基于自适应元学习的5G核心网协议字段变异方法

熊炫睿[1]，张俊林[1]，周力[2]，李腾飞[1]，宁兆龙[1]
（1. 重庆邮电大学通信与信息工程学院，重庆 400065；2. 国防科技大学电子科学学院，湖南 长沙 410073）

摘　要：模糊测试是一种通过向目标系统输入异常或畸形数据来发现潜在漏洞的测试技术。针对现有模糊测试技术难以有效理解和适应5G协议字段的复杂语义与处理逻辑，导致生成的变异样本质量低、覆盖率差的问题，提出一种基于自适应元学习的5G核心网协议字段变异方法。该方法通过对5G核心网协议规范进行解析，提取协议字段的语义信息和处理逻辑，构建变异规则集。同时，利用元学习框架，结合在OAI-5G、5GCore_NMP等仿真环境中获得的变异命中率反馈，动态调整并优化字段变异策略。通过迭代学习进行策略更新，模型能够自适应生成更具潜在攻击性的变异样本。实验结果表明，与传统的基于规则或随机变异的模糊测试变异方法相比，所提方法显著提高了协议变异样本的质量与变异覆盖率。

关键词：协议变异；自适应元学习；样本生成；异常检测
中图分类号：TN92
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025164

Protocol field mutation method for 5G core network based on adaptive meta-learning

XIONG Xuanrui[1], ZHANG Junlin[1], ZHOU Li[2], LI Tengfei[1], NING Zhaolong[1]
1. School of Communications and Information Engineering, Chongqing University of Posts and Telecommunications, Chongqing 400065, China
2. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China

Abstract: Fuzz testing is a testing technique that discovers potential vulnerabilities by inputting abnormal or malformed data into a target system. To address the problem that existing fuzzing techniques generate low-quality mutated samples and achieve poor coverage due to their difficulty in effectively understanding and adapting to the complex semantics and processing logic of 5G protocol fields, a protocol field mutation method for 5G core network based on adaptive meta-learning was proposed. In this method, the 5G core network protocol specifications were analyzed to extract the semantic information and processing logic of protocol fields, thereby constructing a mutation rule set. Meanwhile, a meta-learning framework was utilized, combined with mutation hit rate feedback obtained from simulation environments such as OAI-5G and 5GCore_NMP, to dynamically adjust and optimize the field mutation strategy. Through iterative learning and strategy updates, more potentially aggressive mutation samples were adaptively generated. Experimental results show that compared with traditional rule-based or random fuzz testing mutation methods, the proposed adaptive meta-learning method significantly improves the quality of protocol mutation samples and increases the mutation coverage.

Keywords: protocol mutation, adaptive meta-learning, sample generation, anomaly detection

收稿日期：2025–07–01；**修回日期：**2025–09–16
通信作者：周力，zhouli2035@nudt.edu.cn
基金项目：国家自然科学基金资助项目（No.62171449）；重庆市自然科学基金资助项目（No.CSTB2024NSCQ-JQX0013）
Foundation Items: The National Natural Science Foundation of China (No.62171449), The Natural Science Foundation of Chongqing (No.CSTB2024NSCQ-JQX0013)

0　引言

随着5G网络在全球范围的大规模商用部署，5G网络安全问题日益成为急需解决的重要课题之一[1]。5G不仅显著提升了通信速度和连接密度，还引入了网络切片、虚拟化、边缘计算以及物联网等复杂的技术体系[2]。在边缘网络中，模仿学习算法虽然能实现高效服务迁移和资源协同以优化网络性能，但也显著增加了5G整体架构的复杂性[3]，导致网络安全面临前所未有的多样化挑战。目前，5G安全研究主要集中于控制面协议的消息传输机制、网络架构中的潜在安全漏洞识别与防护等领域[4]。相比4G网络，5G的复杂性和动态性对安全提出了更高要求。尤其是在5G核心网中，复杂的信令流程和多样化的应用场景使安全问题变得尤为突出[5]。

从历史脉络来看，在3G时代，网络安全研究的重心主要集中在用户隐私保护和认证机制的优化[6]。在4G时代，随着虚拟化技术的引入，网络安全研究扩展至分布式攻击防护和网络功能虚拟化的安全问题[7]。在5G时代，随着控制面协议信令流程的复杂化以及动态化应用场景的增加，网络安全挑战进一步加剧，研究焦点逐渐转向智能化威胁分析、动态监测和自动化响应[8]。此外，5G支持网络切片、边缘计算和大规模物联网设备接入，使得网络安全不再局限于传统网络边界防护，而需要更综合的安全解决方案，涉及隐私保护、身份认证、数据完整性保障、资源隔离、防御拒绝服务攻击等方面[9]。已有研究尝试引入高级调度算法来优化资源配置，以提升网络安全性[10]。

为应对这些挑战，学术界和工业界积极探索有效的安全分析与防护手段。模糊测试作为一种自动化的安全测试技术，通过向目标系统中输入异常或畸形数据来发现潜在漏洞，已成为协议安全领域广泛应用的方法之一[11]。然而，当把传统模糊测试技术应用于5G核心网协议时，其有效性受到较大挑战。5G协议字段间复杂的语义关联与处理逻辑，使许多模糊测试工具生成的变异样本质量低、覆盖率差，难以发现深层次的漏洞。

当前，无论是基于固定规则还是简单随机变异的传统模糊测试方法，都普遍存在盲目性问题，即缺乏对协议上下文和变异效果的感知，导致大量测试资源被浪费在无效的变异上。虽然一些覆盖率引导的工具能够提升探索效率，但它们往往忽略了协议的语义信息，难以生成能够触发特定业务逻辑错误的测试用例。因此，如何使模糊测试具备更强的智能性，使其能够自适应地学习协议特性并生成高质量的变异样本，已成为5G协议安全测试领域需要解决的关键问题。

为进一步提升模糊测试在新协议或未知攻击场景下的适用性和效率，本文引入一种结合传统模糊测试技术优势的自适应元学习[12]方法。该方法从多任务中提取共性特征，针对不同应用场景动态优化变异策略。与基于固定规则或随机变异的传统模糊测试方法相比，该方法能够基于实际测试反馈进行持续迭代和策略调整，从而显著提高变异覆盖率和测试效率。

本文的主要研究工作如下。

1) 提出一种基于元学习的自适应协议字段变异方法，该方法通过对5G核心网协议规范进行深度解析，提取协议字段的语义信息和处理逻辑，构建变异规则集。同时，利用元学习框架，结合在OAI-5G、5GCore_NMP等协议仿真环境中获得的变异命中率反馈，动态调整并优化字段变异策略。

2) 针对5G核心网中的NGAP和HTTP/2协议，深入挖掘协议字段的语义信息和处理逻辑，系统梳理各字段的作用及其交互关系，结合协议特性识别潜在的异常注入点和可能产生的异常行为，为自适应变异策略提供有效的语义支撑。

3) 基于搭建的OAI-5G核心网仿真环境、5GCore_NMP和商业协议栈平台，对初始变异样本进行3层注入测试。基于测试反馈和变异覆盖率统计，利用元学习算法更新变异策略的权重和参数，并将新策略存储至策略库，生成新的变异样本，持续提升异常覆盖能力和检测精度。

1　相关工作

本节将回顾协议模糊测试的相关工作，并分析其在5G核心网场景下的适用性与局限性。模糊测试根据策略不同，主要分为基于随机变异的协议模糊测试、基于覆盖率引导的智能模糊测试和基于协议语法的模糊测试3类[13]。

1.1　基于随机变异的协议模糊测试

传统的协议模糊测试多依赖于预定义规则或随机变异，基于规则的方法通过专家知识定义变异策略。例如，文献[14]针对5G NAS协议设计了一种

基于预定义规则的智能模糊测试算法，通过解析协议规范指导变异过程，取得了良好效果。然而，此类方法严重依赖专家经验，规则库更新滞后，难以应对协议的演进和复杂的未知攻击模式。相较之下，随机变异方法（如文献[15]中用于基站测试的框架）虽然实现简单，但其变异过程具有盲目性，导致生成的测试用例质量较差，难以有效触发深层逻辑漏洞。此类方法通常面临代码覆盖率不足、测试效率低等问题，限制了其在复杂协议场景中的应用。

1.2 基于覆盖率引导的智能模糊测试

为解决随机测试的盲目性所导致的效率低下问题，更先进的模糊测试技术应运而生。基于覆盖率引导的智能模糊测试，以AFL为代表，通过监控程序执行路径，优先选择能够探索新代码路径的变异样本，从而显著提升测试效率。在此基础上，智能模糊测试进一步融合机器学习技术，例如，利用遗传算法[16-17]或联邦学习[18]来学习协议行为与反馈信息，从而生成更具针对性的测试用例，并提升在异构网络环境[19]下的安全性和隐私性。另一个重要方向是基于语法的模糊测试，该方法依据协议规范与数据格式约束，生成在语法上正确但包含恶意变异的输入，以测试系统对合法异常数据的处理能力。

