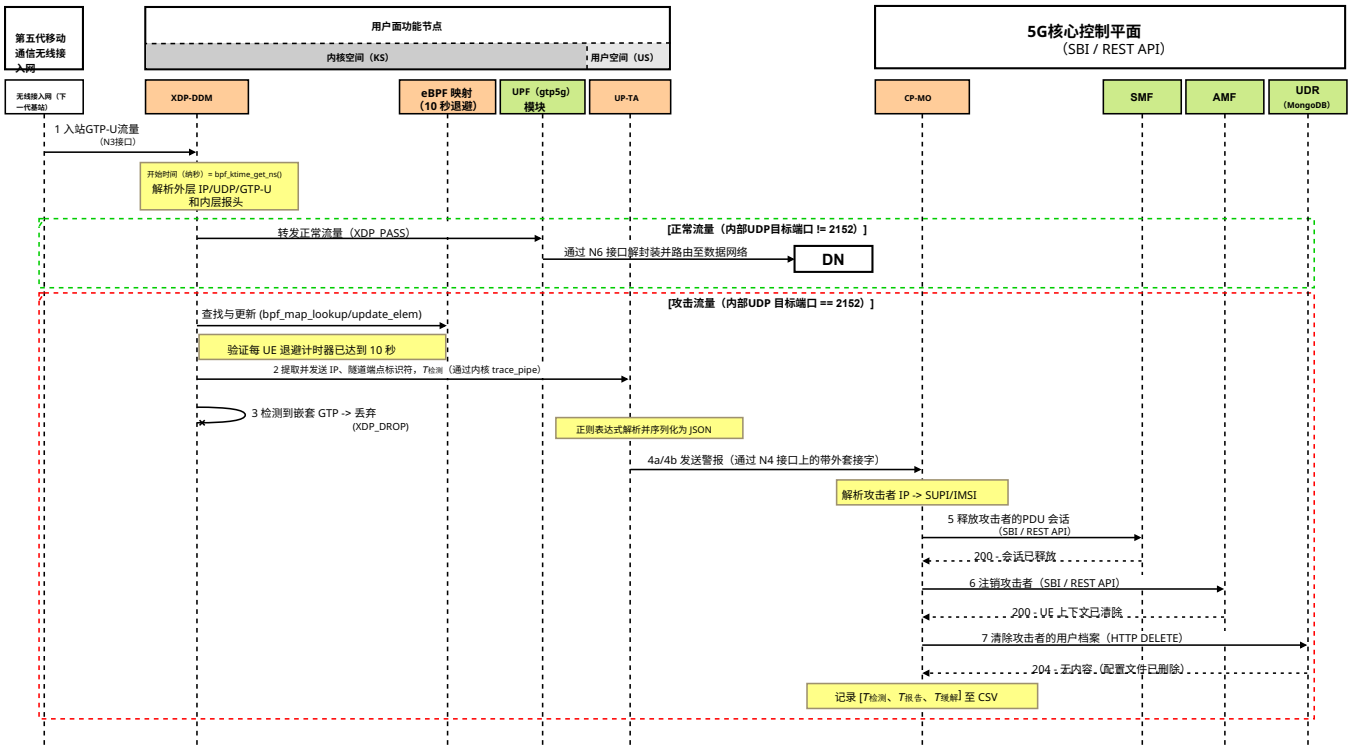


图 3：所提出的闭环 eBPF 防御的调用流程。绿色虚线框显示合法流量的流程，而红色虚线框显示嵌套 GPRS隧道协议攻击流量的处理过程。

该模块不会在内核中执行计算开销巨大的 JSON 序列化，而是异步地通过内核 trace_pipe 将原始遥测数据（攻击者 IP、隧道端点标识符、单调时间戳和 XDP 检测延迟（T_{detect}））发送至用户空间。 ③传输遥测数据后（或检测到攻击流量后），XDP-DDM 会立即返回 XDP_DROP，以线速丢弃恶意帧。

4.3. 用户平面遥测代理（UP-TA）

UP-TA 作为连接数据面线路速率与核心控制平面的中间桥梁（算法2）。它以 UPF 节点上的用户空间守护进程形式部署，并持续轮询 eBPF 跟踪_管道以获取传入的威胁遥测数据。

收到事件后，UP-TA 会计算内核到用户空间的报告延迟，并将原始参数格式化为结构化 JSON告警。这种解耦确保数据面的丢弃效率不受遥测序列化影响。 ④最后，UP-TA 通过在 N4 接口上建立的带外 UDP套接字，将 JSON告警发送至 CP-MO。

4.4. 控制平面缓解编排器（CP-MO）

CP-MO 是闭环防御的最后一个组件，负责永久撤销攻击者的网络访问权限（算法 3）。它位于5G控制平面中，会持续监听来自 UP-TA 的 UDP告警。

为防止协同攻击期间发生套接字阻塞，CP-MO 采用异步多线程执行模式。在将攻击者的 IP 地址解析为特定的永久订阅标识符（SUPI）和会话管理上下文后，它通过基于服务的架构 REST 应用程序接口（API）触发连续的三阶段缓解流程。 ⑤首先，它向 SMF 发出释放命令，以释放攻击者的 PDU 会话并删除 UPF 隧道。 ⑥其次，它命令 AMF 清除信令上下文并注销攻击者 UE。 ⑦最后，它向统一数据存储库（UDR）发起 HTTP DELETE 请求，根据攻击者的永久标识符（SUPI）将其用户档案永久列入黑名单。在闭环缓解结束时，CP-MO 记录 XDP-DDM检测时延（T_{detect}）、报告延迟（T_{report}）和 CP-MO 缓解时延（$T_{mitigate}$）。

4.5. 实现细节与状态机同步

将此防御方案转化为可运行的第五代移动通信原型，需要克服显著的 SBA 状态同步挑战。默认情况下，当 Free5GC [29] 接入和移动性管理功能触发网络发起的注销时，它只会删除本地上下文，却忽略分配给用户设备的活动数据面 PDU 隧道。为防止出现幽灵隧道并确保

