5G 安全测试解决方案

需求分析

当前我国 5G 网络建设步伐加快，已建成 5G 基站近 85 万个，形成全球最大 5G 独立组网网络，5G 行业应用创新案例已超过 1 万个。一方面，5G 延续 2/3/4G 移动通信网络特征，继承 4G 网络分层分域安全架构并在服务域安全、统一认证框架、隐私保护和网间漫游安全等方面具备了比 4G 更强的安全能力；另一方面，由于 5G 引入网络功能虚拟化、网络切片、边缘计算等新技术以及增强移动宽带（eMBB）、超高可靠低时延（uRLLC）和海量机器类通信（mMTC）典型场景，网络架构向云网融合、云边协同演进，给网络建设运行和业务应用带来新的安全风险挑战。特别是 5G 的核心网架构和 4G 相比由于引入了更灵活的部署方式和切片方案，包括 UPF 下沉部署，大量专网复用运营商核心网，导致安全威胁远远大于 4G 核心网。

由于 5G 承载的业务类型更加偏向于关键商业应用，包括工控业务，轨道交通通信，电网通信等，一旦发生安全问题，其危害远远大于普通的消费者通信业务。有可能引发的是关键基础设施的安全威胁或者业务瘫痪的风险。总体来看，5G 安全的风险带来的危害因为其应用场景不同，远远大于 4G 时代。近期在国内相关的 5G 专网用户组织的 5G 安全测试中，也暴露了非常多的 5G 安全漏洞，很多漏洞具有高危特性。

典型的 5G 行业专网用户由于需要复用运营商的 5G 基础设施，因此对 5G 切片的安全性，5G 核心网/MEC 设备本身的协议健壮性，5G 基站的空口安全都有非常明确的技术要求，但是这些安全需求的测试与验证目前仍受限于测试工具，无法进行完整有效的测试，大量 5G 安全相关的测试还是用普通 5G 商用手机作为测试终端进行，无法真正有效验证 5G 设备/网络的安全性。3GPP 规范中对 5G 安全的测试规范目前也处于一个概括描述，没有细化的阶段。因此需要开发真正能对 5G 网络进行安全测试的测试工具及相关攻防平台。

解决方案

5G 安全测试解决方案可分为 5G 信令风暴安全测试方案和 5G 信令模糊测试方案。

5G 信令风暴测试的背景介绍：

信令风暴是自无线移动互联网络建立以来长期伴随和困扰运营商的最重要的网络安全问题之一。在移动互联网时代，由于智能终端用户数量和移动应用种类的爆发增长及移动应用的新特性等，移动通信网络很容易受到由控制面超载的流量模式引起的信令攻击和信令风暴的危害，使得网络收到的终端信令请求超过了网络各项信令资源的处理能力，引发网络拥塞以至于产生雪崩效应，从而导致网络的不可用。

信令攻击和信令风暴都是由一定的流量模式引起的，该流量模式可以通过生成少量经过精心计的用户面流量即可在移动网络控制面中生成过多的信令，而无需修改或破坏移动网络设备基站侧或核心网络侧的协议栈。信令攻击主要是由故意和恶意的攻击行为而形成，而信令风暴主要是由于设计不当或行为不当的移动应用程序，频繁建立和断开数据连接但仅传输少量数据以及非正常的消息和流程所致。

信令风暴对运营商网络的影响和危害，轻可引起部分网络故障或重则导致全网的瘫痪不可用，并且信令风暴具有一般数据业务下触发的条件和意义，相比信令攻击产生范围更加普遍并且危害更加深远。虽然自 4G 网络技术诞生发展以来，无线网络与核心网络性能得到不断提升，终端应用程序得到不断优化，使信令风暴的危害程度明显降低，但即使到了 5G 时代，影响和形成信令风暴的客观因素仍然存在，并且 5G 网络的架构和协议特征又给信令风暴的形成带来更多的变数，尤其是随着 5G 网络的建设发展和 5G 移动用户数量的持续增长，5G 信令风暴问题已不容忽视或迫在眉睫，研究 5G 信令风暴的特征和测试技术、建立行之有效的 5G 信令风暴试方案有着重大的意义和价值。