在5G协议安全领域，研究者广泛借鉴了上述思想。例如，文献[20]开发了针对LTE和5G核心网接口的特定模糊测试框架。尽管这些技术在通用场景下表现出色，但在应用于5G核心网协议时，其局限性依然明显。无论是通用的覆盖率引导还是基于语法的生成方法，往往都缺乏对协议字段深层语义的理解。虽然其变异策略能增加代码覆盖率和保证语法正确性，但仍难以构造出能通过复杂协议状态机验证且触发特定业务逻辑漏洞的测试用例。文献[21]也指出了盲目变异的低效性，并提出优先变异非关键字段的策略，但这本质上仍是一种静态启发式规则，未能真正实现动态自适应。

1.3 基于协议语法的模糊测试

与基于变异的方法不同，协议语法模糊测试不依赖初始种子，而是基于对目标协议的协议规范和文法范式的深入理解，从零开始构建测试用例。例如，基于语法的模糊测试依据协议规范与数据格式约束，生成符合语法且包含部分变异内容的输入，以测试系统对合法异常数据的处理能力[22]。理论上，这种方法能够探索更广阔的输入空间。

然而，在面对5G核心网NGAP、PFCP协议等高度复杂且状态化的场景时，纯粹基于协议语法的模糊测试方法在模型构建上面临较高的成本。因此，为NGAP协议构建一个完整且精确的ASN.1文法模型并包含所有字段间的隐式语义约束和状态依赖，是一项烦琐且容易出错的任务。另外，存在语义鸿沟，即使生成的样本在语法上完全正确，也可能由于不符合当前协议会话的上下文状态，被协议栈的早期逻辑直接拒绝，无法深入测试后端的处理逻辑。这种方法没有考虑实际的核心网在实现3GPP协议规范时的差异，导致生成的数据包无法在真实核心网中注入以达到变异的效果。

综上所述，现有针对5G协议的模糊测试方法存在明显短板，基于规则或随机变异的方法采用固定的变异策略，无法适应协议的复杂性和动态性。通用的覆盖率引导方法缺乏对协议语义的感知，难以构造出高质量的测试用例。而基于协议语法的模糊测试强依赖于一个难以构建和维护的完美协议模型。因此，解决上述问题的关键在于实现变异策略的智能化和自适应。为此，本文提出一种基于自适应元学习的5G核心网协议字段变异方法。

2 系统模型

本文提出了AM-VarProto模型框架，如图1所示。该模型一方面充分利用协议结构信息，另一方面通过反馈驱动对变异策略进行动态优化。

该模型框架主要包含初始策略生成、反馈收集与评估、元学习模型训练和自适应变异策略再生成4个部分。

1) 初始策略生成。借助ASN1编译器，对ASN.1抽象文件进行深度解析，运用C语言提取各字段取值范围、长度、依赖关系等语义信息。同时，深入剖析协议流程C文件，梳理关键函数调用和字段处理逻辑。通过建立语义－逻辑映射规则，将获取的信息转化为初始字段变异策略，存储至初始策略库，为后续变异样本生成提供支持。

2) 反馈收集与评估。将初始变异样本注入5G核心网仿真环境中进行测试，并通过日志分析或系统监控工具的反馈信息评估测试效果。

3) 元学习模型训练。基于测试反馈信息，使

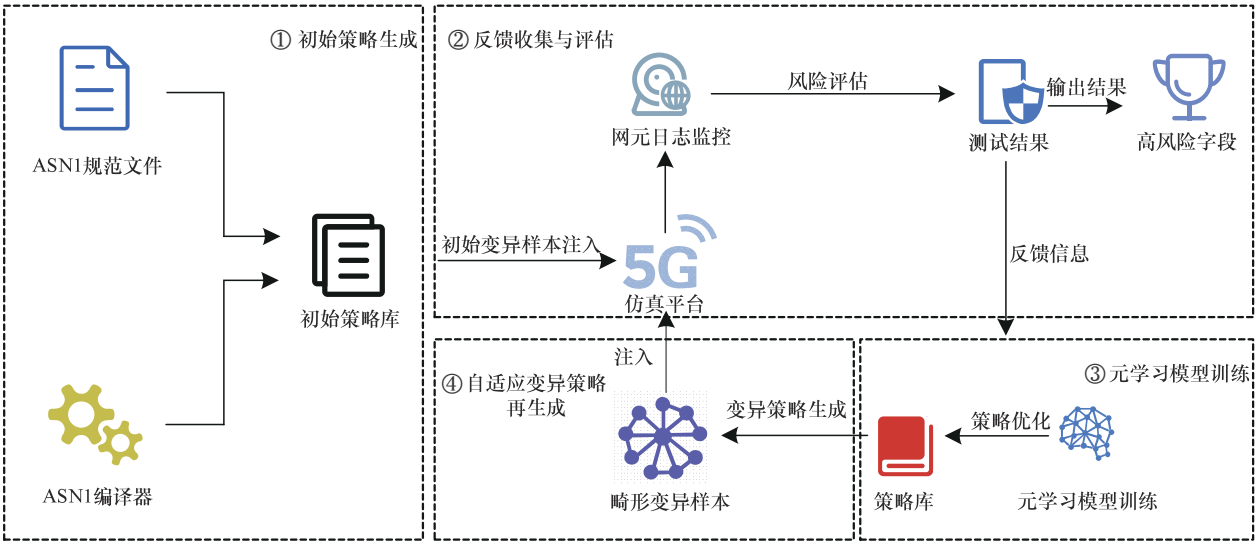


图1　AM-VarProto 模型框架

用元学习算法对变异策略的权重或参数进行更新，并将更新后的策略写入策略库中。

4) 自适应变异策略再生成。在完成元学习算法的参数更新后，结合协议字段的结构信息以及前一轮反馈中对异常覆盖度的统计结果，动态生成新的变异样本。

3　算法设计

3.1　自适应元学习协议字段变异算法

在明确变异设计框架后，将模型框架中的每步映射到具体的计算式和算法，以下详细阐述实现过程。

1) 初始变异样本生成

设 $P=\{f_1,f_2,\cdots,f_n\}$ 为字段集合，F_i 为第 i 个字段，$V(f_i)$ 为合法取值范围。初始变异样本为

$$f_i'=V(f_i)+\Delta_i,\Delta_i=w_i\cdot \mathrm{Random}(\mu_i,\sigma_i) \quad (1)$$

式(1)描述了变异样本的生成过程，其中 Δ_i 是对字段 F_i 的扰动，其大小由变异权重 w_i 和随机分布共同决定。w_i 表示字段触发异常的潜力，初始值为 $\frac{1}{n}$，旨在公平分配变异机会，体现未优化时的均匀性。$\mathrm{Random}(\mu_i,\sigma_i)$ 采用正态分布，$\mu_i=0$ 确保扰动无初始偏置，$\sigma_i=\mathrm{std}(V(f_i))$ 则根据字段范围动态设定。例如，若 $V(f_i)$ 的取值范围为 0~255，则 $\mathrm{sigma}_i\approx 25$，生成的值可有效测试边界条件。结合 5G 协议的 ASN.1 解析，这种方法能快速生成覆盖字段级、字节级和比特级的初始样本，为后续优化提供支持。

2) 损失函数定义

优化目标的损失函数为

$$L(\theta)=\sum_{T_j\in T} l(T_j,\theta_j)+\lambda\|\theta\|_2^2 \quad (2)$$

其中，损失函数 $L(\theta)$ 由任务损失和正则化项两部分构成，θ 为模型的权重参数，λ 为控制正则化强度的超参数，用于防止过拟合。任务损失 $l(T_j,\theta_j)$ 量化变异策略的失效程度，如式(3)所示。

$$l(T_j,\theta_j)=1-\frac{\mathrm{Success}(T_j)}{\mathrm{Total}(T_j)} \quad (3)$$

其中，$\mathrm{Success}(T_j)$ 为触发异常的样本数，$\mathrm{Total}(T_j)$ 为样本总数。这一定义将测试效果转化为可计算指标，值越小说明策略越有效。$\theta=\{w_i,\mu_i,\sigma_i\}$ 包含所有字段的参数，$\lambda\|\theta\|_2^2(\lambda=0.01)$ 通过 L2 范数限制参数幅度，避免过拟合，确保策略在不同任务间的泛化能力。与传统模糊测试的静态规则相比，该损失函数引入动态反馈，使优化更具针对性。

3) 自适应元学习算法优化

内层更新的表达式为

$$\theta_j=\theta-\alpha\nabla_\theta l(T_j,\theta) \quad (4)$$

外层更新的表达式为

$$\theta=\theta-\beta\sum_{T_j}\nabla_\theta\left[l(T_j,\theta_j)+\lambda\|\theta_j\|_2^2\right] \quad (5)$$

通过上述两阶段更新优化 θ。内层更新针对单一任务，使用梯度下降调整 θ 为 θ_i，α 控制步长，

$\nabla_\theta l$通过链式法则计算，例如，对w_i的偏导反映字段变异对异常的影响。外层更新整合多任务反馈，其中，β协调全局优化，正则化项λ确保稳定性。如算法1所示，该算法完整实现了AM-VarProto模型框架，生成优化后的θ，以便于自适应变异策略再生成。