算法 1：XDP-DDM：XDP 检测与丢弃模块（UPF 内核空间）输入：入口数据包 p输出：操作（XDP_放行或 XDP_丢弃）共享状态： $\mathcal{M}_{state} \leftarrow$ BPF LRU 哈希映射（去抖跟踪）共享状态：$\tau_{db} \leftarrow 10$ 秒（去抖超时）1 $t_{start} \leftarrow$ 当前纳秒；2 如果 p 缺少有效的外层 IPv4/UDP/GTP 头部，则 3 返回 XDP_放行；// 步骤 1：解析外层头部 4 结束5 $teid \leftarrow p.gtp.teid$；// 提取外层隧道端点标识符 6 将封装载荷提取为 p_{inner}；// 记录正常流量执行时间（评估基线）7 如果 $p_{inner}.protocol ==$ ICMP，则8 $T_{detect} \leftarrow$ 当前纳秒 $- t_{start}$；9 将 T_{detect} 记录到跟踪管道；10 返回 XDP_放行；11 结束 12 如果 $p_{inner}.protocol \neq$UDP，则 13 返回 XDP_放行；// 放行非 UDP 载荷 14 结束 // 步骤 2：检测嵌套 GTP-U 特征 15 如果 $p_{inner}.dest\ \ port == 2152$则16 $t_{end} \leftarrow$ 当前纳秒；17 $T_{detect} \leftarrow t_{end} - t_{start}$；18 $ip_{src} \leftarrow p_{inner}.saddr$；19 $t_{last} \leftarrow \mathcal{M}_{state}[ip_{src}]$；20 如果 t_{last} 为空或（$t_{end} - t_{last}$），则 $> \tau_{db}$；21 $\mathcal{M}_{state}[ip_{src}] \leftarrow t_{end}$；22 将 $\langle ip_{src}$、$teid$、t_{end}、$T_{detect}\rangle$ 导出到用户空间（UP-TA）；23 结束 24 返回 XDP_丢弃；// 步骤 3：丢弃并导出遥测数据 25 结束 26 返回 XDP_放行；// 放行合法的内层 UDP 流量

算法2： UP-TA：用户面遥测代理（UPF 用户空间）

输入： 来自 BPF TracePipe 的事件流

1 **在监听 *BPF TracePipe*时执行**
2 接收到事件时 $e = \langle ip_{src}, teid, t_{end}, T_{detect}\rangle$;
3 $t_{arr} \leftarrow$当前纳秒;
4 $\Delta t_{hop1} \leftarrow t_{arr} - t_{end}$；// 跳数 1：内核到用户空间的延迟
5 $\mathcal{A} \leftarrow$ 构建 JSON告警 $\langle ip_{src}, teid, \Delta t_{hop1}, T_{detect}\rangle$;
6 通过 N4 向 CP-MO转发警报 $\mathcal{A}$；// 步骤 4：分发遥测数据
7 **结束**

根据 3GPP TS 23.502 [30], , 接入和移动性管理功能与会话管理功能的状态机始终保持完全同步。我们的 CP-MO 会严格执行拆除序列。对于与攻击者关联的每个活动 PDU 会话，系统都会显式调用 Nsmf PDUSession ReleaseSMContext 服务 _ _操作，强制会话管理功能在用户设备完全注销并被阻止之前拆除用户面功能隧道。虽然会话释放和注销会调用 3GPP SBI 操作，但用户设备互联网协议到 SUPI 的解析以及 UDR 配置文件移除则通过 Free5GC 的 WebConsole 管理 REST API 执行。

尽管近期的开源社区原型已展示了在 UPF 接口上使用 eBPF/XDP 对未封装流量进行应用层过滤（例如 DNS）的基本可行性， [31]，我们的拟议防御机制利用 eBPF/XDP 构建全面的安全框架。具体而言，我们的工作在设计和范围上有根本差异：解析递归 GTP-in-GTP 封装、实现内核空间去抖，并通过自动控制平面撤销形成闭环。

5. 评估方法

本节概述了用于评估所提出的闭环 eBPF 防御的有效性、韧性和性能影响的实验方法。

5.1. 测试床环境

为严格评估所提出的闭环 eBPF 防御，我们使用了第五代移动通信网络切片测试平台，如图4所示。5G 核心网通过 Free5GC [29]部署在专用虚拟机中，以提供所需的网络功能；无线接入网和用户设备则使用 UERANSIM [32] 进行仿真。我们使用两台不同的虚拟机，分别承载切片1（增强型移动宽带（eMBB））和切片 2（超可靠低时延通信（URLLC））的仿真用户设备和下一代基站实例。每个切片都由相应的数据网络提供服务：DN_{eMBB}和 DN_{URLLC}。5G 数据面 UPF 使用 Containerlab [33]部署并编排在 VirtualBox 虚拟机 [34] 中，以便灵活地自定义数据路径。该容器化拓扑为部署 XDP 挂钩和执行高保真流量生成提供了高度可复现的环境。

为准确建模现实的核心网，我们假设采用由中间 UPF（$I-UPF$）、中央 UPF（$C-UPF$）和 PDU 会话锚点 UPF（$P-UPF$）组成的多层 UPF 拓扑。 $I-UPF$充当边缘分支节点，将时延敏感的 URLLC 流量直接路由至边缘数据网络，同时将增强型移动宽带流量转发至核心网更深处。 $C-UPF$纯粹充当中转节点，以模拟多跳核心网中转，并不连接任何数据网络。

算法 3： CP-MO：控制平面缓解编排器（控制平面）

输入： 警报 $\mathcal{A} = \langle ip_{src}, teid, \Delta t_{hop1}, T_{detect} \rangle$ 来自 UP-TA

