面向5G NR L2协议安全的自动化模糊测试技术

Automated Fuzzing Technology for Security of 5G NR L2 Protocol

钟宏/ZHONG Hong[1,2]，夏云浩/XIA Yunhao[1,3]，
张金鑫/ZHANG Jinxin[1,3]，马致原/MA Zhiyuan[1,3]
（1. 移动网络和移动多媒体技术国家重点实验室，中国 深圳 518055；
2. 深圳市中兴软件有限责任公司，中国 深圳 518057；
3. 南京中兴新软件有限责任公司，中国 南京 210012）
(1. The State Key Laboratory of Mobile Network and Mobile Multimedia Technology, Shenzhen 518055;
2. Shenzhen Zhongxing Software Company Limited, Shenzhen 518057, China;
3. Nanjing Zhongxing new Software Company Limited, Nanjing 210012, China)

DOI：10.12142/ZTETJ.202406015
网络出版地址：http://kns.cnki.net/kcms/detail/34.1228.TN.20240726.1711.006.html
网络出版日期：2024-07-29
收稿日期：2024-06-15

摘要：5G协议的安全性直接影响到5G通信系统能否正常提供服务，而新空口（NR）协议是其重要组成部分，因此对5G NR协议进行安全检测具有重要意义。提出一种基于模糊测试的5G NR协议漏洞检测自动化系统，针对媒体接入控制层（MAC）、无线链路控制层（RLC）和分组数据汇聚协议层（PDCP）的L2协议，分析协议特征来设计高效的数据变异策略，提高测试用例的有效性，实现多种工作模式适配以提高漏洞挖掘效率。接着，基于5G基站和移动终端设备，开发了一套原型系统用以评估本文所提方案的性能。实验数据显示，数据包处理时间能够满足5G业务时延性能要求，同时能够发现MAC、RLC和PDCP协议的多种安全漏洞，验证了所提方案可以有效提升测试数据包的合法性和漏洞挖掘的有效性。

关键词：5G NR；网络协议；漏洞挖掘；模糊测试

Abstract: New radio (NR) is an important part of the 5G protocol, and its security directly affects whether the 5G communication system can provide services properly. Therefore, it is of great significance to perform security testing on the 5G NR protocol. In order to efficiently perform security detection on medium access control (MAC), radio link control (RLC) and packet data convergence control (PDCP) of 5G NR L2 protocol, this paper proposes an automated system based on fuzzing technology. The proposed method designs efficient data mutation strategies by analyzing protocol characteristics to improve the effectiveness of test cases, and implements multiple working modes to improve the efficiency of vulnerability detection. Furthermore, in order to evaluate the performance of the proposed method, we implement a fuzzing prototype system based on 5G gNodeB and mobile terminal, and then conduct practical security detection on 5G NR protocol. Experimental results show that packet processing time of our proposed method can meet 5G latency requirements. In addition, various vulnerabilities in MAC, RLC, and PDCP are exposed in this paper which verifies that the proposed method can effectively improve the compliance of test data and the effectiveness of vulnerability detection.

Keywords: 5G NR; network protocol; vulnerability detection; fuzzing test

引用格式：钟宏, 夏云浩, 张金鑫, 等. 面向5G NR L2协议安全的自动化模糊测试技术 [J]. 中兴通讯技术, 2024, 30(6): 100-107. DOI: 10.12142/ZTETJ.202406015
Citation：ZHONG H, XIA Y H, ZHANG J X, et al. Automated fuzzing technology for security of 5G NR L2 protocol [J]. ZTE technology journal, 2024, 30(6): 100-107. DOI: 10.12142/ZTETJ.202406015

5G通信技术具备更高速率、更大连接、更低时延等技术优势，使得5G通信网络得到大规模部署和应用，在社会生活中发挥着重要作用。5G安全将直接影响到行业安全甚至是国家安全。其中，5G协议是保证5G通信系统能够正常提供网络服务的重要组成部分，对5G协议进行安全检测和脆弱性分析具有重要意义[1]。

第3代合作伙伴计划（3GPP）安全保证规范（SCAS）[2]、通信监管部门和运营商均有5G新空口（NR）协议安全测试要求。5G NR协议安全漏洞挖掘是目前的研究

基金项目：国家自然科学基金项目（U23B2003）；广东省重点领域研发计划项目（2020B0101120003）

热点[3]。然而，由于网元数量庞大、设备源代码无法获取等，传统的白盒测试和代码审计方法在5G NR协议的安全检测中已经失效。其次，现有的5G NR协议测试是针对功能和性能的测试，而针对那些更深更广层次安全问题的技术方案仍比较缺乏[4]。此外，在5G NR协议测试中大多聚焦应用层L3协议，针对数据链路层L2协议的研究不多，测试的完整性不高[5]。因此，实现5G NR三层协议的自动化安全测试是一个急需解决的难题。

模糊测试是一种通过向目标系统提供非预期的输入并监视异常结果来发现软件漏洞的方法，能够在不了解相关源代码和逻辑流程的情况下进行黑盒测试，因此被广泛应用于网络协议和可执行文件的安全检测[6]。现有的通信网络协议模糊测试方法主要基于对3GPP技术规范的手动分析，耗时长且资源消耗高。在变异策略阶段中使用简易的变异策略来生成测试用例，例如位翻转和字节算术，无法根据数据情况动态调整变异策略，这导致测试用例的有效性较低。