算法1 字段变异的自适应元学习算法

输入 ASN.1字段P，任务集T，α，β，λ

输出 优化后的θ

1) 初始化$\theta=\{w_i=\frac{1}{n},\mu_i=0,\sigma_i=\mathrm{std}(V(f_i))\}$

2) 解析ASN.1文件和C文件 for $V(f_i)$

3) for k=1 to K

4) sample T_{batch} from T

5) for each T_j in T_{batch}

6) $M_0=\{f_i'=V(f_i)+w_i\cdot\mathrm{Random}(\mu_i,\sigma_i)\}$

7) 注入M_0到OAI

8) $F_j=\mathrm{CollectFeedback}(\mathrm{Wireshark})$

9) $l(T_j,\theta_j)=1-\frac{\mathrm{Success}(T_j)}{\mathrm{Total}(T_j)}$

10) $\theta_j=\theta-\alpha\nabla_\theta l(T_j,\theta)$

11) $\theta=\theta-\beta\sum_{T_j}\nabla_\theta[l(T_j,\theta_j)+\lambda\|\theta_j\|_2^2]$

12) end for

13) end for

14) 返回θ

上述流程表明，自适应元学习在设计协议字段变异策略中既能充分利用ASN.1抽象文件和C代码包含的结构与语义信息，又能结合测试反馈不断完善策略。相比传统基于固定规则或随机采样的模糊测试方法，该方法大幅降低了无效变异样本比例，显著提升了5G核心网协议变异效率及覆盖深度。

3.2 变异方法设计

在对协议字段特性进行详细分析的基础上，本节聚焦于设计高效的变异方法，以实现对5G核心网协议中潜在漏洞的深度检测。与传统“盲目”变异不同，自适应元学习方法能够在测试过程中根据协议字段的重要性、系统响应反馈和历史变异结果动态优化策略。具体而言，变异方法从字段级、字节级和比特级3个层次展开，并融入自适应元学习的优化机制。

3.2.1 字段级变异

字段级变异针对协议字段整体的结构和语义特性，测试系统对异常输入的容错能力。基于前期对协议字段的深入分析，本文方法优先变异对协议逻辑影响较大的字段，如控制信令、状态标识字段。传统字段变异多为随机改值或字段删除，缺乏系统性和针对性，而自适应元学习通过动态权重优化，使变异更聚焦关键字段，如式(6)所示。

$$f_i'=V(f_i)+\Delta_i^f,\Delta_i^f=w_i\cdot\mathrm{Random}(\mu_i^f,\sigma_i^f)\cdot S(f_i) \tag{6}$$

其中，$V(f_i)$是字段的合法取值范围，从ASN.1文件中解析获得。扰动项Δ_i^f由自适应权重w_i、正态分布$\mathrm{Random}(\mu_i^f=0,\sigma_i^f=\mathrm{std}(V(f_i)))$和操作函数$w_i$组成，定义具体变异类型，如式(7)所示。

$$S(f_i)=\begin{cases}\mathrm{llegalScale}(V(f_i)), & \text{字段值篡改}\\ 0, & \text{字段缺失}\\ 2\cdot V(f_i), & \text{字段重复}\\ \mathrm{ReorderOffset}(f_i,P), & \text{字段顺序调整}\end{cases} \tag{7}$$

式(7)中对字段级别4种变异方法进行定义，下面将详细说明其含义。1) 字段值篡改：通过llegalScale()函数生成超出范围的值；2) 字段缺失：若$S(f_i)=0$，即$f_i'=V(f_i)$，模拟必填字段丢失；3) 字段重复：表示重复插入；4) 字段顺序调整：ReorderOffset()函数根据w_i计算偏移量，例如，将高权重字段移至末尾，检测顺序依赖漏洞。

3.2.2 字节级变异

字节级变异针对字段内部的二进制结构，测试系统对数据完整性与一致性的处理能力。传统字节级变异多采用随机插入或删除字节，难以针对协议特性进行精准调节。本文结合字段长度和编码分析设计自适应权重，以动态调整字节变异方向。如式(8)所示。

$$B(f_i')=B(f_i)+\Delta_i^b,\Delta_i^b=w_i\cdot\mathrm{Random}(\mu_i^b,\sigma_i^b)\cdot B_{\mathrm{op}}(f_i) \tag{8}$$

其中，$B(f_i)$为字节序列，Δ_i^b由w_i、$\mathrm{Random}(\mu_i^b,\sigma_i^b)$和$B_{\mathrm{op}}$决定，$B_{\mathrm{op}}$为字节操作函数，Random()中的$\mu_i^b=0$，$\sigma_i^b=0.5\cdot\mathrm{std}(B(f_i))$，定义字节变异操作类型如式(9)所示。

$$B_{\mathrm{op}}(f_i)=\begin{cases}\mathrm{BitFlip}(B(f_i)), & \text{字节内容修改}\\ \mathrm{InsertByte}(n), & \text{字节插入}\\ -B(f_i)_k, & \text{字节删除}\end{cases} \tag{9}$$

其中，字节内容修改指BitFlip翻转字节值；字节插入指插入n个随机字节；字节删除指移除第k个字节，模拟数据丢失。

3.2.3　比特级变异

比特级变异深入字段的最小单位，针对二进制表示进行微调，测试系统对底层数据变化的敏感性。传统方法通常忽略比特级操作，而5G协议的标志位或校验位对系统逻辑至关重要。本文方法利用自适应元学习优化比特选择，分别如式(10)和式(11)所示。

$$f_i' = f_i + \Delta_i^t \tag{10}$$

$$\Delta_i^t = w_i \cdot \mathrm{Random}(\mu_i^t,\sigma_i^t) \cdot T(f_i,k) \tag{11}$$

其中，f_i是字段的二进制值，$\mu_i^t = 0$，$\sigma_i^t = 1$（比特级扰动较小），$T(f_i,k)$为比特操作函数，选择变异位k，自适应优化根据反馈调整k的优先级，其定义分别如式(12)和式(13)所示。

$$T(f_i,k) = (1 \ll k) \tag{12}$$

$$k = \mathrm{SelectBit}(w_i,H) \tag{13}$$

其中，式(12)表示比特翻转，翻转第k位，例如，将标志位从0变为1。式(13)表示比特掩码，若σ_i^t增加，可扩展为多位操作，如$f_i' = f_i \oplus 0x03$。

上述3层变异策略依赖于自适应元学习算法对参数进行动态调整，并在下文中将该机制与具体实现方法相结合。与传统固定不变的变异策略不同，本文采用反馈驱动的优化机制，以提升变异操作的针对性和执行效率。参数更新基于式(2)进行，其中$\theta = \{w_i,k_f,k_b,k\}$包含各层次的可调参数。在优化过程中，系统根据反馈信息动态调整w_i和缩放因子。例如，若字段缺失触发异常，则k_f增大；若字节插入无效，则k_b降低。这种动态调整使变异策略逐步聚焦高风险操作，提升漏洞发现率。本文所提出的分层自适应变异算法的具体实现流程如算法2所示。

算法2　分层自适应变异算法

输入　P,θ,H

输出　M'

1) 对于P中的每个f_i

2)　if 层级=“field”

3)　$\Delta_i^f = w_i \cdot \mathrm{Random}(0,1.5 \cdot \mathrm{std}(V(f_i))) \cdot S(f_i)$

4)　$f_{i'} = V(f_i) + \Delta_i^f$

5)　else if 层级=“Byte”

6)　$\Delta_i^b = w_i \cdot \mathrm{Random}(0,0.5 \cdot \mathrm{std}(B(f_i))) \cdot B_{\mathrm{op}}(f_i)$

7)　$B(f_{i'}) = B(f_i) + \Delta_i^b$

8)　else if 层级=“bit”

9)　$k = \mathrm{SelectBit}(w_i,H)$

10)　$\Delta_i^t = w_i \cdot \mathrm{Random}(0,1) \cdot (1 \ll k)$

11)　$f_{i'} = f_i + \Delta_i^t$

12) 将f_i'添加到M'

13) 将M'注入环境，收集F

14) 通过MAML更新$\theta(L(\theta),F)$

15) 返回M'

通过上述分层变异策略设计，本文在字段、字节和比特3个层面实现对协议数据中潜在异常的全面覆盖。通过引入动态权重分配与反馈机制，有效保障变异操作的针对性与执行效率。相较于传统无指导的随机变异方法，本文结合系统响应信息与字段特征，在字段级变异中对高权重字段的扰动更易快速触发边界异常（如缓冲区溢出）。而在字节级和比特级，则通过微小的数据变动揭示协议实现过程中的深层次缺陷。

4　实验评估

本节系统介绍了实验环境的搭建过程与配置信息，构建包括OAI-5G仿真平台[23]和5GCore_NMP协议仿真平台的测试环境，以真实还原5G核心网各关键网元的协议交互过程。在此基础上，针对NGAP及HTTP/2核心协议，结合上述自适应元学习变异算法，开展多层次协议字段的变异注入测试。通过对信令数据包的捕获分析、网元运行日志的监测以及协议流程的对比验证，系统评估变异策略在协议异常触发及漏洞检测中的效果与性能表现。