当在 *UDP* 端口上监听 **时**
  接收警报 $\mathcal{A}$;
  $t_{n4_arr} \leftarrow$ 当前纳秒;
  解析 JSON 载荷 $\mathcal{A}$;
  // 计算 N3 到 N4 总时延报告时间
  $T_{report} \leftarrow \mathcal{A}.\Delta t_{hop1} +$（当前纳秒 $- t_{n4_arr}$）;
  // 异步执行以维持非阻塞套接字
  生成后台线程 缓解($\mathcal{A}.ip_{src}$, $\mathcal{A}.teid$, $\mathcal{A}.T_{detect}$, T_{report});
结束
过程 缓解($ip_{src}, teid, T_{detect}, T_{report}$)
  $t_{mit_start} \leftarrow$ 当前纳秒;
  $\mathcal{L}_{ue} \leftarrow$ HTTP GET 接入和移动性管理功能 已注册用户设备;
  $supi, sm_ctx, plmn \leftarrow$ NULL, NULL, NULL;
  遍历 $ue \in \mathcal{L}_{ue}$ **do**
    如果 ue 包含 ip_{src} **则**
      $supi \leftarrow ue.SUPI$;
      $sm_ctx \leftarrow ue.SmContextRef$;
      $plmn \leftarrow ue.PLMN$;
      跳出; // 解析攻击者 SUPI 和 SM上下文
    end
  end
  如果 $supi \neq NULL$ 且 $sm_ctx \neq NULL$ **则**
    // 步骤 5：触发 UPF 会话拆除
    HTTP POST 会话管理功能(sm_ctx, 释放);
    // 步骤 6：触发注销
    HTTP POST 接入和移动性管理功能($supi$, release);
    // 步骤 7：将用户设备列入黑名单
    HTTP DELETE 统一数据存储库($supi$, $plmn$);
  end
  $T_{mitigate} \leftarrow$ 当前纳秒 $- t_{mit_start}$;
  追加 $\langle ip_{src}, teid, T_{detect}, T_{report}, T_{mitigate} \rangle$ 至评估日志;

最后，$P-UPF$终止与云数据网络的连接。因此，URLLC 的 PDU数据路径建模为（$gNB \rightarrow I-UPF \rightarrow DN_{URLLC}$），而增强型移动宽带切片的路径建模为（$gNB \rightarrow I-UPF \rightarrow C-UPF \rightarrow P-UPF \rightarrow DN_{eMBB}$）。

5.2. 大流量攻击下的韧性

为评估我们的防御机制在主动攻击下的韧性，我们编排了一次跨切片的嵌套 GTP volumetric

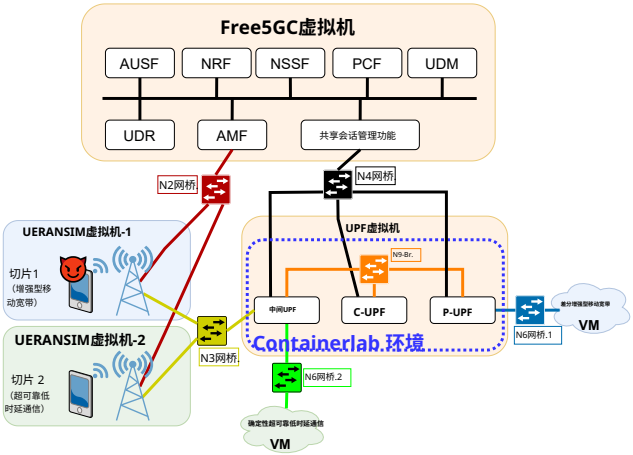


图4：实验用 5G 网络切片测试平台架构。控制平面依托 Free5GC，增强型移动宽带（切片1）和超可靠低时延通信（切片 2）切片的无线接入网和 UE 则通过 UERANSIM 在专用虚拟机上进行仿真。数据平面由 Containerlab 编排，采用多层用户面功能拓扑，并通过专用网桥（N2、N3、N4、N6 和 N9）互连，以隔离流量并验证跨切片攻击场景下的 eBPF防御。

洪泛攻击。攻击者 UE 配置在切片1中，而受害 UE 运行于切片 2 中。为规避 UERANSIM 软件在高流量生成场景下崩溃这一固有限制 [35], 我们使用 TRex 流量生成器 [36]。我们将精心构造的嵌套 GTP 负载捕获到 PCAP 文件中，并由 TRex 以 10,000 包/秒的持续速率进行高强度重放。

在整个攻击时段内，我们持续测量受害 UE 的往返时间（RTT）延迟和传输控制协议吞吐量。同时，通过受害 UE 的 UERANSIM 隧道捕获穿透性攻击流量，并记录到 PCAP 文件中。该方法能够直接比较基线环境（未部署所提出的 eBPF/XDP 防御）与缓解环境的网络韧性。

5.3. 对合法流量的性能影响

运营商级第五代移动通信部署要求安全机制不得降低良性用户的服务质量。为量化系统开销，我们测量了所提出的 eBPF/XDP 程序对合法用户流量的影响。

评估重点关注两项主要性能指标：**端到端 RTT 时延**和**TCP 吞吐量**。我们在无攻击环境下，使用标准 ICMP 和 TCP 流，对穿越超可靠低时延通信和增强型移动宽带切片的流量进行基准测试。通过记录这些指标，我们建立基线，并将其与用户在用户面功能启用扩展伯克利包过滤器/XDP 程序时的端到端时延和吞吐量直接进行比较。

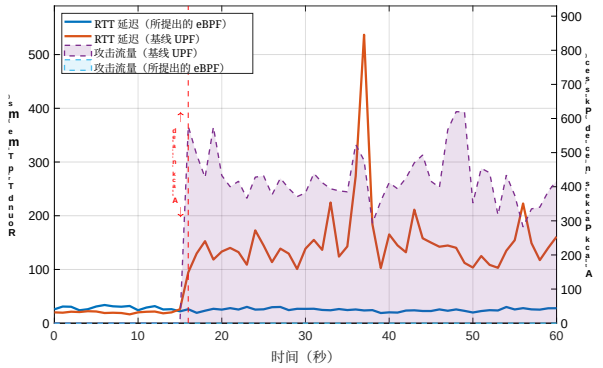


图 5：对切片 2 中受害 UE 往返时间（RTT）韧性的双轴评估。在嵌套 GTP-U 洪泛攻击期间，基线 UPF 受到严重影响并出现延迟尖峰（>500 毫秒）；而所提出的 eBPF 防御成功保护了受害者，使其保持稳定的基线延迟。