5G 信令风暴测试的条件与特征：

5G 信令风暴的客观潜在因素有：5G 终端的销售数量与 5G 各种在线业务（教育、会议、购物等）及金融与远程医疗等业务数据量呈显著增长趋势、软硬件和信令面/用户面接口解耦技术促进了垂直行业应用的迅速拓展和运营商的技术与市场转型以及 5G 网络和应用促进了终端种类、业务类型和需求更加多元化。

5G 信令风暴的业务沿袭因素有：

- 移动互联网业务中大规模小流量的应用程序形成的业务组合类型，小流量的应用程序会频繁地断开和重连网络，是移动网络信令风暴发生的主要原因；
- 移动互联网业务中终端的应用程序为保持永远在线的状态，定期地向网络发起心跳消息，心跳消息发送间隔的设置不当将会直接引起移动网络的信令风暴；
- 移动互联网业务中终端为节省电源产生的自动睡眠功能，也会引起网络数据的频繁断开与重连；
- 网络内切换与网际切换带来的大量认证消息负载。

5G 网络架构与协议特征带来的信令风暴新痛点：

- 5G RAN 的 CU-DU 相分离以及多种切分与接口方式，带来网元信令在 CU 单元部分更加集中，造成基带资源的进一步紧张与处理压力；
- 相比于 3/4G，5G 为了进一步提升系统的安全性，在各个环节进行了安全层面的加固，例如为克服 2G/3G/4G 网络空口用户身份信息和用户数据的泄密问题，5G 升级了强度更高的加密/鉴权算法，引入加密的用户身份信息和用户面数据完整性保护措施，更复杂的认证流程等，在带来更高安全性的同时，基站核心网计算量和算法复杂性显著提升、对计算/存储资源的消耗也更高，5G 认证过程的复杂性导致网络由初始认证、切换认证以及跨网络漫游认证所形成的信令负载将会超过 3G 与 4G 网络；
- 5G 为适应大规模机器互联应用场景引入的新 RRC 不活跃态即 RRC INACTIVE，虽然可减轻频繁的 service request 消息造成的信令负担，但其状态的引入需要额外的资源用以保留临时上下文，将占据和保持一定大小的基站资源，如果不活跃态计时器设置不当，大量无业务终端的资源得不到及时释放或由于软件设计的不当而永久不释放，可对其他正常终端业务的接入与响应产生处理延时的影响甚至拒绝服务，严重情况下可形成新的信令风暴点；
- 存在 DC 连接和更多的 Inter-RAT 可能，NSA/SA 双链接以及 3G/4G 切换带来更多的消息交互，需要确保 5G 网络在各种极端情况下提供持续、稳定、可靠的服务，高可靠的信令风暴模拟仿真测试尤为重要。

5G 接入网信令风暴潜在因素：

- 5G NR 引入了新的 RRC 非活跃状态，RRC 状态由 4G 的 2 种增加到 3 种，即：NR-RRC 已连接/NR-RRC 非活跃/NR-RRC 空闲，对应的状态管理计时器为 T380，总计时器数增多；
- 3 种 RRC 连接状态的保持与状态间频繁切换与新连接建立申请同时发生将是造成 5G 无线接入网信令风暴的隐患。

5G 核心网信令风暴潜在因素：

- 5G 无线接入网产生的信令风暴可直接形成对 5G 核心网 N1N2 接口的信令冲击；
- 来自网络侧的大量业务请求对 5G 核心网产生的信令风暴对终端业务产生影响。