目前5G NR协议模糊测试实现了无线资源控制（RRC）和非接入层（NAS）的L3协议的漏洞挖掘工作，而在MAC、RLC和PDCP的L2协议模糊测试中进展缓慢，主要存在以下问题与难点：测试需要高效算法来控制数据链路层的通信，涉及任意修改数据包字段，这对算法提出了较高的要求，需要针对数据链路层协议及数据格式等特点设计策略；在复杂的5G协议通信中，检测基站的无效或不符合规范的响应需要全面的模糊测试和验证策略；测试需要利用上下文信息，如安全配置，这只有在实时通信中才能获得，需要结合5G终端设备；需要优化模糊测试算法，以提高协议状态覆盖率和测试效率。此外，模糊测试在5G NR协议测试中遇到最大的问题是时延限制，这是因为5G数据链路层的测试需要满足低延迟要求，以确保实时通信。拦截和转发数据包的时间需要控制在有限的传输时隙内，无法满足5G业务时延性能要求将导致测试用例无法正常测试，因此需要设计特定的协议报文解析和报文处理方式。

为了解决上述问题，我们提出了一种针对5G NR L2协议安全的模糊测试系统。该系统可以根据5G NR L2协议特征设计针对性的变异策略，满足5G业务时延性能要求，提高测试用例的有效性，高效挖掘5G NR协议的安全漏洞，从而提升5G基站的健壮性和安全性。为了评估系统方案的正确性，我们设计并实现了5G NR L2协议的模糊测试原型系统，并在真实的5G gNodeB上进行了漏洞挖掘和性能评估。本研究中，我们的主要贡献总结如下：

1）提出了一种5G NR协议漏洞的自动检测框架，可以覆盖更底层的L2协议安全，实现MAC、RLC以及PDCP协议的模糊测试；

2）针对5G NR L2协议特征，设计高效的模糊测试数据变异策略，以及多种模糊测试工作模式；

3）基于真实的5G网络设备和5G基站，实现了整套原型系统，包含服务端子系统和移动终端子系统；

4）实验数据表明，我们的数据包操作的处理时间优越，能够满足5G业务时延性能要求。此外，系统能够有效检测出MAC、RLC以及PDCP协议漏洞。

1 5G模糊测试技术

在通信网络中，无线接入网络（RAN）为用户设备（UE）提供无线通信服务。RAN由无线基站组成，使用的无线接入技术称为新空口技术。5G NR协议分为3层，即物理层、数据链路层和网络层。其中，数据链路层是本文的研究重点，对应MAC、RLC和PDCP，主要功能是信道复用和解复用、数据格式的封装、数据包调度等。完成的主要功能是具有个性的业务数据向没有个性的通用数据帧的转换。

随着5G移动通信网络的大规模部署和应用，5G移动通信领域出现了一波安全研究浪潮。在过去几年中，研究人员发现3GPP规范中存在许多设计缺陷[7–8]和协议漏洞[9–11]。如3GPP技术规范33.501中所述，大量预认证消息通过未加密的格式发送，可被用来发起拒绝服务（DoS）攻击，并获取5G中移动用户的位置或其他敏感信息[4]。LIU等在文献[12]中针对5G网络新协议——扩展认证协议–认证和密钥协商算法（EAP–AKA），提出一种基于Lowe分类法的安全性分析模型。HUSSAIN等在文献[13]中通过对5G协议栈进行建模并使用验证工具来发现协议中的设计缺陷，但是这种方法并不针对5G UE实际实现中的漏洞。HU等在文献[14]中通过分析5G核心网下一代应用协议（NGAP），研究其协议格式，提出一种基于分区权重表的选择变异模糊测试算法。WANG等在文献[15]中提出一种面向5G专网鉴权协议——扩展认证协议–传输层安全协议（EAP–TLS）的细粒度形式化建模与验证方案并验证了保密性、认证性、隐私性3类安全属性。POTNURU等在文献[16]中提出了一种针对RRC和NAS协议的模糊测试工具，生成包含所有可能标识符的模糊测试用例，并发现了srsLTE和openLTE两个开源电信项目中的新漏洞。YANG等在文献[17]中提出了一种结合机器学习算法的RRC协议模糊测试系统，在无需事先了解协议实现的情况下捕获和解释数据包，通过自动生成全面的用例集来检测协议漏洞。HE等在文献[18]中提出了一种基于预定义规则的5G NAS协议智能模糊测试算法，通过对NAS协议分析设计动态变异策略，并在开源仿真环境OAI中验证了所提算法在

覆盖率和测试用例上具有较好的功能。WANG等在文献[19]中实现了基于模糊测试的5G RRC协议漏洞检测模型，发现了UE和gNodeB的若干漏洞，最后给出了几项增强5G安全性的对策。目前大多数研究集中在5G NR L3协议，即RRC和NAS，而针对更底层的L2协议如MAC、RLC和PDCP的安全测试深度不够且较片面。主要原因在于，更底层协议的安全检测对模糊测试系统和算法的设计提出了较高的标准要求，需要满足5G业务更严苛的性能需求。为了解决上述问题，我们提出一种适配5G NR L2协议安全的自动检测框架，针对协议特征设计高效的变异策略和测试用例，能够更好地对NR协议进行模糊测试，并在真实的5G网络设备和5G基站中实现了整套原型系统，通过实验测试和性能评估验证本文所提方案的有效性。