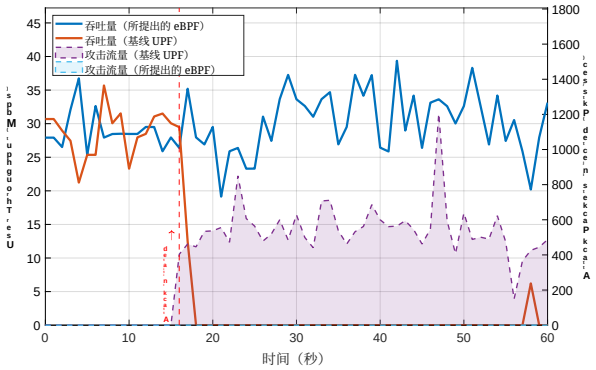


图 6：对切片 2 中受害 UE 的 TCP 吞吐量韧性进行双轴评估。攻击流量淹没队列，导致基线 UPF 资源完全耗尽（0 兆比特每秒）。相比之下，所提出的 eBPF防御完美隔离了各个切片，悄然丢弃攻击流量，并为受害者保留了最佳的 $25-40$ 兆比特每秒吞吐量。

5.4. 闭环防御的延迟 e

为精确量化闭环管线的响应能力，我们将系统总时延分解为与架构组件对应的三个不同指标：

- **检测延迟 (T_{detect})：** XDP-DDM 将入口数据包识别为正常流量或恶意流量所需的执行时间。测量时间从扩展伯克利包过滤器/XDP 程序接收数据包时开始，到转发或丢弃决策最终确定时结束。对于攻击流量，该计时机制已原生集成到特征检测逻辑中。为建立正常流量的基线，评估期间专门对扩展伯克利包过滤器程序进行了插桩，以测量正常 ICMP 数据包的执行时间。
- **报告延迟 (T_{report})：** 向 5G 核心网发送威胁警报所经过的时间。该时间由内核到用户态传输延迟（从 XDP-DDM 检测到 UP-TA 通过 trace_pipe 接收）与 CP-MO 的 JSON 载荷解析时间相加得出，详见算法 2 和算法 3。如局限性（第 7 节）所述，该测量明确排除了由虚拟机监控程序固有的时钟偏差引入的虚拟交换机延迟。
- **缓解延迟（$T_{mitigate}$）：** CP-MO 成功协调缓解所需的时长。该指标涵盖控制平面缓解过程（执行_缓解）的运行时间。

6. 实验结果

6.1. 大流量攻击下的韧性

图 5 和图 6 展示了部署在 URLLC切片2 中的受害者用户设备，在应对来自切片1攻击者发起的嵌套 GTP-U 容量型洪泛攻击时的韧性。两图均采用双轴表示，将 RTT 和吞吐量等主要用户性能指标与穿透受害者隧道的注入攻击数据包数量进行对照。

攻击前基线稳定性：在初始攻击前时段（0 到 15 秒）内，两种场景下的 RTT 延迟和 TCP 吞吐量都高度相近。基线 UPF 与所提出的扩展伯克利包过滤器解决方案表现几乎完全一致，说明在正常运行条件下，eBPF钩子对合法用户流量造成的开销极小。

基线 ***UPF*** 受到严重影响：在 $t = 16$秒时，嵌套 GTP 流量型攻击开始（如粉色阴影区域所示）。在基线 UPF 场景中（未采用所提出的扩展伯克利包过滤器解决方案），注入的嵌套 GTP 攻击流量立即压垮了核心网。受害者的 RTT 大幅增加，在整个攻击期间始终高于 100 毫秒，最坏情况下峰值超过500毫秒，如图 5 所示。另一方面，攻击期间受害者的吞吐量完全降至零，如图 6 所示，导致服务质量和体验质量（QoE）严重下降。

尽管攻击者在源端以 10,000 包/秒的速率注入流量，但穿过受害者隧道的攻击流量仅为 500 至 1,200 包/秒。这一差异凸显了拒绝服务（DoS）攻击的核心机制：Linux 内核的标准 gtp5g 模块已完全饱和。当队列达到

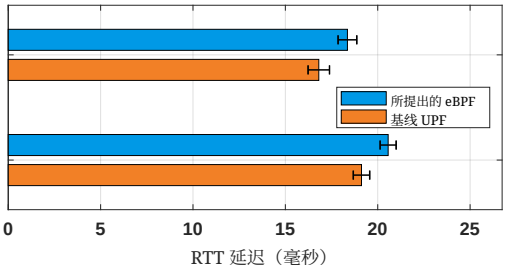


图 7：在 100 个样本（95% 置信区间）中，拟议的扩展伯克利包过滤器防御机制对增强型移动宽带和超可靠低时延通信切片间合法流量端到端 RTT 延迟的影响；与基线 UPF 相比，时延开销极小（< 2 毫秒）。

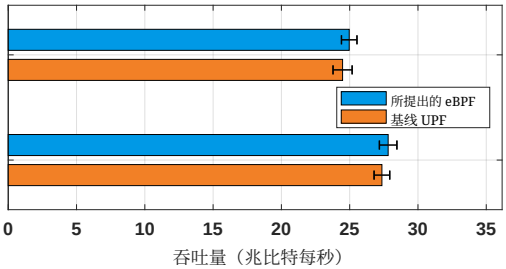


图 8：在 100 个样本中，拟议的扩展伯克利包过滤器防御机制对增强型移动宽带和超可靠低时延通信切片中合法传输控制协议吞吐量的影响；与基线用户面功能相比，重叠的 95% 置信区间表明其开销在统计上并不显著。

最大容量时，操作系统会不加区分地丢弃大多数入站数据包，实际上使受害者的合法流量陷入饥饿。在 $t = 58$ 秒时观察到的短暂 6 兆比特每秒吞吐量异常，是 TCP 饥饿的典型表现：在拥塞队列发生微小波动期间，网络窗口探测会暂时成功。

拟议防御机制的韧性：与此形成鲜明对比的是，启用所提出的扩展伯克利包过滤器防御后，用户的 RTT 延迟和传输控制协议吞吐量始终与攻击前水平完全一致，如图 5 和图 6 所示。受害者隧道中记录的攻击流量始终为零，表明恶意嵌套 GTP 流量在网络驱动程序层被 XDP-DDM 立即拦截并丢弃。在线速 XDP-DDM 吸收攻击冲击的同时，CP-MO 会异步撤销攻击者的连接，并将攻击者 UE 列入黑名单，以防止其后续接入（具体数据见第 6.3 节）。