5G 信令风暴测试的方法与方案：

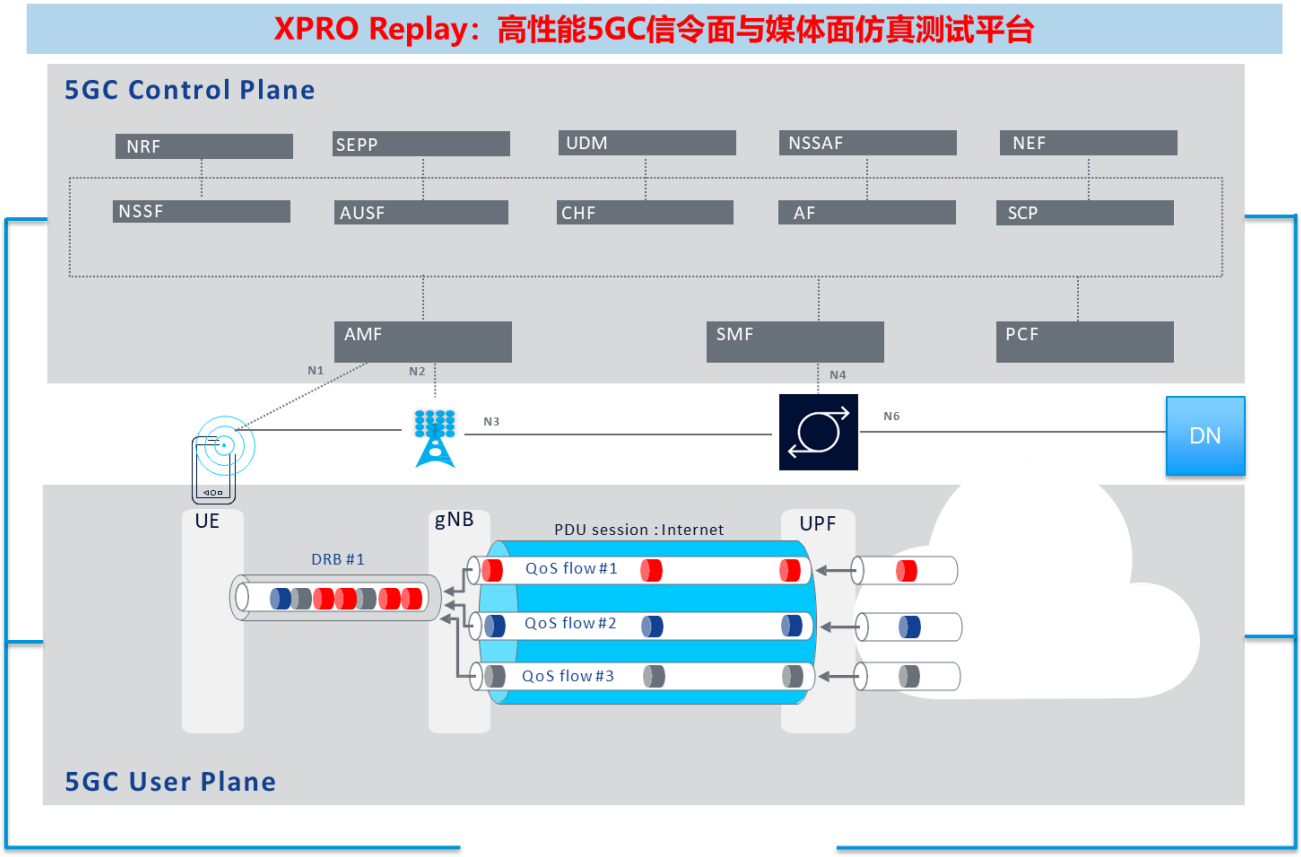
5G 信令风暴的一般测试方法：

基于容易产生信令风暴的场景和一定的移动业务组合模型，针对 5G 网络条件下的信令风暴特征，使用 5G 核心网仿真测试仪和终端仿真测试仪对 5G 基站设备与核心网网元进行包围测试，通过一定的业务模型和信令流量变化的仿真来构造基站和核心网信令风暴的形成，以检验 5G 基站设备和核心网设备在设计和使用上的安全性与健壮性，测试可通过从核心网仿真测试仪和终端仿真测试仪上导入定制化的模拟业务流后加以执行。