4.1　实验环境

4.1.1　OAI-5G仿真平台

OpenAirInterface （OAI）是一个开源的无线通信软件平台，支持符合3GPP标准的5G NR网络协议栈，实现完整的无线接入网和核心网功能。本文基于Docker容器技术部署OAI平台，以满足在通用计算机环境下实现快速搭建和高度可控的需求。OAI-5G软硬件环境配置如表1所示，其中系统选用Ubuntu 18.04，搭配Docker和Docker compose，并使用UERANSIM进行用户设备仿真。

表 1　　OAI-5G 软硬件环境配置

软硬件环境	版本
Linux 操作系统	Ubuntu 18.04
Docker	v19.03.6
Docker-compose	v1.27.4
UERANSIM	v2.2.1
USRP	B210

为实现真实的无线信号传输，采用 USRP B210 射频设备模拟 5G 基站的 N78 频段射频，实现硬件级别的信号复现，仿真网络平台硬件如图 2 所示。

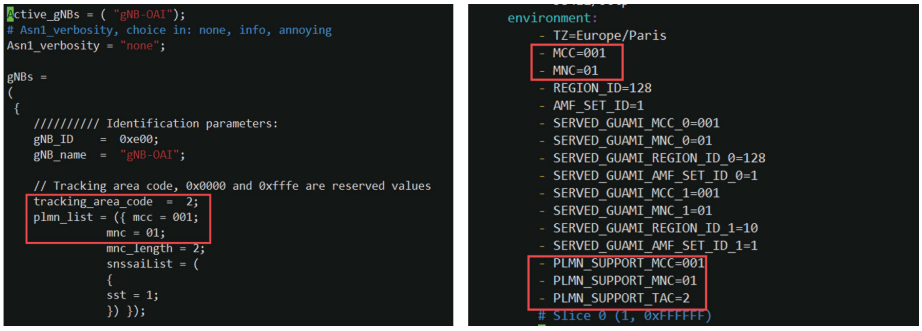
图 2　仿真网络平台硬件

同时，为确保基站与核心网成功相连，需保证基站与核心网相关配置一致，图 3 展示了下一代基站（GNB）和 OAI 配置信息。

4.1.2　5GCore 协议仿真平台

基于虚拟机的 5GCore_NMP 协议仿真平台利用 SOCKET 通信进程模拟核心网网元间的协议交互，重构了符合 3GPP 规范的网络拓扑与通信接口，5GCore_NMP 物理架构如图 4 所示。

在 5GCore 协议仿真平台中，GNB 通过 NG 接口向接入和移动性管理功能（AMF, access and mobility management function）发起建立请求，携带 GLOBAL_RAN_NODE_ID、MCC、MNC 等关键信息。当 AMF 收到 GNB 发起的 NGSetup Request 后，首先解析并验证该请求，确保 GNB 身份合法且消息格式符合规范。然后，AMF 向 GNB 发送 NGSetup Response，完成 NG 接口的建立。最后，AMF 启动用户认证流程，以验证用户身份的合法性并确保网络接入安全。



(a) GNB配置信息　　(b) OAI配置信息

图 3　GNB 和 OAI 配置信息

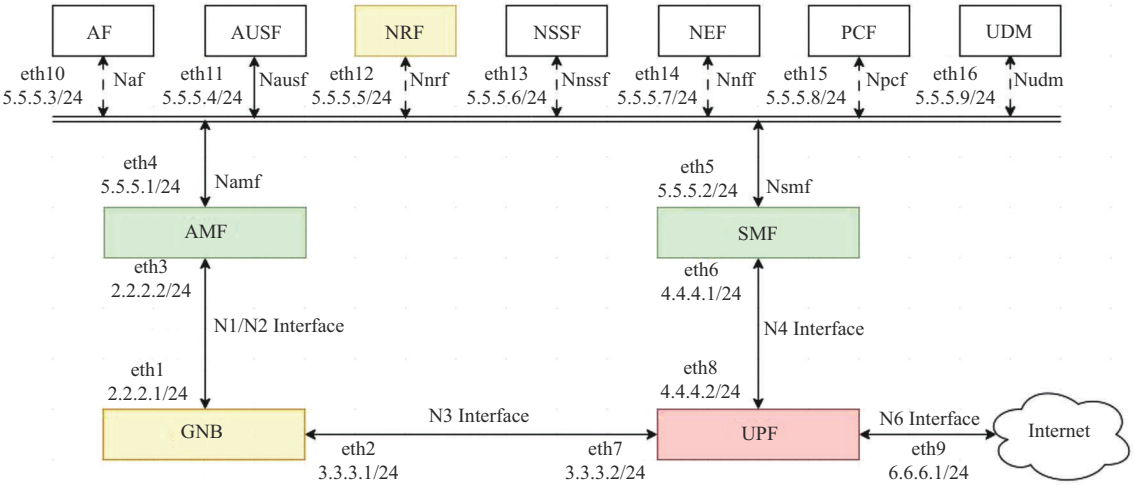


图 4　5GCore_NMP 物理架构

通过搭建上述2个仿真平台，本文成功构建了真实、可靠的5G核心网协议环境，并获取了关键流程的仿真数据，为后续协议变异测试与安全分析工作提供了环境基础。

4.2　超参数分析

为更深入地验证本文模型中各关键超参数设置的合理性，本节开展了系统性实验与分析。

在AM-VarProto模型的变异样本生成环节，对式(1)中扰动项$\Delta_i = w_i \cdot \mathrm{Random}(\mu_i,\sigma_i)$所采用的随机分布类型进行分析。本文采用正态分布作为基础变异生成策略，主要由于其他分布类型（如均匀分布）缺乏对边界值与异常跳变区域的聚焦能力，易生成大量被服务端快速过滤的无效变异。指数分布与泊松分布分别适用于小幅度扰动建模与离散事件模拟，其统计特性与协议字段的连续性、结构性存在匹配错误，易导致语义非法或格式错误的无效样本。相较之下，正态分布配合标准差$\sigma_i = \mathrm{std}(V(f_i))$的自适应初始化，能够自动聚焦于边界和异常值等高风险区域。更重要的是，即使初始分布非全局最优，本文所提元学习框架仍可通过动态调整权重w_i与标准差σ_i，在迭代中自适应优化扰动策略，从而有效降低模型对初始分布选择的敏感性。因此，在后续实验中，本文统一采用正态分布作为基础扰动模型，并将优化焦点集中于元学习超参数α、β和λ调优，以更清晰地评估其对模型性能的独立贡献。

在AM-VarProto模型中，变异权重w_i的初始化采用均匀分布策略$w_i = \dfrac{1}{n}$，旨在保证初始阶段各字段获得均等探索机会，避免引入先验偏见。后续通过元学习反馈动态调整权重，使其快速收敛至最优分布。式(4)和式(5)中的超参数α、β和λ共同决定元学习框架的收敛速度与泛化能力。表2展示了在不同超参数配置下，模型在多个训练轮次中的变异覆盖率表现。

从表2的实验结果可以看出，内循环学习率α显著影响模型的探索广度。当$\alpha = 0.001$时，模型在所有迭代轮次中表现最佳，在第25轮达到最高覆盖率0.578，这表明该设置能够保持稳定的探索性能，且在后期迭代中仍能持续提升覆盖率。外循环学习率β反映模型对元更新步长的敏感性，当$\beta = 0.000\,1$时，模型在早期迭代中即展现出较高的覆盖率增长趋势，并在后期持续领先，说明较小且稳定的元更新步长有助于提升模型的全局探索能力。正则化系数λ体现模型复杂度与泛化能力之间的权衡，当$\lambda = 0.001$时，模型在第20轮和第25轮均表现较佳，这说明适度的正则化是必要的。过低的正则化可能使模型对已探索的路径产生过拟合，限制了其向新领域泛化的能力；而过高的正则化可能过度平滑权重，使模型无法有效识别并优先探索高价值的变异字段，从而抑制整体探索效率。

表2　超参数对变异覆盖率的影响

超参数	值	第10轮	第15轮	第20轮	第25轮
α	0.000 1	0.364	0.430	0.490	0.502
	0.001	0.365	0.437	0.495	0.578
	0.01	0.348	0.403	0.462	0.531
β	0.000 1	0.275	0.367	0.454	0.524
	0.001	0.299	0.355	0.414	0.502
	0.005	0.278	0.380	0.406	0.475
λ	0.001	0.360	0.447	0.489	0.483
	0.005	0.349	0.415	0.470	0.472
	0.01	0.344	0.417	0.443	0.447

基于上述超参数分析结果，在后续对比实验中均采用统一的参数配置以控制变量。对于AM-VarProto模型，内循环学习率α设置为0.001，外循环学习率β设置为0.000 1。正则化项系数λ设置为0.001，上述参数能够在模型拟合能力与泛化性能之间实现良好平衡。

4.3　实验评价指标

为系统评估本文提出的AM-VarProto方法在5G核心网协议安全测试中的有效性与效率，并确保与现有基准模糊测试方法的比较具备公平性和可比性，本节将详细阐述实验所采用的量化评价指标。本文从探索广度、变异精度和资源消耗3个维度，综合评估各类模糊测试方法的性能表现。