要点：所提出的扩展伯克利包过滤器防御成功在数据平面实施了严格的跨切片隔离。标准 UPF 在嵌套 GTP 洪泛攻击导致队列饱和时，连接性能会严重恶化；而我们的线速 XDP-DDM 确保受害者的合法流量仅产生极小开销，从而维持最佳服务质量。

6.2. 对合法流量的性能影响

运营商级安全解决方案必须透明运行，且不能对良性用户造成影响。为量化拟议防御机制在正常、无攻击条件下产生的运行开销，我们评估了其对增强型移动宽带和超可靠低时延通信网络切片中合法用户设备流量的影响。

6.2.1. 对端到端时延（RTT）的影响。 图 7 展示了穿越增强型移动宽带和超可靠低时延通信切片的合法 ICMP 流量的端到端 RTT 时延，并对比了基线 UPF 与运行所提出的扩展伯克利包过滤器解决方案的 UPF。为确保统计严谨性，每个柱状条表示基于 100 个干净数据包样本计算得出的平均 RTT，并附带其 95% 置信区间。

在基线配置中，增强型移动宽带切片的平均 RTT 为 16.8 ms，而超可靠低时延通信切片的平均值为19.1 ms。尽管增强型移动宽带拓扑经过三个用户面功能跳数，而超可靠低时延通信切片仅经过一个用户面功能跳数，但超可靠低时延通信切片的基线 RTT 略高。这种现象是容器化 5G 仿真以及 UERANSIM 对用户空间 UDP 套接字上物理层 5G 新空口（New Radio）进行抽象所产生的预期结果。由于共享主机内核中虚拟以太网（veth）对之间的容器间转发仅需微秒级时间，增强型移动宽带路径中额外的用户面功能跳数所引入的延迟，与独立的下一代基站和用户设备进程之间正常的跨核线程调度方差相比可以忽略不计。

当所提出的 eBPF 防御在 N3 接口上启用时，两个切片的平均 RTT 均仅小幅增加 1 至2 ms，eMBB 切片达到约18.3ms，URLLC 切片达到20.5 ms。鉴于内核中的 XDP-DDM 检查每个数据包所需时间少于 $0.4\ \mu$s（如图 9 所示），这一1–2ms 的差异反映的是测试运行之间正常的虚拟化网络方差、轻微的用户空间上下文切换，以及评估过程中的 ICMP 遥测日志记录（算法 1），而非数据平面排队时延。更为关键的是，紧密的95% 置信区间证实，XDP 挂钩不会引入延迟尖峰或抖动，从而保持时延敏感切片的确定性性能。

6.2.2. 对用户吞吐量的影响。 图 8 展示了 eMBB 和 URLLC 网络切片中合法用户设备流量的端到端 TCP 吞吐量，并对比了基线 UPF 与所提出的 eBPF 防御。与延迟评估一致，每个柱状条表示基于 100 个无攻击样本计算的平均吞吐量，并附有其95% 置信区间。

在两个网络切片中，集成所提出的 eBPF 程序都保留了基线带宽性能。具体而言，在增强型移动宽带切片中，基线

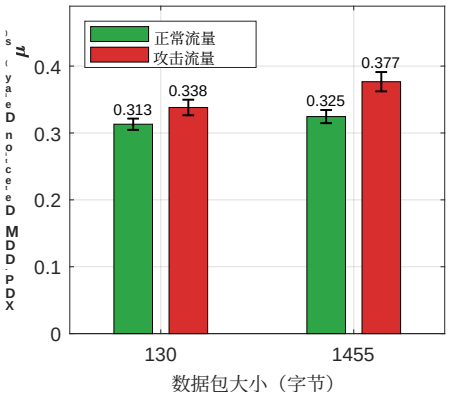


图 9：在标准数据包大小和最大传输单元（MTU）数据包大小下，正常流量与攻击流量的 XDP-DDM 检测时延（T_{detect}），取 100 个样本的平均值（95% 置信区间）。算法 1 详细说明了该指标的具体计算方法。

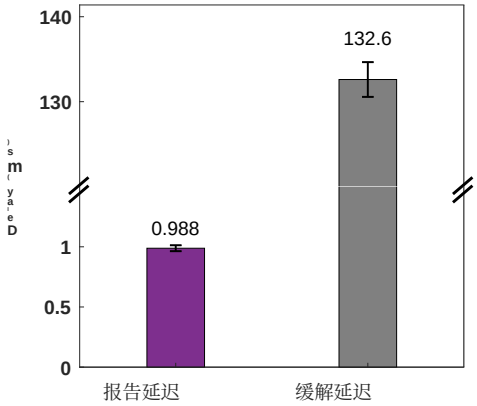


图10：UP-TA 遥测报告时延（T_{report}）以紫色显示，CP-MO 缓解编排时延（$T_{mitigate}$）以灰色显示，数据为 100 个样本的平均值（ 95% 置信区间）。算法 2 和算法 3详细说明了这些指标的具体计算方法。

UPF 和所提出的 eBPF 配置均实现了约 24.5 至25 兆比特每秒的平均吞吐量。同样，在超可靠低时延通信切片中，在两种场景下吞吐量均稳定在约 27.5 至28 兆比特每秒。值得注意的是，与空闲状态下的 ICMP 往返时间测量结果相比，超可靠低时延通信切片的吞吐量高于增强型移动宽带切片。在持续的大流量传输协议传输过程中，数据平面处于主动饱和状态，这意味着增强型移动宽带拓扑中三个 UPF 跳数所产生的累积 GTP-U 封装和虚拟接口转发开销，与单用户面功能超可靠低时延通信路径相比，会使最大吞吐量略有下降。

关键的是，在各自切片内比较基线 UPF 与所提出的 eBPF 防御时，95%置信区间大幅重叠。这种统计重叠表明，平均吞吐量的微小差异在统计上并不显著，反映的是测试床的自然波动，而非 eBPF 处理开销。由于 XDP-DDM 在数据包到达 UPF 转发逻辑之前，直接在内核中执行轻量级的零拷贝报头检查，因此不会对活跃的 TCP 流造成明显瓶颈。