5G 核心网信令风暴测试着重关注下述业务模型与测试场景：

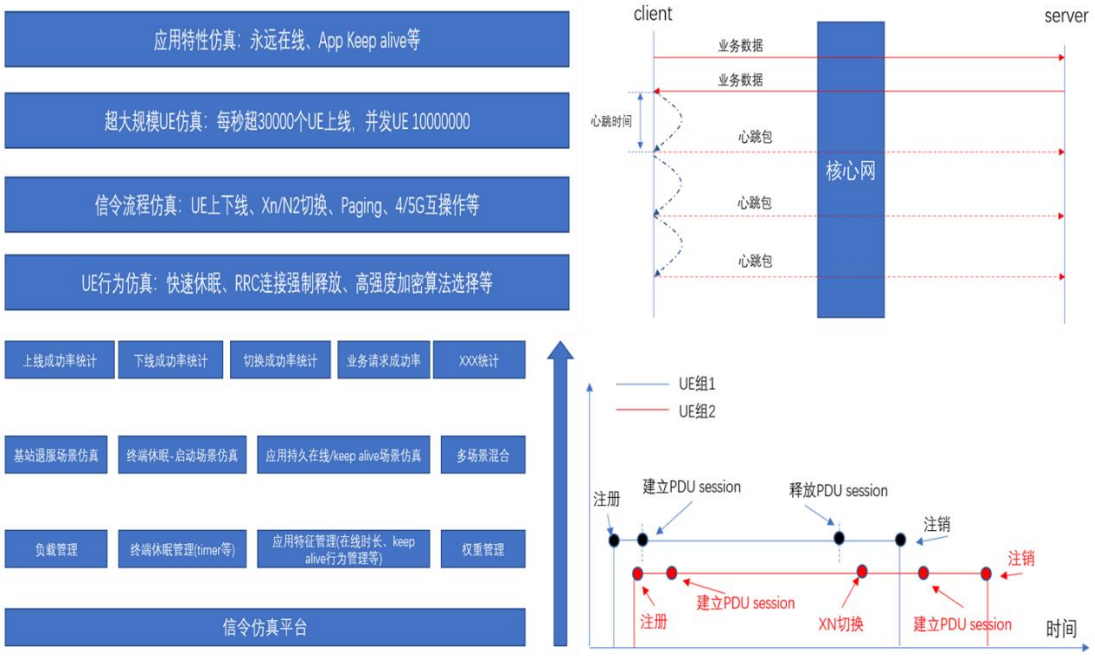
- 大规模 GNB 下海量 UE 的认证接入与多媒体业务下的切换组合测试；
- 5G 核心网海量 UE 在线背景下 UE 通过基站请求接入的混合业务测试。