2 方案设计

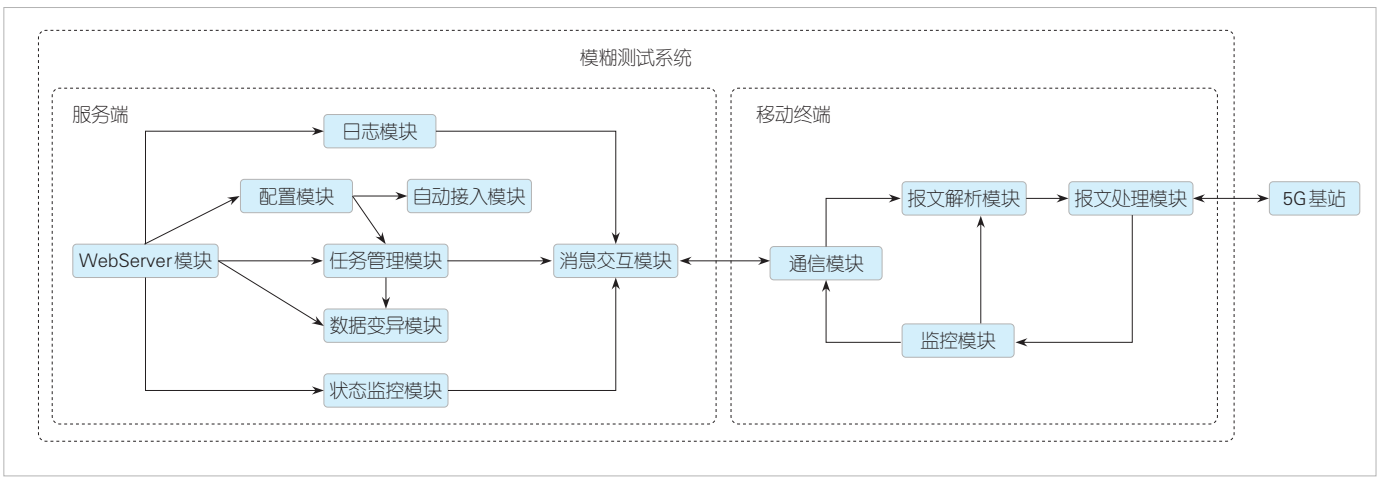
2.1 方案概述

本文提出的基于模糊测试的5G NR协议漏洞挖掘系统架构如图1所示，包括服务端和移动终端。服务端运行在高性能计算机上并提供模糊测试的主要功能，包括数据变异模块、任务管理模块、配置模块、状态监控模块、日志模块、自动接入模块、消息交互模块、Webserver模块，主要提供5G NR协议配置树生成和管理、5G NR协议数据变异、测试任务管理和下发、状态接收处理等功能。其中，数据变异模块和任务管理模块中涉及本文所提方案的关键技术，将在后文详细描述，而其他模块功能只是配合系统整体实现，这里不做赘述。移动终端基于5G通信设备定制化开发功能模块辅助模糊测试，包括报文通信模块、解析模块、报文处理模块、监控模块，主要提供状态监控、共享内存管理、变异数据转发、报文字段解析及变异数据配置等功能。其中，报文解析模块和报文处理模块中涉及本文所提方案的关键技术，也将在后文中详细描述，而其他模块功能只是配合系统整体实现，将不做过多描述。

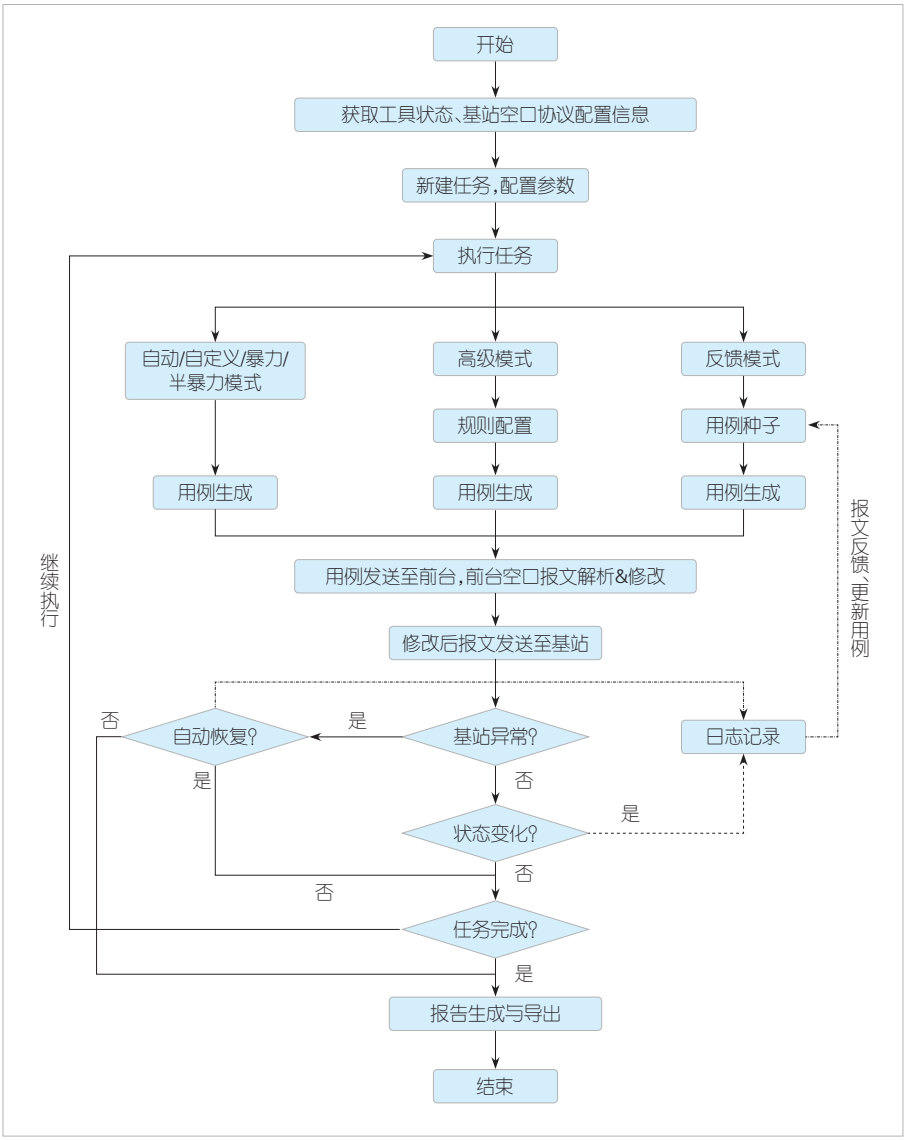
系统开始运行后，首先从5G基站网管系统获取基站空口协议的配置信息。服务端根据基站空口协议配置的协议字段生成5G空口协议配置树（含协议字段名称、类型、长度等），并使用智能变异器对5G空口协议数据进行变异，然后使用服务端转发模块将变异后的配置树数据发送给移动终端。移动终端通信模块接收到变异后的配置树数据后写入共享内存，其中变异数据存储在设备的内存中，报文解析和处理在上层进行，因此需要采用共享内存进行通信。根据获取到的5G基站配置信息，用户在服务端人机交互界面配置将要模糊测试的协议字段。服务端将模糊测试的协议字段配置发送至移动终端。移动终端根据用户配置的协议字段匹配适合的变异配置树数据。移动终端报文解析模块解析MAC层出口的协议数据流，确认协议字段在报文中的确切位置。报文处理模块由共享内存读取变异数据，将变异数据写入对应协议字段位置的数据流，再由物理层处理后经移动终端射频天线发送至5G基站。5G基站收到报文后作出响应。移动终端的监控模块会实时监控5G基站的响应状态，若5G基站业务流程异常，则返回异常状态。监控模块会修改共享内存中的模糊测试状态标志位，将异常状态和导致异常的数据报文记录到日志中，同时将其回传给服务端任务管理模块存储。模糊测试系统工作流程如图2所示。