总之，对端到端时延和持续带宽的评估证实，所提出的 eBPF 安全机制能够在数据平面中透明运行，在保护 UPF 的同时，不会降低良性切片流量的性能。

关键要点：所提出的闭环 eBPF 防御对合法用户流量几乎没有性能影响。通过直接在网络驱动程序层执行数据包检查，XDP-DDM 在不同类型的网络切片中保持了基线端到端延迟和吞吐量，同时不损害服务质量。

6.3. 闭环防御时延

任何安全机制都会带来性能开销，在我们的解决方案中，这一开销以处理延迟来衡量。为了评估所提出的 eBPF/XDP 防御的处理效率，我们首先分析各运行阶段的延迟：检测（T_{detect}）、报告（T_{report}）和缓解（$T_{mitigate}$）。我们使用两种数据包大小来评估检测延迟：较小的 130 字节数据包，以及较大的 1455 字节数据包，后者代表最大传输单元载荷。

XDP-DDM检测时延：如图 9 所示，XDP-DDM 的检测延迟极低，在所有测试场景中始终低于 $0.4\ \mu$s。对于 130 字节的数据包，正常流量的平均检测时间为 $0.313\ \mu$s，而攻击流量所需时间略长，为 $0.338\ \mu$s。对于 1455 字节的数据包，也存在类似的细微差距：正常流量和攻击流量分别为 $0.325\ \mu$s 和 $0.377\ \mu$s。

攻击流量的延迟略有增加，这是由算法的执行路径直接导致的。对于良性流量，XDP程序读取协议报头后便会提前终止。另一方面，当检测到嵌套GTP-U攻击流量时，算法会执行额外操作：解析内部UDP报头、匹配目的端口特征，并提取内部源IP地址，然后进行 BPF LRU映射查找并丢弃数据包。

关键的是，尽管数据包总大小增加了十倍（从 130 字节增至 1455 字节），检测延迟仅增加了12 至 40 纳秒。这证明，eBPF/XDP 程序能够正确解析报头，而无需缓冲或将整个载荷复制到内存中，因此无论载荷大小如何，执行速度都能保持近乎恒定。总体而言，各项检测延迟结果高度相近，数值差异不到100 纳秒。

报告与缓解延迟：图10展示了报告和 CP-MO 缓解延迟，使用断轴刻度呈现，

以突出报告延迟与核心编排延迟之间的差异。

UP-TA 报告延迟（T_{report}）平均仅为 0.988毫秒。这1毫秒的开销代表了将单调事件通过内核跟踪_管道传输到用户空间（UP-TA），并在 CP-MO 处解析生成的 JSON 警报所需的时间。这表明遥测分发的开销极低，即使在高频生成警报的情况下，也不会成为 UPF 节点 CPU 的瓶颈。

相比之下，CP-MO 缓解延迟（$T_{mitigate}$）是闭环防御中最耗时的阶段，平均为 132.6 毫秒。这代表了在 5G 核心网中执行复杂 HTTP REST API 所产生的固有网络与处理开销，包括调用 SMF 进行会话释放、调用接入和移动性管理功能进行 UE 注销，以及调用统一数据存储库清除攻击者配置文件。

总而言之，尽管闭环延迟主要由 132.6 毫秒的缓解阶段所主导，但这一延迟不会使受害 UE 暴露于嵌套 GTP 攻击之下。由于 XDP-DDM 已在 0.4 μ秒内于 DP 中隔离并丢弃恶意数据包，受害者会立即受到保护。此外，由于 CP-MO 在独立的后台线程中执行 REST API 拆除，因此绝不会阻塞接收来自 UP-TA 的新 UDP 告警。该系统完全异步；XDP-DDM 会立即吸收嵌套 GTP 攻击，而 CP-MO 则在后台永久撤销攻击者的网络访问权限。

要点：拟议防御机制可在数据平面实现亚微秒级（< 0.4 μs）威胁隔离，立即保护受害 UE 免受嵌套 GTP 攻击。通过异步卸载控制面拆除流程，系统可永久撤销攻击者的访问权限，同时不会给 UPF 数据路径带来阻塞开销或瓶颈。

7. 局限性

尽管实验结果证明，拟议的闭环扩展伯克利包过滤器防御机制具有亚微秒级的效能和韧性，但本研究在实现和环境方面仍存在以下局限性：

虚拟机监控器时钟偏差对报告测量的影响：如第5.4节所述，报告延迟（T_{report}）的测量未包含虚拟交换机的中间传输延迟。由于 UP-TA 和 CP-MO 在彼此隔离的虚拟化边界上运行，虚拟机监控器固有的时钟偏差会导致独立系统时钟之间出现亚毫秒级漂移。因此，若不使用硬件时间戳，就无法可靠地分离虚拟交换机上的单向网络传输延迟；为确保测量准确性，本研究未将其纳入测量。

测试平台虚拟化与可扩展性上限：我们的实验测试平台将第五代移动通信和无线接入网组件部署在通过半虚拟化（virtio-net）网络接口互连的 VirtualBox 虚拟机中。由于 UERANSIM 在用户空间通过标准 UDP 套接字模拟 5G NR协议栈，且数据包转发需经过宿主机虚拟机监控器的虚拟交换机，基线用户吞吐量被限制在约 $25–35$ 兆比特每秒，而 virtio-net 上的 XDP执行仍受虚拟机监控器上下文切换开销的影响。因此，我们的评估重点在于单个攻击者发起的 10,000 包/秒洪泛下的功能有效性和跨切片保护，而非使 XDP-DDM 达到其线速上限。广泛的裸机压力测试（包括 UPF 和控制面CPU利用率分析、协调多UE洪泛，以及与其他过滤方法进行对比基准测试）仍是未来一项重要工作。

加密的 ***N3*** 接口（***IPsec***）：由于 XDP 程序在网络驱动程序级别执行，早于 Linux 内核分配内存和 IPsec 解密协议栈，因此 XDP-DDM 需要能够查看明文 GTP-U 头部。我们的防御假设：如果部署了 N3 IPsec 隧道，则这些隧道会在流量到达 UPF N3 入接口之前由外部安全网关终止，或者通过智能网卡的内联 IPsec 卸载在硬件中解密。