为完成以上的测试任务，除了真实基站外，我们使用高性能的 5G 核心网仿真测试仪与 5G 真实终端共同配合构成 5G 信令风暴测试平台加以实现。

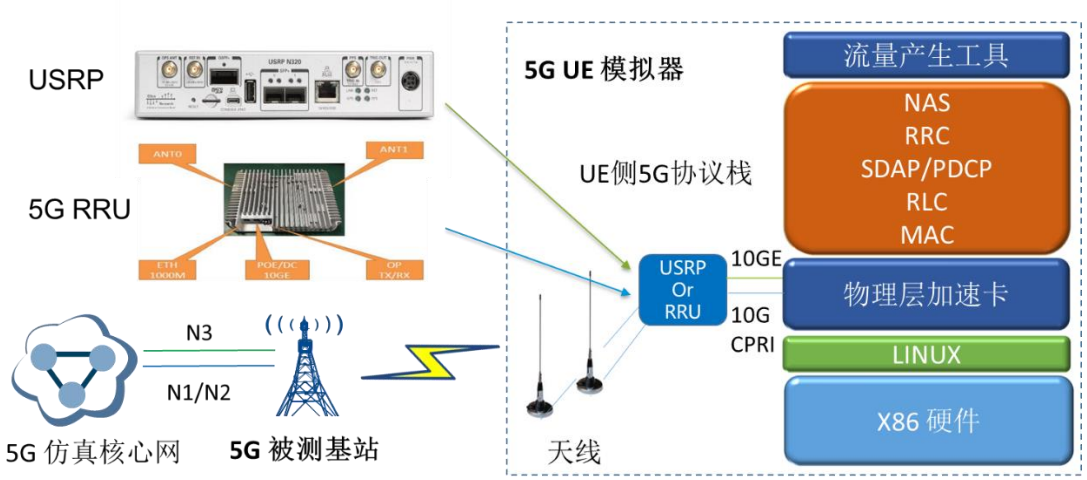


5G 核心网信令风暴仿真测试平台以高性能 5G 核心网仿真测试仪为核心，实现对 5GC 主要信令网元 AMF、SMF、AUSF、UDM、NSSF、NRF、PCF 和 AF 以及各网元之间接口协议的仿真；同时仿真无线接入网的非无线部分，提供对 GNB、UE 非无线侧和 N1、N2 接口的仿真，通过 40000TPS 以上单节点业务过程、200Gbps 单节点的媒体流量带宽、20Gbps 单 UE 接入吞吐量、65536 个最大仿真节点数实现高度逼近现网规模的仿真。

以 5G 核心网信令风暴仿真测试平台为基础，针对 5G 核心网架构的新变化和新特征，产生相应的信令风暴业务模型和流量触发：如 5G UE 上下线、Paging（UE 和网络触发）、多 PDU 会话、Xn 切换、N2 切换、4/5G 互操作、PDU Session Modify 等业务组合流程的仿真，支持如周期性的大规模仿真终端的睡眠、重新激活、数据连接的断开和重连、永远在线消息等仿真功能，因而形成综合有效的 5G 核心网信令业务仿真模型，使得测试结果更加逼真可信。



5G 接入网信令风暴测试平台以高性能 5G 多用户仿真终端和 5G 核心网仿真测试仪为核心，对被测 5G 基站进行包围测试。5G 接入网信令风暴测试的关键在于多 RRC 连接状态的建立与释放，而并非简单地仿真短时间内 UE 的上下线行为，短时间内的大规模用户上下线并不是产生信令风暴的充分必要条件。接入网信令风暴的设计基于不同的场景和不同的信令风暴仿真方式，从多个维度入手，即运用多用户仿真终端技术，实现不同用户端到端的各种信令行为仿真，如短时间内大量终端的瞬间接入以及不同的终端同时仿真不同的信令流程等，并对 RRC 计时器参数设置、各个时间点进行控制，形成大规模的基站信令风暴触发模型。



5G 信令模糊测试背景介绍：

5G 网络的设计目标是增强的移动宽带、大规模机器类型连接通信和实时控制、提供超高稳定性的无处不在的高速、低延迟的连接服务等，因此相比现有网络具有更高的速度、更多更广的设备接入和更低的网络延迟、更多的接口、更多的应用类型、更多的信令消息流程以及更复杂的保护机制、更复杂的安全架构、更多的安全问题等特征，因此在各种消息和流程中也更容易触发各种错误类型，如：核心网/接入网的 bug 等，在特定情况下产生异常信令消息；网络传输设备丢包，部分信令消息的丢失导致异常流程；3GPP 技术规范存在某些定义

不够严谨的问题，不同厂商的理解不一致，在异厂商设备对接时，可能因为某个特定字段解析失败，导致无法响应而产生异常的信令流程等。

5G 信令模糊测试的依据和必要性即来源于 5G 网络系统中上述客观存在的系统和协议发生的错误消息和异常流程。Fuzzing 模糊测试是一种通过构造能够使得软件崩溃的畸形输入来检验和发现系统中是否存在缺陷和隐患的安全测试方法，具有自动化程度高、适应性广的特点，是漏洞挖掘领域最有效的方法之一。模糊测试是一种反向或负面的软件测试方法，它向运行的软件程序、设备或系统提供错误格式和意外消息的输入数据，目的是发现程序、设备或系统与安全相关的缺陷，即导致拒绝服务、服务降级或其他意料之外的任何关键缺陷行为。如将在服务器与客户端之间通信的数据报文截获并在包头加以改变后重新发送到对端的过程，即是一种在输入端添加错误或异常的模糊数据产生过程。