2.2 服务端

数据变异模块：负责生成针对性的变异测试数据。服务端分析5G NR L2协议特征和业务特征，结合当前基站的协



▲图1 模糊测试系统框架



▲图2　模糊测试系统工作流程

议配置生成数据模型，然后采用多种算法生成变异数据用于测试。该数据变异算法主要依托于对现有5G NR L2协议各字段特性的研究，同时考虑自动化变异算法的效率和可行性的动态平衡。

我们首先分析5G NR L2协议（PDCP/RLC/MAC）具有的特征。5G NR特征主要包括协议特征和业务特征。协议特征如MAC层协议有MAC控制元素（MAC CE）和填充（PADING）两种类型。RLC层协议具有透明模式（TM）、非确认模式（UM）和确认模式（AM）3种不同的工作模式。PDCP层协议有信令无线承载（SRB）和数据无线承载（DRB）两种类型。业务特征则是各协议层在业务上所发挥的作用，例如小区搜索、系统消息、寻呼、测量、随机接入等。接着根据基站的5G NR协议配置选择对应的业务场景数据模型，结合协议特征和业务特征生成应对不同业务场景的5G NR协议数据模型，如小区搜索模型、随机接入模型。

在模糊测试的生成变异测试数据阶段，采用多协议字段同时变异、无序变异和反馈变异等方式生成新的测试数据，如图3所示。多协议字段同时变异的方法可以极大提升用例覆盖率。无序变异的方式通过设置变异规则可实现重放、顺序、倒序用例测试。反馈变异的方法通过针对报文进行监控、记录、分析，利用行为学习与反馈算法提升测试用例的有效性。系统采用的数据变异算法能够自动逐步提高测试用例覆盖率和有效性，进而发现深层次的问题。

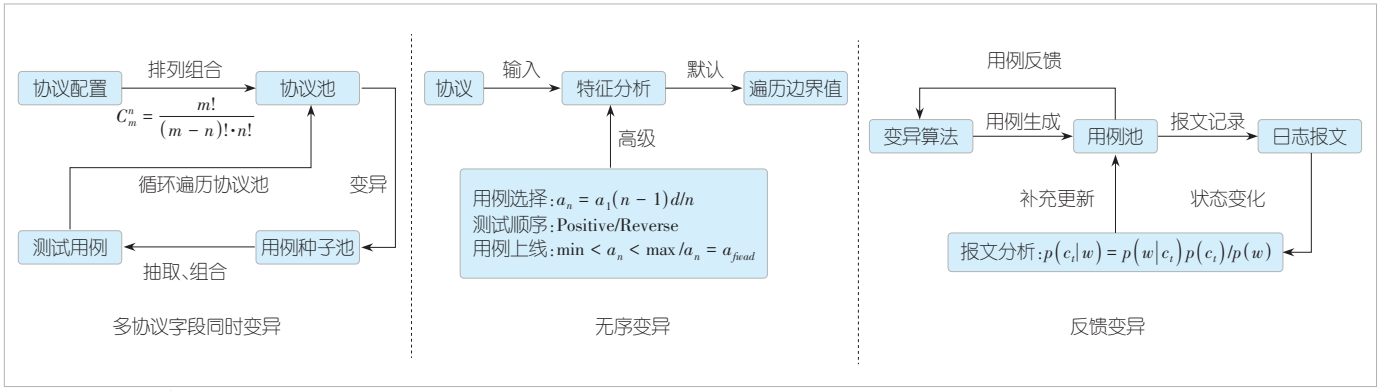
任务管理模块：负责模糊测试任务下发及任务管理功能。测试任务支持自动模式、自定义模式、半暴力模式、暴力模式、反馈模式和高级模式等场景测试。各工作模式特性对比如表1所示。