内层 ***IP*** 欺骗与外层 ***TEID*** 关联：虽然 XDP-DDM 会在遥测载荷中提取并报告外层 GTP-U TEID 和内层 IPv4 源地址，但当前防御方案仅使用内层源 IP 地址对 10 秒 eBPF 去抖映射进行索引，并执行 CP-MO 会话查找和撤销。此设计假设在 UPF N3 接口之前（例如在下一代基站处）已实施入口源 IP 验证。如果攻击者能够发送内层源 IP 地址遭到欺骗的嵌套 GTP-U 数据包，则会产生三种次生风险：①随机化的内层 IP 地址可绕过按 IP 划分的去抖映射，并使遥测通道遭受洪泛攻击；②无法识别的欺骗 IP 地址可逃避 CP-MO 会话查找；③ 冒用另一名活跃用户的 IP 地址可能会导致无辜受害 UE 的会话被错误撤销。由于外层 GTP-U TEID 由可信的服务下一代基站分配，UE 无法伪造（除非攻击者控制了该下一代基站），因此，若 eBPF 去抖映射和 CP-MO 用户解析均严格基于外层 GTP-U TEID，就能消除这三种风险，且无需改变闭环架构。

检测特征与解析范围：我们提出的 XDP-DDM 通过匹配发往 GTP-U 端口 2152 的内部 UDP 流量，来识别嵌套 GTP-U 数据包。如果良性 UE 与外部服务器通过端口 2152 通信，此检查可能触发误报。在商用部署中，可通过验证内层目的 IP 地址是否指向运营商核心/内部网络而非数据网络，并验证内层 GTP-U 头字段来消除误报。在本研究的范围内，我们假设良性 UE 不会产生发往端口 2152 的非 GTP UDP 流量。此外，当前解决方案针对未标记、未分片的 IPv4 流量；IPv6、802.1Q VLAN 标签和 IP 分片则可通过标准 XDP 解析器扩展予以支持。

8. 伦理考量

本研究中的所有实验评估和数据平面攻击均在本地私有托管的 5G测试平台上进行。为确保完全隔离，并保证没有恶意流量能够逃出受控环境，承载 5G测试平台的虚拟机（VM）与公共互联网完全隔离。此外，本研究未引入任何新型攻击向量或零日漏洞利用。所实施的攻击，具体而言是嵌套 GTP（GTP-in-GTP）攻击，利用的是此前已发表且经学术界认可的漏洞。我们仅在隔离环境中复现这些已知漏洞利用，以通过实证验证所提框架的防御效果。

9. 结论

本文提出了一种闭环 eBPF/XDP 安全防御，旨在缓解近期发现的、针对第五代移动通信及未来第六代移动通信核心网的嵌套GTP-U协议隧道攻击。实证评估表明，该系统能在 $0.4\ \mu$秒内消除跨切片攻击，同时完全保障受害切片的性能。本研究的发现对第五代移动通信-Advanced及未来第六代移动通信数据平面的设计和运行具有多项实际意义。首先，我们的结果表明，直接在UPF入口部署轻量级、带防抖机制的eBPF/XDP过滤器，可有效主动防御跨切片GTP-U攻击，使运营商能够安全地在异构切片间共享底层UPF资源。其次，由于XDP-DDM在网络驱动程序内处理帧，因此该防御不受具体UPF软件实现的影响。随着标准化组织在保留5G服务化架构和GTP-U基础的同时迈向第六代移动通信，这种即插即用的防御为网络运营商提供了一条实用途径，无需修改VNF源代码即可强化现有及未来基于 Linux 的 UPF。

致谢

本研究得到加拿大自然科学与工程研究委员会（NSERC）的支持。本研究部分得益于卡尔顿大学研究计算服务（https://carleton.ca/rcs）提供的支持。

生成式人工智能使用注意事项

我们作者对本文所有内容的原创性和正确性承担全部责任，包括研究贡献、拟议防御机制、评估方法、实验结果和结论。本文稿在编辑过程中使用了生成式人工智能，作者对所有输出均进行了检查，以确保其准确性和原创性。

参考文献

[1] 3GPP，《6G系统架构研究；第2阶段》，技术报告（TR），3GPP TR 23.801-1，版本0.8.0，第20版，第三代合作伙伴计划，2026年。[2] 3GPP，《通用分组无线业务（GPRS）隧道协议用户面（GTPv1-U）》，技术规范（TS），3GPP TS 29.281，版本19.2.0，第19版，第三代合作伙伴计划，2025年。[3] A. Shaik、R. Jaschek 和 J.-P. Seifert，《揭示5G中的隐藏路径：利用协议隧道和网络边界桥接》，载于*2025*年*ACM SIGSAC*计算机与通信安全会议论文集，第231–245页，2025年。[4] A. Shaik 和 R. Jaschek，《The 5G Titanic》，载于*Black HatUSA*，2025年。[5] Y. Zhang、T. Wan、Y. Yang、H. Duan、Y. Wang、J. Chen、Z. Wei 和 X. Li，《入侵围墙花园：评估蜂窝网络中的GPRS隧道协议安全性》，载于*2025*年*IEEE*安全与隐私研讨会（*SP*），第1159–1177页，IEEE，2025年。[6] A. AbdulGhaffar 和 A. Matrawy，《切片隔离即服务：主动防御5G-Advanced及超5G网络中跨切片攻击的隔离机制》。arXiv预印本 arXiv:2611.23826，2026年。DOI: https://doi.org/10.48550/arXiv.2611.23826。[7] S. I. Salim，《深入剖析数据包反射漏洞：该漏洞可让攻击者侵扰专用5G网络——趋势科技（美国）》。趋势科技研究部门深度研究，2023年。[在线]。可访问：https://www.trendaisecurity.com/en-us/resources-insights/deep-research/plague-private-5g-networks。访问日期：2026-10-15。[8] MITRE，《MITRE FiGHT（5G威胁层级）框架：协议隧道：通过GTP-U进行UE接入（FGT1572）》，2025年。 [在线]。可访问：https://fight.mitre.org/techniques/FGT1572.501/。[9] S. Kwon、S. Park、D. Kim、D. Kim、S. Kim 和 T. Shon，《使用UE的移动核心网攻击技术》，*IEEE Access*，2026年。[10] S. I. Salim，《来自用户设备的5G基础设施攻击》。趋势科技研究部门，2023年。[11] D. Sattar、A. Matrawy 和 A. AbdulGhaffar，《用于DDoS缓解的安全5G核心网切片》，*IEEE*系统期刊，第19卷，第3期，第754–765页，2025年。[12] M. Mahyoub、A. AbdulGhaffar、E. Alalade 和 A. Matrawy，《面向安全的5G切片网络功能共享模型》，*Security and Privacy*，第8卷，第3期，文章编号e70039，2025年。[13] M. Bolourian、N. Limam、M. A. Salahuddin 和 R. Boutaba，《5Guard：面向隔离的5G网络端到端切片》，*IEEE*移动计算汇刊，2025年。[14] M. S. Khan、B. Farzaneh、N. Shahriar、N. Saha 和 R. Boutaba，《SliceSecure：DoS/DDoS攻击对5G网络切片的影响与检测》，载于*2022*年*IEEE*未来网络世界论坛（*FNWF*），第639–642页，2022年。[15] F. Parola 和 F. Risso，《基于扩展伯克利包过滤器的5G移动网关概念验证》，*SIGCOMM'20*海报与演示论文集，2020年。[16] F. Messaoudi、L. Wang、A. Mekrache、A. Ksentini、B. Li、J. Su、S. Messaoudi 和 S. El Ghalbzouri，《5G数据平面中的风暴酝酿：基于eBPF/XDP的高性能用户面功能的设计与评估》，*IEEE*网络与服务管理汇刊，2026年。[17] A. T.-J. Akem 和 M. Fiore，《面向P4可编程5G用户面功能的实时入侵检测》，载于*2024*年*IEEE*第*32*届网络协议国际会议（*ICNP*），第1–6页，IEEE，2024年。[18] M. Repetto、G. Bruno、J. Yusupov、G. Lamanna、B. Ertl 和 A. Carrega，《自动缓解NFV服务中的放大攻击》，*IEEE*网络与服务管理汇刊，第19卷，第3期，第2382–2396页，2022年。