基于生成的模糊测试测试步骤：

1) 协议解析：通过公开资料或者对网络数据流量的分析，理解待测协议的层次、包字段结构、会话过程等信息，为后续测试用例的生成打下基础；
2) 测试用例生成：依据上阶段整理出来的字段结构，采用变异的方式生成畸形测试用例，发送给待测对象；
3) 异常捕获和定位：通过多种探测手段发现由测试用例触发的异常，保存异常相关数据信息，为后续异常的定位和重现提供依据。

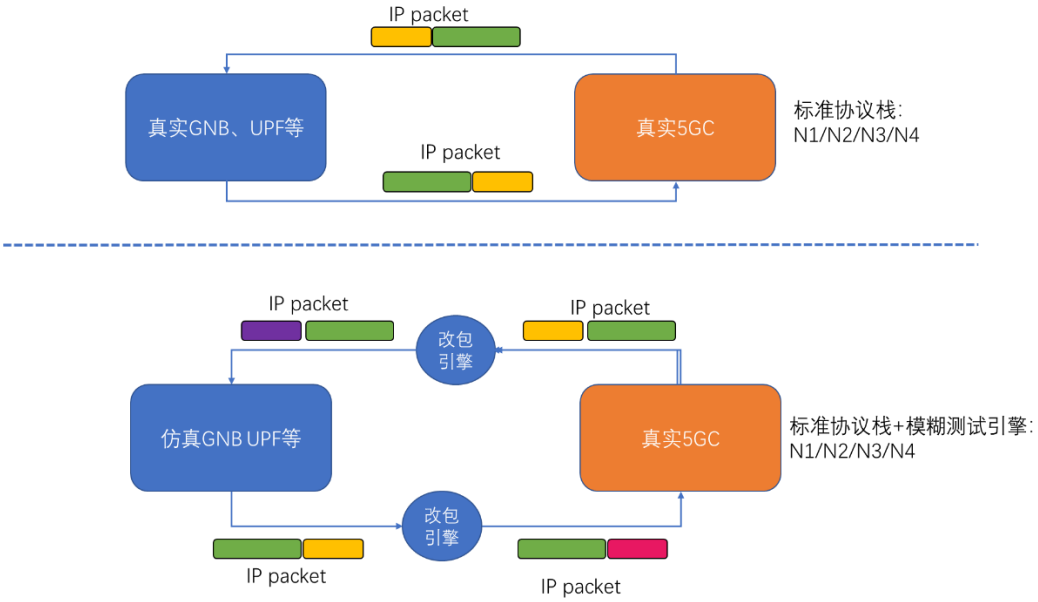
模糊测试与回归测试的区别在于：

1) 方法不同：
   回归测试：输入正常参数，查看系统是否有错
   模糊测试：输入非法参数，查看系统是否出错
2) 目标不同：
   回归测试：防止用户正常步骤下遇到系统错误
   模糊测试：防止攻击者发现可利用的系统错误

5G 信令模糊测试是由 5G 模糊测试管理工具建立和控制的基于 5G 协议生成的模糊数据输入过程，可针对 5G 核心网或 5G 空口协议字段加以改包后对核心网接口和空口发起攻击，由内嵌在 5G 高性能核心网测试仪与 5G 高性能多用户仿真终端中的改包引擎执行，即分别从核心网接口和空口接口侦听、截获并修改目标数据包，然后将修改后的数据包发往对端。5G 核心网协议模糊测试的目标协议字段可针对 N1/N2/N3/N4 各接口数据包，5G 空口协议模糊测试的目标协议修改字段可针对 MAC/RLC/PDCP/RRC/NAS 各层消息。