任务管理模块支持报告查看功能。报告中展示测试的配置及协议组测试结果的详细情况。此外，任务管理还提供模糊测试复测功能，根据需求进行安全漏洞复测，便于开发人员进行漏洞修复。以发现5G基站下行失步漏洞为例，系统发现该漏洞后会存储此时模糊测试使用的业务场景配置、5G NR协议数据模型生成的变异数据以及测试用例。若需要进行漏洞复测，则可以在系统触发任务管理的模糊测试复测功能，系统会使用发现漏洞时存储的信息，按照发现漏洞的流程再次进行模糊测试，进而完成安全漏洞复现。

2.3 移动终端

报文解析模块：负责对5G NR协议报文进行解析。移动终端接入5G基站做数据业务，解析模块按照标准协议报文格式将移动终端5G NR协议组包后的业务报文进行解析，识别出协议层、协议字段及协议字段属性。

系统主要参考3GPP协议格式完成业务报文解析，从移动终端接口获取5G NR协议业务报文，经报文解析后能够识别出协议层如MAC、RLC等，协议字段如逻辑信道标识符（LCID）、序列指示符（SI）、序列号（SN）等，及协议字段



▲图3　数据变异方式

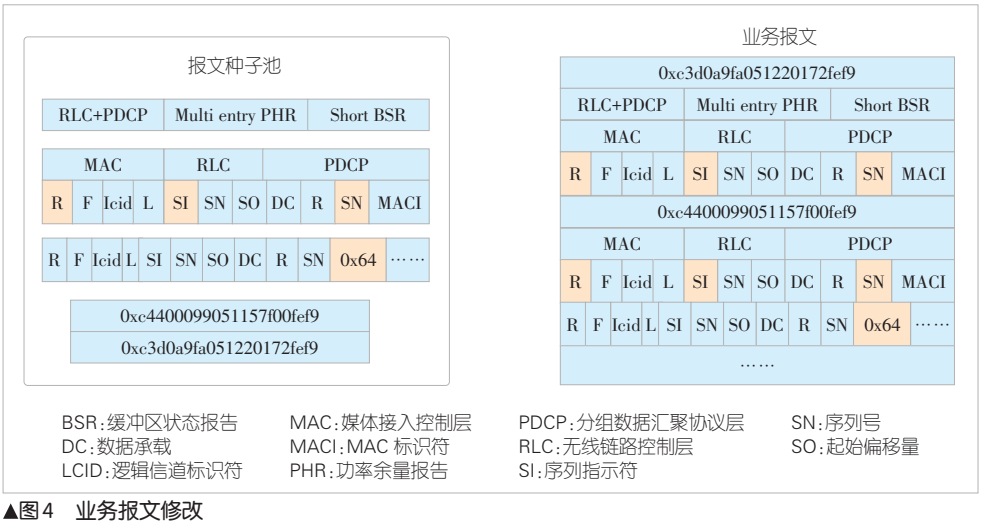
▼表1　各工作模式特性对比

模式	测试粒度	生成方式	特点
自动模式	协议字段	基于突变	持续化，协议字段随机排列组合用例测试
自定义模式	协议字段	基于突变	协议字段指定组合精准测试
半暴力模式	协议组	基于生成	协议组字段变异，粗粒度测试
暴力模式	比特流	基于突变	完全随机化测试
高级模式	协议字段	基于生成	手动针对协议字段设置用例，精细化测试
反馈模式	报文、数据服务单元	基于反馈演进	依据信令变化反馈测试，形成测试闭环

属性如Length等。

报文处理模块：获取根据5G NR协议数据模型自动生成的变异数据，并据此对发送给基站的报文进行修改，经射频天线发给5G基站。变异业务报文数据由报文头和变异数据组成，其中报文头可根据需求定制。

报文处理模块首先从共享内存中获取变异数据，接着根据服务端的模糊测试任务配置完成5G NR协议报文修改。其中，获取和修改5G NR协议报文要满足5G NR协议时延要求。业务调度按照原有的时间窗将修改后的业务报文经物理层及射频天线发送给5G基站。采用字符串匹配算法修改5G NR协议报文，可使获取和修改5G NR协议报文耗时不超出业务调度的时间范围。以反馈变异为例，获取业务报文码流经变异后存储至报文种子池，进而以报文种子池中的报文修改业务报文，完成报文修改。以反馈模式中业务报文一个TB块的若干服务数据单元（SDU）格式修改方法如图4所示。