变异覆盖率的定义如下。在完成N轮迭代优化后，成功触发协议栈异常响应的协议字段数量与本次实验中被选为变异目标字段总数的比值。该指标用于评估模糊测试策略的探索广度与自适应学习能力，较高的变异覆盖率表明测试方法能够有效探索协议结构中的潜在脆弱点，避免陷入局部搜索或重复测试已知路径。

致效率的定义如下。在某轮次中，被判定为成功致效的变异样本数量与该轮生成的变异样本总数的比值，该指标是衡量模糊测试策略攻击精度的核心标准。其中，成功致效并非指变异样本被核心网元的表层校验机制识别并按预期丢弃，如格式错误检测、长度越界等正常过滤行为，而是指其成功绕过基础防御机制，并引发网元产生非预期行为，如信令流程异常中断、内存访问越界或服务崩溃等。此类行为表明，协议解析逻辑或状态处理模块存在深层缺陷，具有较高的安全危害性。因此，致效率不仅反映测试方法的漏洞触发能力，还体现了其对高危漏洞的精准挖掘水平。

4.4 实验结果

4.4.1 NGAP协议字段变异生成与注入

在变异处理阶段，需要解析NGAP协议的ASN.1规范文件，利用开源工具asn1c将其转换为对应的C语言编码或解码模块，实现对NGAP协议消息的自动处理。本文实验共提取2564个协议交互流程，并对所有与AMF网元相关的协议流程进行语义分析和刻画。协议变异应针对具体目标协议流程开展，而非仅针对单一协议字段，原因在于部分字段为通用标识字段。例如，RAN-UE-NGAP-ID协议字段在66个与无线侧RAN分配给用户设备（UE, user equipment）相关的协议流程中，该字段是UE在NG接口中的唯一标识。相比之下，NAS-PDU协议字段涉及7个协议流程，代表UE与核心网AMF网元之间用于认证、移动性管理及会话管理的非接入层数据单元。由此可见，在进行协议变异时，不能仅依据单一字段，还需结合具体的协议流程进行针对性处理。

经过筛选可知，关键字为“mandatory”的协议层共包含324个IEs消息层。本文选取初始UE消息InitialUEMessage流程开展实验，通过对ASN.1规范文件的分析可知，该流程共涉及22个IEs消息层，其中4个为必需项，分别为RAN-UE-NGAP-ID、NAS-PDU、UserLocation Information和RRCEstablishmentCause。参考3GPP TS 24.501（Release 17）技术规范进行分析总结，在22个消息层中，5个消息层与UE首次接入核心网的过程相关。UE初始化协议流程如图5所示，除了上述4个消息层，还涵盖UEContextRequest协议层。

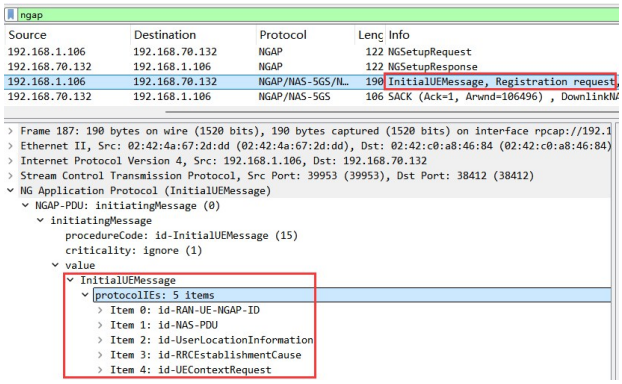


图5 UE初始化协议流程

从上述UE初始化协议流程的Pcap数据包分析可知，InitialUEMessage消息的传输共涉及5个协议层级。通过对消息字段的语法结构进行深入分析，进一步确定这5个协议层级下共包含46个协议字段，而每个协议字段又对应多个具体的取值或枚举选项。在前期研究中，本文将协议变异方法划分为字段级、字节级和比特级3个层次。基于此分类，本文将该流程中的协议变异操作也相应地划分为3个层级。在此基础上，本文将协议字段的异常特征划分为9类，并对每类特征进行明确定义，协议字段异常种类定义如表3所示。

表3 协议字段异常种类定义

异常特征类型	异常特征缩写	描述
Field Value Modification	FVM	字段值篡改
Field Missing	FM	字段缺失
Field Repetition	FP	字段重复
Field Reordering	FRO	字段顺序调整
Byte Content Modification	BCM	字节内容修改
Byte Insertion	BI	字节插入
Byte Deletion	BD	字节删除
Bit Flip	BF	比特翻转
Bit Mask Addition	BMA	比特掩码增加

随后，对46个协议字段进行初步变异测试，采用AM-VarProto算法生成初始变异字段集合F_{initial}。然而，首轮变异难以确保变异的有效性，部分字段未能有效触发异常响应。为进一步提升变异效果，将F_{initial}中触发异常的字段提取为变异种子，结合AM-VarProto算法进行优化，内层更新基于种子样本优化异常参数，外层更新利用OAI核心网的异常

响应反馈，生成优化后的变异字段集合$F_{optimized}$。优化后的$F_{optimized}$通过信令接口注入OAI核心网中，并对信令数据包进行捕获，监控响应状态。

为进一步验证自适应元学习的效果，本文实验记录了变异覆盖率随迭代轮次的变化趋势。经过前期预实验和理论分析发现，若迭代轮次过少，则无法充分展现模型性能的变化趋势；若过多，则会耗费大量计算资源且边际效益递减，因此将迭代轮次设置为20轮。在此过程中，为增强实验对比性，引入基于AFL的覆盖引导[24]和基于Atheris的覆盖引导[25]模糊测试2个开源模型，对46个协议字段的覆盖率变化趋势进行对比，图6展示了趋势变化过程。

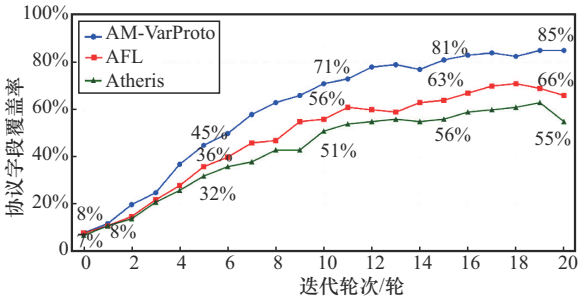


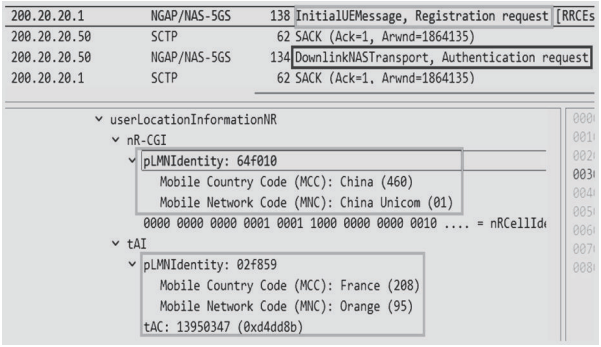
图6　变异字段覆盖率变化趋势

从图6可以看出，随着迭代轮次的增加，基于AM-VarProto算法的覆盖引导机制展现出动态调整变异参数的能力，并通过结合初始种子样本与核心网反馈信息，持续优化变异策略。相比之下，AFL与Atheris作为通用型模糊测试工具，虽然具备一定分支覆盖引导能力，但其变异过程依赖固定的规则策略，导致迭代效率较低，无法充分挖掘协议上下文信息，从而限制了变异覆盖的广度与深度。实验结果表明，在10轮迭代后，AM-VarProto的覆盖率已突破70%；经过20轮迭代后，其覆盖率比AFL模型高19%，比Atheris模型高30%，这充分说明本文方法在捕捉和利用协议流程特征方面具有显著优势。

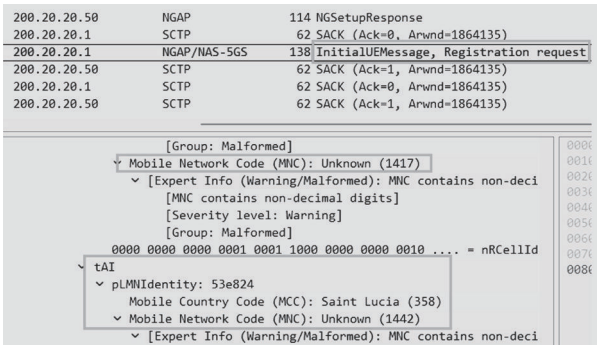
为准确评估变异效果，依据核心网对重放变异数据包的响应行为进行判定。若核心网通过容错机制维持正常运行，且未检测到关键字段异常，则判定为变异未触发异常；若核心网流程异常终止，并可定位到关键字段的异常行为，则判定为变异成功。以UE的PLMN字段为例，图7展示了该字段在初始变异与基于AM-VarProto算法变异下的实验结果对比情况。

通过对比图7(a)与图7(b)可见，在初始变异阶段，由于缺乏有效的学习样本，核心网的容错机制被激活。该机制使核心网忽略了变异字段的影响，从而维持后续交互流程的正常执行。如图7(a)中深黑色框标注所示，此时UE已进入下行数据传输阶段。图7(b)展示了在对变异样本进行多轮迭代学习后的实验结果，在此阶段，经过优化策略处理的变异字段成功触发了关键字段异常，导致核心网发生错误并终止后续信令流程。