[19] L. Loureiro、V. Pereira、T. Cruz 和 P. Sim˜oes，《使用eBPF/XDP增强5G核心安全》，载于NOMS 2024-2024 IEEE网络运营与管理研讨会，第1–6页，IEEE，2024年。[20] A. Javadpour、F. Ja'fari、T. Taleb 和 C. Benza¨ıd，《基于强化学习的切片隔离，抵御超5G网络中的DDoS攻击》，IEEE网络与服务管理汇刊，第20卷，第3期，第3930–3946页，2023年。[21] N. Yarkina、A. Gaydamaka、D. Moltchanov 和 Y. Koucheryavy，《符合ITU-T标准的5G无线接入网网络切片机器学习增强性能评估》，IEEE移动计算汇刊，第23卷，第1期，第719–736页，2022年。[22] A. AbdulGhaffar、M. Mahyoub 和 A. Matrawy，《不同VNF共享配置下泛洪攻击对5G切片的影响》，载于2024年第20届可靠通信网络设计国际会议（DRCN），第136–142页，IEEE，2024年。[23] M. Mahyoub、A. AbdulGhaffar、E. Alalade、E. Ndubisi 和 A. Ma- trawy，《关键5G接口的安全分析》，IEEE通信调查与教程，第26卷，第4期，第2382–2410页，2024年。[24] Y. He、R. Guo、Y. Xing、X. Che、K. Sun、Z. Liu、K. Xu 和 Q. Li，《跨容器攻击：云环境中令人困惑的eBPF》，载于第32届USENIX安全研讨会（USENIX Security 23 5988, 2023 5971），第–页。[25] T. Høiland-Jørgensen、J. D. Brouer、D. Borkmann、J. Fastabend、T. Herbert、D. Ahern 和 D. Miller，《快速数据路径：操作系统内核中的快速可编程数据包处理》，载于第14届新兴网络实验与技术国际会议论文集，第54–66页，2018年。[26] D. Soldani、P. Nahi、H. Bour、S. Jafarizadeh、M. F. Soliman、L. Di Gio- vanna、F. Monaco、G. Ognibene 和 F. Risso，《eBPF：面向当前（5G）及未来移动网络（6G及超6G）的云原生可观测性、网络与安全新方法》，IEEE Access，第11卷，第57174–57202页，2023年。[27] Free5GC，《GitHub - free5gc/go-upf》。 [在线]。可访问：https://github.com/free5gc/go-upf。访问日期：2026-07-10。[28] Free5GC，《GitHub - free5gc/gtp5g：GTP-U Linux内核模块》。 [在线]。可访问：https://github.com/free5gc/gtp5g。访问日期：2026-07-10。[29] Linux基金会，《free5GC》。 [在线]。可访问：https://free5gc. org/。访问日期：2026-07-10。[30] 3GPP，《5G系统（5GS）流程》，技术规范（TS），3GPP TS 23.502，版本19.9.0，第19版，第三代合作伙伴计划，2026年。[31] H.-X. Huang（c1ydehhx），《面向Free5GC的高效且与硬件无关的深度包检测》。Free5GC博客与源代码仓库，2026年。[在线]。可访问：https://free5gc.org/blog/ 20260225/20260225/ 和https://github.com/c1ydehhx/dpi5g。访问日期：2026-10-15。[32] UERANSIM，《GitHub - aligungr/UERANSIM：开源5G用户设备和无线接入网（gNodeB）实现》。 [在线]。可访问：https://github.com/aligungr/UERANSIM/。访问日期：2026-08-10。[33] 诺基亚，《containerlab》。 [在线]。可访问：https://containerlab.dev/。访问日期：2026-07-10。[34] 甲骨文，《Oracle VirtualBox》。[在线]。可访问：https://www.virtualbox.org/。访问日期：2026-07-10。[35] Adamali1985，《蜂窝 [1] 来自gNB的信号丢失：UE突发流量 · aligungr/UERANSIM问题#714》。 [在线]。可访问：https://github.com/aligungr/UERANSIM/issues/714。访问日期：2026- 07-10。[36] 思科，《TRex》。 [在线]。可访问：https://trex-tgn.cisco.com/。访问日期：2026-07-10。