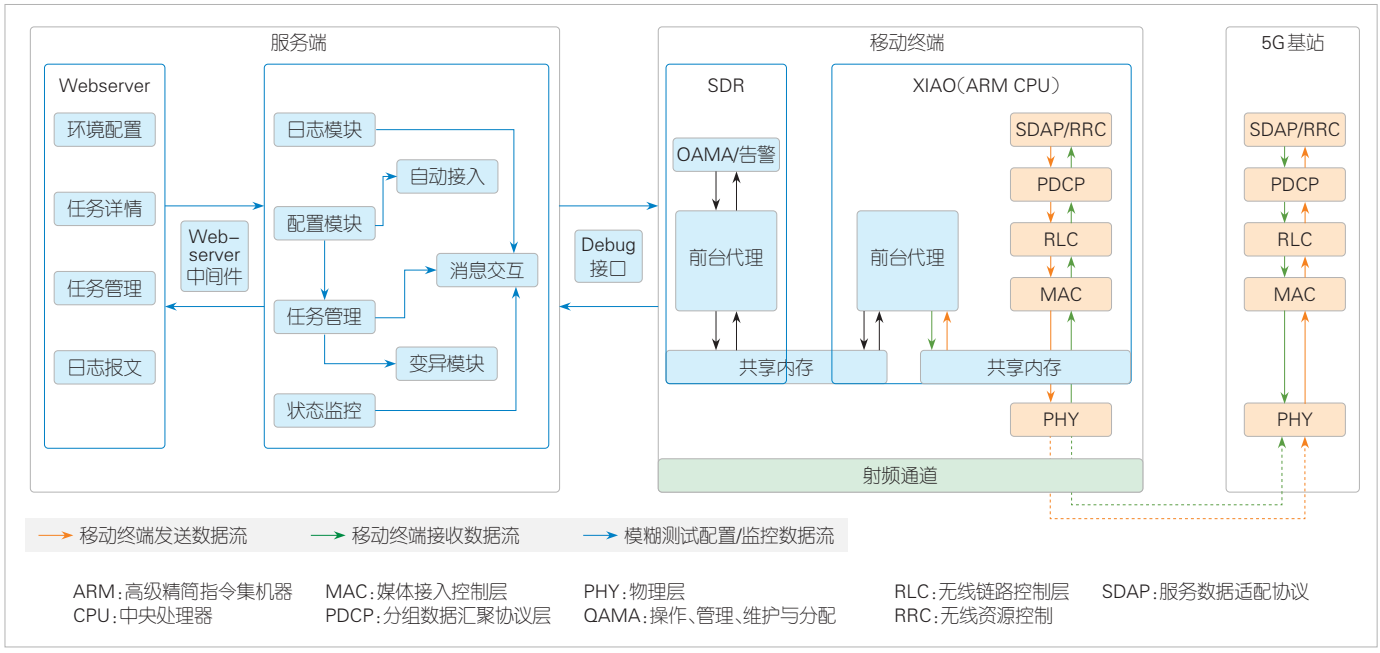
▲图4　业务报文修改

3 实验评估

3.1 实验环境

为了评估本文设计的解决方案，本章节中我们搭建实际的测试平台。测试实验的5G NR协议模糊测试系统架构如图5所示。服务端使用Python语言开发，运行在高性能计算机上，通过网口与移动终端Debug口连接。移动终端的硬件平台基于5G CPE设备深度定制开发，包含两大Linux子系统，分别是SDR系统和XIAO系统。移动终端主要完成SDR、XIAO系统的调度及消息交互。SDR系统主要完成5G NR协议业务流程，包括模糊测试变异数据存储、模糊测试测试控制信息的转发及模糊测试状态的获取及回传等；XIAO系统主要完成5G NR协议的实现，包括NR协议数据解析、NR协议数据处理、模糊测试场景判断及变异数据修改等功能。

5G模糊测试移动终端是基于5G设备开发的，因此在图



▲图5　基于5G设备的模糊测试系统架构

1的移动终端中主要展示模糊测试定制功能模块，移动终端固有支持功能未提及，而图5中移动终端是按照功能模块具体技术实现展示的，包括系统组成、数据流向及通信方式等，其中系统组成包括SDR子系统、XIAO子系统及射频通道。通信模块主要采用核间共享内存通信技术完成模糊测试配置和变异数据传输。监控模块对应操作、管理、维护与分配（OAMA）和告警功能通过该模块获取目标基站的状态信息。报文解析和处理模块均由XIAO系统的前台代理实现。SDR子系统的前台代理完成数据中转及目标状态实时反馈至用户界面。图5中红色箭头代表移动终端发送数据报文到5G基站的数据流向，绿色箭头代表移动终端接收5G基站响应数据报文的数据流向，蓝色箭头代表模糊测试系统配置及监控的数据流向。

测试实验主要工作流程为：服务端根据指定的5G NR协议字段生成协议配置树，并使用变异策略对5G NR协议数据进行变异，然后将协议配置树和变异数据发送给移动终端。5G模糊测试移动终端首先通过SDR子系统接收配置树，并读取变异数据，再将配置树和变异数据写入共享内存。然后，XIAO子系统从共享内存中读取配置树后，解析MAC层出口的协议数据流，读取共享内存的变异数据，将变异数据写入对应协议字段位置的数据流中。数据在PHY层处理后经5G模糊测试终端空口发送至gNodeB。gNodeB收到报文后进行响应。若gNodeB业务流程异常，则返回异常状态。移动终端监控到异常状态后，修改片内共享内存中的模糊测试状态标志位，将异常状态和导致异常的数据报文记录到日志中，同时将其回传给后台监控服务。

3.2 性能评估

我们通过验证模糊测试中解析修改MAC、RLC、PDCP层数据包所消耗的时间来衡量系统性能，并通过详尽枚举协议的模式、类型、SN长度来展示测试的完整性。模糊测试耗时测试分为修改1个TB块的1个SDU和11个SDU数据两种场景。修改1个TB块的若干个SDU数据可根据需求由程序控制。耗时测量结果如表2所示。总体而言，设计方案的5G数据包处理时间远远低于5G业务数据报文一次调度最大时延为200 μs的性能要求。以最复杂的PDCP协议DRB 18 bit SN场景下修改1个TB块的11个SDU为例，测试所使用的时间是4.293 μs，即1个TB块若有1 000个SDU，则在该场景下最多能够修改368个SDU数据，处理能力远高于gNodeB业务需求。