考虑实际应用场景，字节层面的变异在网络协议测试中具有重要意义，为进一步拓展AM-VarProto变异算法的应用边界，本文基于5GCore_NMP开源工具，在NGAP协议中实现针对性的字节级变异模块。该模块将AM-VarProto算法应用于字节层面，将操作级别level设定为Byte，并对5G核心网的复杂协议交互进行形式化建模。本文实验选择Downlink NAS Transport流程作为变异测试的对象，并重点提取该流程中与NAS-PDU相关的定义部分，以执行字节层面的变异。



(a) 初始变异效果



(b) AM-VarProto算法变异效果

图7　初始变异效果对比AM-VarProto算法

为全面评估AM-VarProto在字节级变异场景下的有效性，本文实验选取2种基于覆盖引导的主流模糊测试工具AFL和Atheris作为对比模型。针对AM-VarProto、AFL和Atheris测试模型，分别在10轮、20轮和30轮不同设定的迭代轮次下进行实验，并统计了各自的变异致效率。结果如表4所示。

表4　　变异模型致效率对比

模型	迭代轮次/轮	协议异常次数/次	致效率
AM-VarProto	10	5	50%
	20	13	65%
	30	25	83%
AFL	10	6	60%
	20	11	55%
	30	19	63%
Atheris	10	4	40%
	20	9	45%
	30	17	56%

从表4的数据可以看出，AM-VarProto算法的致效率随着迭代轮次的增加而显著提升，在30轮迭代时，其针对NAS-PDU数据单元的变异致效率达83%。在所有测试的迭代轮次中，AM-VarProto的变异致效率均高于Atheris模型。在20轮迭代时，其变异成功率比AFL模型高10%；在30轮迭代时，差距进一步扩大至20%。上述结果充分体现了AM-VarProto在引发协议异常方面的优势。

结合3种模型的变异覆盖率和变异致效率对比实验结果表明，AM-VarProto算法在变异任务中的整体性能优于其他2种模型。为更直观展示该算法模块的实际效果，图8呈现了AM-VarProto在NAS-PDU数据单元上进行字节级变异所引发的具体协议异常行为。

图8　变异算法针对字节变异效果

从图8可见，NAS-PDU数据单元中部分字节被恶意变异，导致Downlink NAS Transport流程异常终止。该异常进一步影响了GNB向AMF发起的Initial UE Message流程，破坏了正常信令交互序列。NAS-PDU作为非接入层的核心承载结构，通常封装了UE的身份标识、鉴权密钥、安全算法选择、位置更新请求、状态信息及服务请求类型等关键信令内容。因此，对该字段进行语义感知的字节级变异，容易破坏消息的完整性与协议处理逻辑，从而引发核心网元的异常响应，甚至导致UE无法完成注册或建立会话，影响网络连接的稳定性与网元间通信的正常运行。

为进一步验证实验结果的准确性，本文通过前置部署的抓包工具，从GNB与AMF的网络接口捕获Downlink NAS流程产生的Pcap数据包，并对异常NAS-PDU中的变异字节进行精细化分析。如图9所示，经AM-VarProto算法生成的变异字节序列严重偏离NGAP协议规定的编码格式与语义约束，导致协议解析层校验失败，进而触发异常处理机制，最终造成后续信令流程中断。

同时，本文选取正常通信流程中的NAS-PDU数据单元作为对照，展示其标准字节结构，如图10所示。对比分析结果表明，在正常流程中，NAS-PDU能够正确携带UE的注册信息，并顺利推进注册及后续信令流程。而采用AM-VarProto算法对NAS-PDU关键字段实施字节级变异后，系统结合

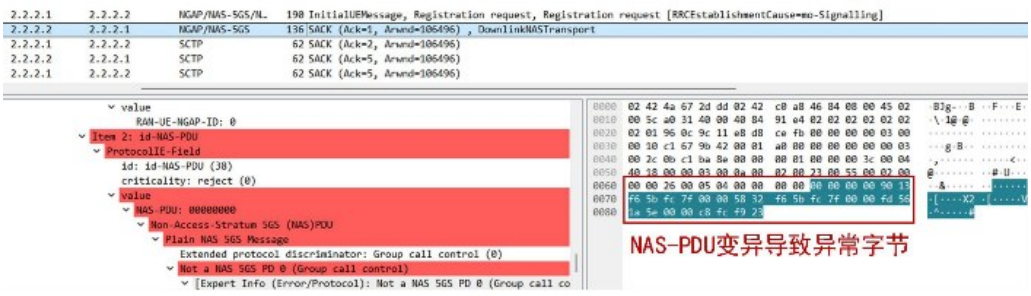


图9　NAS-PDU异常字节部分展示

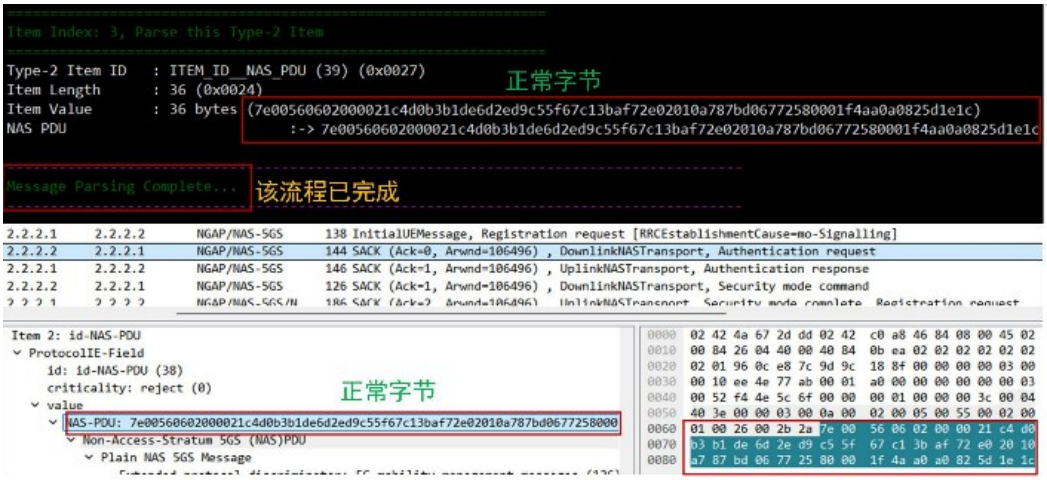


图10　NAS-PDU正常字节部分展示

协议字段的语义特征与上下文依赖关系，动态调整变异策略，成功生成具有高穿透性的畸形报文。此类报文可绕过部分浅层检测机制，直接作用于协议栈的核心解析逻辑，最终引发AMF网元崩溃或服务拒绝，导致信令流程被迫中断。

该结果不仅验证了AM-VarProto在字节级协议变异中的可行性与高效性，还体现了其通过语义引导与反馈学习相结合的方式，在不依赖先验漏洞知识的前提下，实现对深层协议逻辑缺陷的精准挖掘。与传统模糊测试方法相比，AM-VarProto显著提升了漏洞触发概率与攻击面覆盖深度，为5G核心网协议的安全评估提供有用的自动化测试手段。

4.4.2　资源消耗分析

为评估不同测试模型在运行过程中的资源消耗情况，实验从执行效率、内存占用和CPU使用率3个维度对AM-VarProto、AFL与Atheris方法进行对比分析，结果如图11所示。图11通过多组柱状图清晰展示了3种方法的单位时间执行次数（次/s）、峰值内存增长（MB）、平均CPU使用率以及最大CPU使用率4项关键性能指标上的表现。从实验结果可以看出，不同方法在资源利用方面呈现明显的权衡特征。在执行效率方面，AFL表现最优，单位时间内可完成最多测试用例的生成与执行。AM-VarProto次之，但仍显著高于Atheris。这一差异主