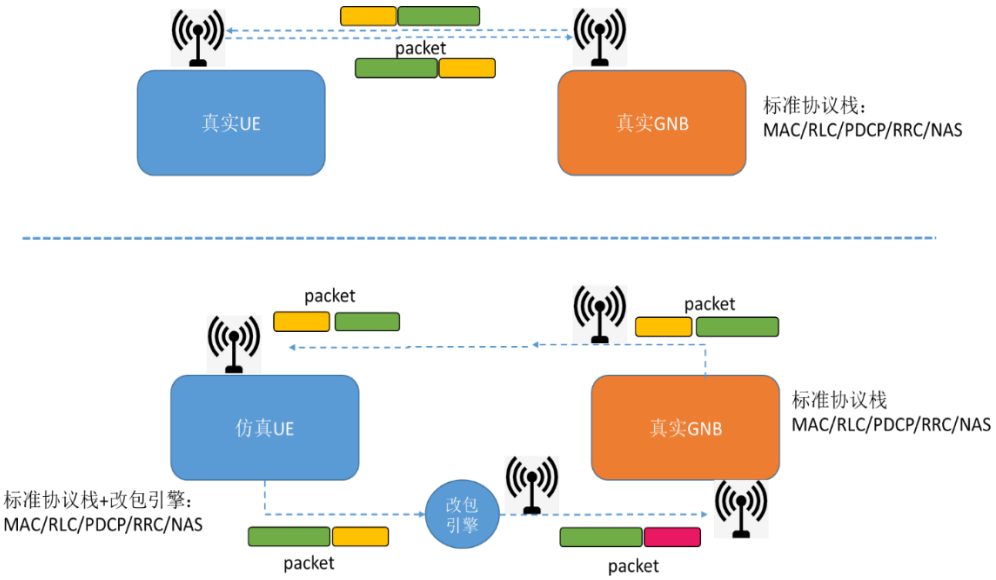
在 5G 核心网协议模糊测试过程中，由 5G 核心网改包引擎负责构造目标接口异常信令，即构造不完整信令流程(如只有单向请求无响应)、非法信令流程（如在没有收到请求的情况下直接回应）、异常协议字段等方面来进行。在确定被测网元对象或业务流程后，构造特定的异常业务流程并发送至被测设备，观察被测设备的反应。核心网改包引擎的主要改包信令接口包括：N1/N2/N4，用户面接口：N3。

5G 核心网接口通信协议模糊测试过程如下图：



在 5G 空口协议模糊测试过程中，空口改包引擎可以根据预先定义的规则灵活地修改 PDCP/RRC/NAS 层的任意字段。同时支持变量化的修改规则可以按照一个预先指定的数据范围和步长进行更改。这样的策略可以保证协议模糊化遍历所有的协议字段和变量，从而充分的测试 UE 到基站的协议健壮性。核心网改包引擎可通过与星载基站之间的接口对接口上的消息进行改包。

5G 空口通信协议模糊测试过程如下图:



改包引擎改包的流程分为如下几步:

A. 测试仪表根据标准协议栈构造正常通信的数据报文进行通信

B. 改包引擎监听仪表网络端口的发包并获取协议栈准备发送的数据报文，在改包引擎返回结果之前先暂时不按照标准协议栈发送原始报文

C. 获取的协议栈准备发送的数据报文按照改包引擎预先配置好的策略进行匹配，没有命中

策略的继续按照协议栈原来的行为发送数据报文，如果命中策略则按照预先设定的策略进行修改后把修改后的报文进行发送
D. 每命中一次策略，在仪表上进行统计并最终形成统计报告。

改包引擎的语法规则定义采取了结构化类似脚本的定义方法。通过定义每个层次的字段进行规则匹配。当测试人员确认一个测试用例发现漏洞之后，需要记录相关测试用例和工具配置脚本及被测设备的环境和版本等信息，把所有相关信息整理加工，存入漏洞库。同时后续可以通过安全测试平台重新进行测试和复现相关漏洞问题。

经多个客户的实测证明，模糊测试是一种十分有效的 5G 网络系统软件安全漏洞的检测方法，已发现的较大漏洞有核心网 N2 和 N4 接口的管理与认证漏洞等。具体到核心网和空口通信协议模糊测试的消息种类和异常流程，应根据接口协议和规范的要求，在模糊测试工具已积累的安全漏洞测试脚本的基础上，以能够产生模糊数据输入和改包的消息与流程种类和数量为准。