在漏洞挖掘方面，我们首先罗列了MAC、RLC、PDCP的32个代表性协议字段，然后针对性地对每个字段进行了模糊测试，如表3所示。通过我们方案设计的变异策略，如多协议字段同时变异、无序变异和反馈变异等方式，生成畸形的数据包被注入系统，以监测是否发生崩溃，从而进行进一步漏洞挖掘。5G基站上各协议字段的模糊测试结果如表3所示。基站在收到无效的MAC“mac-nr.dlsch.lcid”和RLC“rlc-nr.am.dc”字段后发生了崩溃（gNB Crashed）。此外，由于PDCP字段“pdcp-nr.srb.maci”格式错误，被测试设备

▼表2 NR协议模糊测试测试场景验证结果

协议	模式	类型	SN长度/bit	Fuzz耗时/μs（1个SDU）	Fuzz耗时/μs（11个SDU）
MAC	--	MACCE	--	1.813	4.238
		填充	--	1.634	4.026
RLC	AM	CTRL	无SN	0.407	3.719
		DATA	12	0.509	4.127
			18	0.516	4.266
	UM	分片	6	0.486	4.069
			12	0.506	4.137
		不分片	无SN	0.369	3.649
PDCP	--	SRB	12	0.477	3.817
	--	DRB	12	0.514	4.201
			18	0.514	4.293

AM：确认模式　MAC：媒体接入控制层　SDU：服务数据单元
CTRL：控制信息　MACCE：MAC控制元素　SN：序列号
DATA：用户数据　PDCP：分组数据汇聚协议层　SRB：信令无线承载
DRB：数据无线承载　RLC：无线链路控制层　UM：非确认模式

在一次实例中也发生了崩溃（gNB Crashed）。因此，基站gNodeB容易受到MAC、RLC、PDCP层的DoS攻击。除了崩溃，在测试MAC的“mace-nr. shortBSR. buffersize”和“mace-nr.longBSR.lcg”字段时，用户设备发生了重连（UE Reconnect）和断连（UE cannot Reconnect），从而导致数据传输的延迟增加，以及额外的网络资源和设备资源消耗。此外，设备在重连过程中可能会受到恶意攻击，导致用户数据的泄露或设备被攻击。更严重的是，在测试PDCP“pdcp-nr.drb.reserved”时触发断链（Broken Chain），可能导致数据丢失或损坏，以及生产流程中断或事故等。

4 总结与展望

本文中我们提出了一套主要实现5G NR L2协议的模糊测试解决方案。整套系统主要包含数据变异的服务端子系统和数据处理的移动终端子系统，解决MAC、RLC以及PDCP协议安全漏洞自动化挖掘的难点。针对协议特征采用多协议字段同时变异、无序变异和反馈变异等方式生成高效测试用例，我们定义基于突变、基于生成和基于反馈演进多种工作模式进行5G NR协议安全测试，最后将模糊测试技术融入移动终端设备，结合5G基站设计并实现实验评估系统，验证了本文所设计方案的数据包解析处理性能优越。结果表明，所提方案能够有效解决5G测试数据的时延挑战，有效发现5G NR L2协议中的安全缺陷。与现有技术相比，该方案弥补了5G NR L2协议模糊测试技术的不足，促进了5G NR协议安全漏洞挖掘有效性的进步，提升了5G基站的健壮性和安全性。

未来，我们计划继续改进本文所提模糊测试算法，融入机器学习算法指导数据变异，提高测试用例的有效性。此外，我们将设计包括L3协议即RRC和NAS的安全测试，实现一个覆盖5G NR三层协议的模糊测试系统。

▼表3 5G基站上各协议字段的模糊测试结果

协议	协议字段	是否检测	问题
PDCP	pdcp-nr.srb.reserved	√	
PDCP	pdcp-nr.srb.sn	√	
PDCP	pdcp-nr.srb.direction	√	
PDCP	pdcp-nr.srb.maci	√	gNB Crashed
PDCP	pdcp-nr.drb.reserved	√	Broken Chain
PDCP	pdcp-nr.drb.sn	√	
PDCP	pdcp-nr.drb.direction	√	
PDCP	pdcp-nr.drb.maci	√	
RLC	rlc-nr.am.dc	√	gNB Crashed
RLC	rlc-nr.am.p	√	
RLC	rlc-nr.am.si	√	
RLC	rlc-nr.am.so	√	
RLC	rlc-nr.am.reserved	√	
RLC	rlc-nr.am.dc	√	
RLC	rlc-nr.um.p	√	
RLC	rlc-nr.um.si	√	
RLC	rlc-nr.um.so	√	
RLC	rlc-nr.seqnum.length	×	
RLC	mac-nr.reserved	√	
MAC	mac-nr.dlsch.flag	√	
MAC	mac-nr.dlsch.lcid	√	gNB Crashed
MAC	mac-nr.subheader.sdu-length	×	
MAC	mace-nr.crnti.crnti	√	
MAC	mace-nr.longBSR.buffersize	√	
MAC	mace-nr.longBSR.lcg	√	UE cannot Reconnect
MAC	mace-nr.shortBSR.buffersize	√	UE Reconnect
MAC	mace-nr.shortBSR.lcgid	√	
MAC	mace-nr.single-entry-phr.ph	√	
MAC	mace-nr.single-entry-phr.pcmax	√	
MAC	mace-nr.pre-emptiveBSR.lcg	√	
MAC	mace-nr.pre-emptiveBSR.buffersize	√	
MAC	mace-nr.scell-bfr.ac	√	