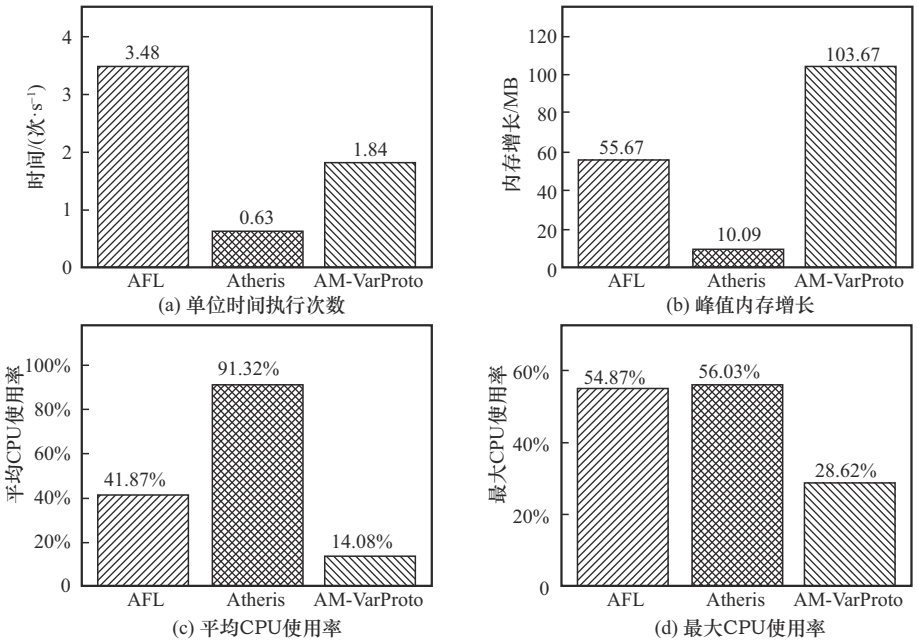


图11　消耗资源分布

要源于 AM-VarProto 引入元学习机制，在每轮迭代中需进行策略评估与参数更新，产生一定的计算延迟。

在 CPU 资源占用方面，AM-VarProto 的平均 CPU 使用率与最大 CPU 使用率均为三者中最低，表明该方法在实现智能变异时未引发严重的计算负载，元学习模块的运行开销控制在合理范围内。在内存消耗方面，AM-VarProto 的峰值内存增长最显著，明显高于 AFL 与 Atheris。这主要归因于其需要维护策略网络参数、历史反馈数据缓存及学习状态信息，体现了智能化策略所付出的额外存储代价。

综合来看，AM-VarProto 在牺牲部分执行速度与增加内存开销的前提下，实现对 CPU 等核心计算资源的高效利用。这一特性使其能够在有限的算力环境下稳定运行，同时保持高变异致效率。同时，验证了 AM-VarProto 在性能与资源消耗之间实现了良好的平衡，具备较强的工程实用价值。

4.4.3 HTTP/2 协议 SBI 接口注入

为验证本文提出的 AM-VarProto 自适应元学习变异策略在 HTTP/2 协议场景下的有效性，实验整合了 OAI-5G 核心网与测试环境，用于模拟核心网各个网元之间的通信过程。同时，在商用可编程协议栈平台上搭建关键信令流程，进一步验证 AM-VarProto 在真实协议交互过程中的变异效果。

协议数据单元（PDU, protocol data unit）会话建立过程是由 AMF 发送给会话管理功能（SMF, session management function）一个请求消息，目的是使 SMF 创建并维护与该 PDU 会话相关的会话管理上下文。这个过程是 5G 核心网中会话建立的关键步骤之一。AMF 通过调用 API 向 SMF 网元发送请求。随后，在已二次开发的协议栈平台上，选定目标信令流程，对基于服务的接口（SBI, service-based interface）的统一资源标识符（URI, uniform resource identifier）路径实施变异重定向。该平台集成了 AM-VarProto 变异引擎，并针对协议字段的比特级变异进行专项优化，支持通过前端界面配置对路径及消息体字段实施定向模糊测试。图 12 展示了针对路径的模糊测试配置。

(a) 变异路径重定向 (b) 模糊测试突变

图 12 针对路径的模糊测试配置

其中，address 为变量标识符，表示变异字段的初始样本，并历经 15 次变异策略的迭代更新。在变异过程中，将以 3GPP 协议规范中针对 SMF 的资源 API 定义的字符集为基础，进行变异策略更新。同时，限定变异后字符串的最大长度为 20。随后，还需要针对 PDUSession CreateSMContext_Req 协议流程携带的字段进行变异，针对不同字段类型采用差异化变异策略，如图 13 所示。

图 13(a)展示了需要进行变异的字段，图 13(b)展示了结合变异的字段特性，从而选择合适的变异类型，图 13(c)展示了对该类型字段变异的配置。随后运行该变异流程，通过协议栈平台的网元运行状态判断信令流是否正常交互，如图 14 所示，该

(a) 选择变异字段 (b) 选择变异类型 (c) 变异配置

图 13 变异目标字段及相关配置

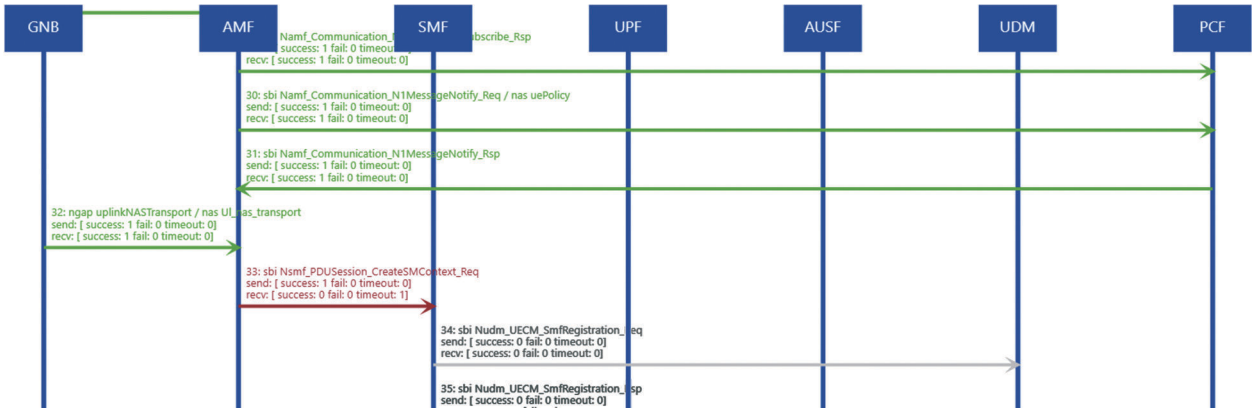


图14　目标信令流终止

信令流程经过变异后，造成PDUSession_CreateSMContext_Req信令流终止。

为系统评估AM-VarProto在HTTP/2协议下的泛化能力与稳定性，本文在会话建立流程CreateSMContext、会话更新流程UpdateSMContext以及会话释放流程ReleaseSMContext核心业务流程上进行测试。每个流程独立生成50个变异样本，覆盖其关键字段。所有样本均在AM-VarProto框架下经过20轮后生成。在每轮迭代中，模型根据上一轮反馈动态调整字段权重与扰动策略，最终采用统一标准致效率来自动化判定是否变异致效。本文实验选取AFL进行对比测试，主要原因是其作为广泛采用的模糊测试工具，对C语言实现的协议栈支持良好，且其反馈机制与AM-VarProto在技术路径上具备可比性。相较之下，Atheris则主要面向Python环境，在处理HTTP/2二进制协议结构时适配性较弱，因此，本节主要与AFL模糊测试工具进行对比，以更清晰地体现AM-VarProto在语义感知与自适应优化方面的优势。

实验结果如表5所示。在会话建立流程CreateSMContext中，致效率达64%。该流程涉及会话上下文的初始化，AM-VarProto通过字段权重自适应机制，优先扰动sNssai、dnn等必选且验证过程相对宽松的字段，从而有效提升异常触发率。在会话更新流程UpdateSMContext中，致效率为54%，相对较低，主要由于该流程中系统对字段一致性、状态依赖性的验证过程更严格，限制了部分变异样本的生效空间。在会话释放流程ReleaseSMContext中，致效率为60%，介于前两者之间。实验结果表明，AM-VarProto不仅适配HTTP/2协议架构，还能依据不同业务流程的语义特征动态聚焦高危字段，在初始化、状态更新、资源释放等不同阶段均保持较高的异常触发能力。相较之下，传统模糊测试工具AFL在3个流程中平均致效率为41%，这是由于AFL仅依赖覆盖率作为反馈信号，无法识别更易触发深层异常或服务崩溃的字段。这表明AM-VarProto在协议语义理解与自适应变异策略上具有显著优势。

表5　协议字段异常种类定义

模型	协议流程	异常次数/次	致效率
AM-VarProto	CreateSMContext	32	64%
	UpdateSMContext	27	54%
	ReleaseSMContext	30	60%
AFL	CreateSMContext	21	42%
	UpdateSMContext	23	46%
	ReleaseSMContext	18	36%

为验证变异造成信令流终止，通过tcpdump对运行过程中的信令Pcap数据包进行捕获，并与正常状态下的Pcap数据包进行对比，通过Wireshark工具对一条完整的HTTP/2协议流进行追踪，对比结果如图15所示。

对比分析结果表明，提交POST请求的路径已发生变异，当前呈现为/sm-contexts/yfpVV72yUMtc。在此情况下，SMF网元针对AMF所发起的信令流，未给出201 Create这样符合预期的正常回应。随后，通过追踪HTTP/2协议流携带的POST请求下的JSON格式数据负载，对比说明是否实现协议字段的变异，变异前后字段对比如图16所示。

图15　正常和异常信令流对比

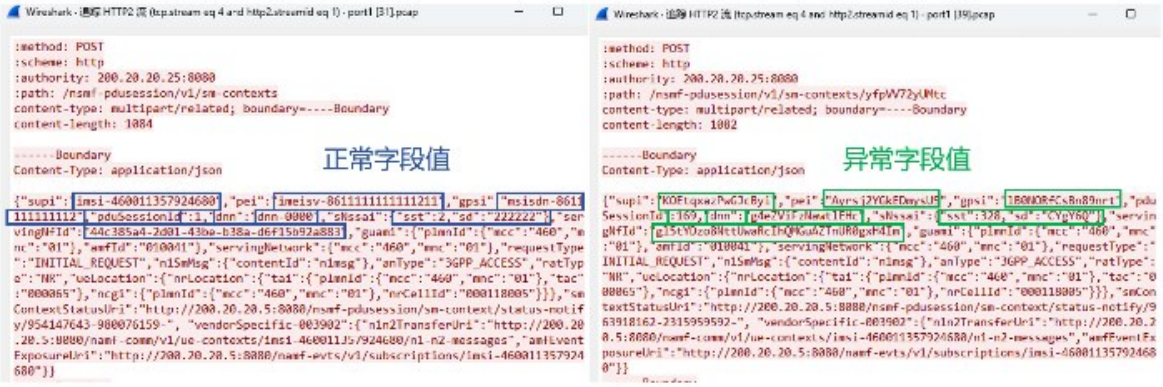


图16　变异前后字段对比

从图16中能够清晰地观察到，实验过程中设置的变异字段（如supi、pei）和会话相关的信息（如PDU、dnn、sst和sd等字段），其字段值均出现变异情况。综合考量这一系列变化，可以判定是协议层面产生异常，进而导致整个信令流程被迫终止，证明了AM-VarProto算法变异策略的有效性。

5　结束语

本文提出并系统性验证了一种基于自适应元学习的协议字段智能变异方法AM-VarProto。该方法通过对NGAP、HTTP/2等核心协议字段的语义结构与交互逻辑进行深入分析，综合字段级、字节级与比特级的多层级动态变异策略，设计了基于反馈驱动的持续优化机制。在OAI-5G、5GCore_NMP平台以及商用协议栈等仿真与真实测试环境中进行严格评估。实验结果表明，在多轮迭代后，AM-VarProto在变异覆盖率方面较AFL和Atheris均提升了19%以上，变异致效率提升了10%以上，并在资源开销与执行性能之间取得良好平衡，充分体现了其技术优势。未来，在本研究的基础上将探索元学习与强化学习相结合的方法，以有效建模协议演化过程，精准优化变异策略，进一步提升自动化变异的效率与效果。

参考文献：

[1] YU G F. A multi-objective decision method for the network security situation grade assessment under multi-source information[J]. Information Fusion, 2024, 102: 102066.

[2] DAO N N, TU N H, HOANG T D, et al. A review on new technologies in 3GPP standards for 5G access and beyond[J]. Computer Networks, 2024, 245: 110370.

[3] NING Z L, CHEN H D, NGAI E C H, et al. Lightweight imitation learning for real-time cooperative service migration[J]. IEEE Transactions on Mobile Computing, 2024, 23(2): 1503-1520.

[4] SENEVIRATHNA T, LA V H, MARCHA S, et al. A survey on XAI for 5G and beyond security: technical aspects, challenges and research directions[J]. IEEE Communications Surveys & Tutorials, 2025, 27(2): 941-973.

[5] MORADI M, LIN Y K, MAO Z M, et al. SoftBox: a customizable, low-latency, and scalable 5G core network architecture[J]. IEEE Journal on Selected Areas in Communications, 2018, 36(3): 438-456.

[6] PENG X N, WEN Y Y, ZHAO H. Security issues and solutions in 3G core network[J]. Journal of Networks, 2011, 6(5): 823-830.

[7] HUSSAIN S R, ECHEVERRIA M, CHOWDHURY O, et al. Privacy attacks to the 4G and 5G cellular paging protocols using side channel information[J]. NDSS, 2019, DOI:10.14722/ndss.2019.23442.

[8] PATIL R, TIAN Z X, GURUSAMY M, et al. 5G core network control plane: Network security challenges and solution requirements[J]. Computer Communications, 2025, 229: 107982.

[9] 宁兆龙, 张凯源, 王小洁, 等. 基于多智能体元强化学习的车联网协同

服务缓存和计算卸载[J]. 通信学报, 2021, 42(6): 118-130.
NING Z L, ZHANG K Y, WANG X J, et al. Cooperative service caching and peer offloading in Internet of vehicles based on multi-agent meta-reinforcement learning[J]. Journal on Communications, 2021, 42 (6): 118-130.

[10] 王小洁, 刘子依, 唐守泽, 等. 面向支付通道网络的多优先级资源调度算法[J]. 通信学报, 2025, 46(2): 83-96.
WANG X J, LIU Z Y, TANG S Z, et al. Multi-priority resource scheduling algorithm for payment channel networks[J]. Journal on Communications, 2025, 46(2): 83-96.

[11] ZHANG X H, ZHANG C, LI X H, et al. A survey of protocol fuzzing[J]. ACM Computing Surveys, 2025, 57(2): 1-36.

[12] VETTORUZZO A, BOUGUELIA M R, VANSCHOREN J, et al. Advances and challenges in meta-learning: a technical review[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2024, 46 (7): 4763-4779.

[13] MALLISSERY S, WU Y S. Demystify the fuzzing methods: a comprehensive survey[J]. ACM Computing Surveys, 2024, 56(3): 1-38.

[14] HE F J, YANG W C, CUI B J, et al. Intelligent fuzzing algorithm for 5G NAS protocol based on predefined rules[C]//Proceedings of the 2022 International Conference on Computer Communications and Networks (ICCCN). Piscataway: IEEE Press, 2022: 1-7.

[15] GARBELINI M E, SHANG Z W, CHATTOPADHYAY S, et al. Towards automated fuzzing of 4G/5G protocol implementations over the air[C]//Proceedings of the GLOBECOM 2022 - 2022 IEEE Global Communications Conference. Piscataway: IEEE Press, 2022: 86-92.

[16] GHEISARNEJAD M, MOHAMMADZADEH A, FARSIZADEH H, et al. Stabilization of 5G telecom converter-based deep type-3 fuzzy machine learning control for telecom applications[J]. IEEE Transactions on Circuits and Systems II: Express Briefs, 2022, 69(2): 544-548.

[17] KHAN A A, ABOLHASAN M, NI W, et al. A hybrid-fuzzy logic guided genetic algorithm (H-FLGA) approach for resource optimization in 5G VANETs[J]. IEEE Transactions on Vehicular Technology, 2019, 68(7): 6964-6974.

[18] ISTIAQUE A K, TAHIR M, LUN L S, et al. Trust-aware authentication and authorization for IoT: a federated machine learning approach[J]. IEEE Internet of Things Journal, 2025, 12(8): 9889-9904.

[19] WANG X J, WANG B B, WU Y, et al. A survey on trustworthy edge intelligence: from security and reliability to transparency and sustainability[J]. IEEE Communications Surveys & Tutorials, 2025, 27(3): 1729-1757.

[20] BENNETT N, ZHU W D, SIMON B, et al. RANsacked: a domain-informed approach for fuzzing LTE and 5G RAN-core interfaces[C]// Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security. New York: ACM Press, 2024: 2027-2041.

[21] WANYAN H X, LAI Y X, LIU J, et al. NCMFuzzer: using non-critical field mutation and test case combination to improve the efficiency of ICS protocol fuzzing[J]. Computers & Security, 2024, 141: 103811.

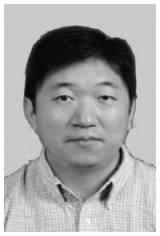
[22] HUANG L, SUN W F, YAN M, et al. Neuron semantic-guided test generation for deep neural networks fuzzing[J]. ACM Transactions on Software Engineering and Methodology, 2025, 34(1): 1-38.

[23] NIKAEIN N, MARINA M K, MANICKAM S, et al. OpenAirInterface: a flexible platform for 5G research[J]. ACM SIGCOMM Computer Communication Review, 2014, 44(5): 33-38.

[24] FIORALDI A, MANTOVANI A, MAIER D, et al. Dissecting American fuzzy lop: a FuzzBench evaluation[J]. ACM Transactions on Software Engineering and Methodology, 2023, 32(2): 1-26.

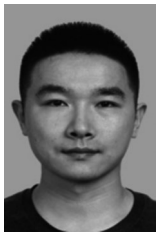
[25] SHEIKHI S, KIM E, DUGGIRALA P S, et al. Coverage-guided fuzz testing for cyber-physical systems[C]//Proceedings of the 2022 ACM/IEEE 13th International Conference on Cyber-Physical Systems (ICCPS). Piscataway: IEEE Press, 2022: 24-33.

[作者简介]



熊炫睿（1976– ），男，四川德阳人，博士，重庆邮电大学副教授，主要研究方向为人工智能应用、网络入侵检测、车联网网络安全、5G与6G网络安全。

张俊林（2000– ），男，四川巴中人，重庆邮电大学硕士生，主要研究方向为5G通信安全。



周力（1988– ），男，湖北汉川人，博士，国防科技大学副研究员，主要研究方向为无线网络、软件定义网络、异构网络。

李腾飞（1999– ），男，河南驻马店人，重庆邮电大学硕士生，主要研究方向为网络安全。

宁兆龙（1986– ），男，辽宁沈阳人，博士，重庆邮电大学教授，主要研究方向为移动边缘计算、应急网络、机器学习、资源管理。