MAC：媒体接入控制层　RLC：无线链路控制层
PDCP：分组数据汇聚协议层　UE：用户设备

参考文献

[1] BITSIKAS E, KHANDKER S, SALOUS A, et al. UE security reloaded: developing a 5G standalone user-side security testing framework [C]//Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks. ACM,

2023: 121–132. DOI: 10.1145/3558482.3590194
[2] 王航, 毛俊, 陈利伟. 5G系统安全测试与自动化 [J]. 信息安全与通信保密, 2023, 21(2): 56–70. DOI: 10.3969/j. issn. 1009–8054.2023.02.006
[3] KHAN J A, CHOWDHURY M M. Security analysis of 5G network [C]//Proceedings of IEEE International Conference on Electro Information Technology (EIT). IEEE, 2021: 1–6. DOI: 10.1109/EIT51626.2021.9491923
[4] PIQUERAS JOVER R, MAROJEVIC V. Security and protocol exploit analysis of the 5G specifications [J]. IEEE access, 2019, 7: 24956–24963. DOI: 10.1109/ACCESS.2019.2899254
[5] SULLIVAN S, BRIGHENTE A, KUMAR S A P, et al. 5G security challenges and solutions: a review by OSI layers [J]. IEEE access, 2021, 9: 116294–116314. DOI: 10.1109/ACCESS.2021.3105396
[6] MAYHEW S R. Fuzz testing architecture used for vulnerability detection in wireless systems [EB/OL]. (2022–05–05) [2024–10–25]. https://vtechworks. lib. vt. edu/server/api/core/bitstreams/3be5d061–041e–48da–81e0–e54c45cde529/content
[7] LANOUE M J, MICHAEL J B, BOLLMANN C A. Spoofed networks: exploitation of GNSS security vulnerability in 4G and 5G mobile networks [C]//Proceedings of International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS). IEEE, 2021: 1–8
[8] RAMEZANPOUR K, JAGANNATH J, JAGANNATH A. Security and privacy vulnerabilities of 5G/6G and WiFi 6: survey and research directions from a coexistence perspective [J]. Computer networks, 2023, 221: 109515. DOI: 10.1016/j. comnet.2022.109515
[9] MISHRA S. Cyber–security threats and vulnerabilities in 4G/5G network enabled systems [J]. International journal of computational science and engineering, 2022, 25(5): 548–561. DOI: 10.1504/ijcse.2022.126259
[10] HUSSAIN S R, CHOWDHURY O, MEHNAZ S, et al. LTEInspector: a systematic approach for adversarial testing of 4G LTE [C]//Proceedings 2018 Network and Distributed System Security Symposium. Internet Society, 2018. DOI: 10.14722/ndss.2018.23313
[11] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: a survey on prospective technologies and challenges [J]. IEEE communications surveys & tutorials, 2021, 23(4): 2384–2428. DOI: 10.1109/COMST.2021.3108618
[12] 刘彩霞, 胡鑫鑫, 刘树新, 等. 基于Lowe分类法的5G网络EAP–AKA'协议安全性分析 [J]. 电子与信息学报, 2019, 41(8): 1800–1807. DOI: 10.11999/JEIT190063
[13] HUSSAIN S R, ECHEVERRIA M, KARIM I, et al. 5GReasoner [C]//Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2019: 669–684. DOI: 10.1145/3319535.3354263
[14] HU Y, YANG W C, CUI B J, et al. Fuzzing method based on selection mutation of partition weight table for 5G core network NGAP protocol [M]//Innovative mobile and internet services in ubiquitous computing. Cham: Springer International Publishing, 2021: 144–155. DOI: 10.1007/978–3–030–79728–7_15
[15] 王跃东, 熊焰, 黄文超, 等. 一种面向5G专网鉴权协议的形式化分析方案 [J]. 信息网络安全, 2021(9): 1–7. DOI: 10.3969/j.issn.1671–1122.2021.09.001
[16] POTNURU S, NAKARMI P K. Berserker: ASN.1–based fuzzing of radio resource control protocol for 4G and 5G [C]//Proceedings of 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob). IEEE, 2021: 295–300. DOI: 10.1109/wimob52687.2021.9606317
[17] YANG J D, WANG Y, TRAN T X, et al. 5G RRC protocol and stack vulnerabilities detection via listen–and–learn [C]//Proceedings of IEEE 20th Consumer Communications & Networking Conference (CCNC). IEEE, 2023: 236–241. DOI: 10.1109/CCNC51644.2023.10059624
[18] 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 International Conference on Computer Communications and Networks (ICCCN). IEEE, 2022: 1–7. DOI: 10.1109/ICCCN54977.2022.9868872
[19] WANG H X, CUI B J, YANG W C, et al. An automated vulnerability detection method for the 5G RRC protocol based on fuzzing [C]//Proceedings of 4th International Conference on Advances in Computer Technology, Information Science and Communications (CTISC). IEEE, 2022: 1–7. DOI: 10.1109/CTISC54888.2022.9849690

作 者 简 介

钟宏，中兴通讯股份有限公司首席安全官、技术专家委员会常委；研究方向为网络安全、数据保护、系统安全、人工智能安全等；曾主持或参与多项国家科技重大专项课题，获多项省部级科技奖励。

夏云浩，中兴通讯股份有限公司网络安全工程师；主要研究领域为安全测评、网络安全等。

张金鑫，中兴通讯股份有限公司网络安全专家，高级工程师；主要研究领域为安全攻防、渗透测试、移动通信安全等。

马致原，中兴通讯股份有限公司资深网络安全工程师；主要研究领域为网络安全、虚拟化安全等。