通过端到端流控有效防护信令风暴的方案研究

Research on Effective Protection Against Signaling Storms Through End-to-end Flow Control

尹永鑫[1]，关　威[1]，张　欣[1]，贺晓博[2]（1. 中国联合网络通信集团有限公司，北京 100033；2. 中讯邮电咨询设计院有限公司郑州分公司，河南 郑州 450007）

Yin Yongxin[1]，Guan Wei[1]，Zhang Xin[1]，He Xiaobo[2]（1. China United Network Communications Croup Co. Ltd.，Beijing 100033，China；2. China Information Technology Designing & Consulting Institute Co.，Ltd. Zhengzhou Branch，Zhengzhou 450007，China）

摘　要：

随着运营商网络的云化和集约化部署，研究防控由于网络故障引发的信令风暴已成为保护移动通信网网络安全的重要课题。通过针对核心网前后端信令放大效应的研究及流控模型的构建，制定了核心网前端精准流控和分级流控的部署策略；同时，结合核心网对终端、基站引导机制的研究，构建了可以指导运营商有效防护信令风暴的端到端流控方案。

关键词：

信令风暴；流控；放大效应；终端管控

doi：10.12045/j.issn.1007-3043.2023.05.013

文章编号：1007-3043（2023）05-0077-06

中图分类号：TN915

文献标识码：A

开放科学（资源服务）标识码（OSID）：

Abstract：

With the cloud and intensive deployment of operator networks，research on the prevention and control of the signaling storm caused by network failures is an important issue that protects the security of operator networks. It develops a precise flow control and hierarchical flow control scheme for the front-end of the core network by studying the amplification effect of signaling at the front and rear ends of the core network and the construction of flow control model. Based on the research on the guidance mechanism of terminals and base stations in the core network，an end-to-end flow control protection scheme that can guide operators to effectively respond to signaling storms is constructed.

Keywords：

Signal storm；Flow control model；Amplification effect；Terminal control

引用格式：尹永鑫，关威，张欣，等. 通过端到端流控有效防护信令风暴的方案研究[J]. 邮电设计技术，2023（5）：77-82.

1 概述

近2年境外运营商发生了多例大规模网络故障，故障期间出现的网元过载拥塞和信令风暴导致故障影响范围大、持续时间长，对用户的个人权益和运营商的品牌形象产生了较大的负面影响。2022年7月，某境外运营商移动网核心路由器割接失败后回退，大量终端集中发起注册导致PCRF/HSS过载，进而引发信令风暴，经核心网和无线网的手动流控后仍无法压制信令风暴，故障持续时间超过60 h。

收稿日期：2023-04-02

多起故障案例表明，网络故障发生时的DC容灾倒换和故障恢复后的用户集中注册是引发信令风暴的2类主要原因。经实验室模拟，极端故障场景下注册浪涌对移动核心网的冲击达到常规注册模型的100倍，大量用户集中发起注册可能引发网元拥塞和业务劣化，用户业务失败后的反复重试引发设备过载，进一步导致正常用户业务受影响引发冲击蔓延，最终发生信令风暴。

网元部署自保流控是防护信令风暴的重要手段，但随着运营商5G用户的迅速增长，产生信令风暴的风险呈显著增长态势。5G网络中终端机制与核心网业务流程强耦合，5GC或IMS其一不可用将导致终端重

新注册，而1次注册贯穿核心网10余个网元、近百次信令交互，其中任一消息被流控均将导致注册失败。因此，原有的各自为阵的设备过载自保机制已无法应对5G时代下的网络安全挑战，需制定端到端流控方案以有效应对注册信令浪涌对网络的冲击。

2 端到端流控方案架构

2.1 EPC/5GC/IMS网络的信令流量放大效应

大量终端同时登网产生的注册信令冲击是核心网信令风暴产生的首要原因，注册信令冲击主要存在以下几类特征。

特征1：用户注册请求在网元内部呈现百倍的信令流量放大效应。以5G SA用户注册为例，5G终端需要成功完成1次5GC注册、1次数据PDU会话建立、1次语音PDU会话建立、1次IMS挑战鉴权、2次第三方注册才能正常使用数据、语音和短信业务，用户1次注册请求转化为核心网网元间的近百次信令处理资源消耗。

特征2：用户注册各类信令流程均在后端网元HSS/UDM收敛。终端注册和鉴权流程需通过HSS/UDM下载签约数据、鉴权向量并更新用户状态，因此用户在EPC/5GC/IMS域各类信令流程均会共同占用后端网元HSS/UDM的信令处理能力。

特征3：用户注册失败，终端将多次重试，消耗网络资源。当大量用户终端同时向核心网发起注册请求时，因EPC/5GC/IMS网络对信令流量的放大效应，注册请求将对核心网各网元产生巨大的信令冲击。信令流量如超过网元处理能力，将导致HSS/UDM等网络中的短板网元首先出现过载拥塞，引发用户业务失败。此时注册失败的终端频繁重试将极大地消耗网络资源，导致恶性循环。前后端信令流量放大效应如图1所示。

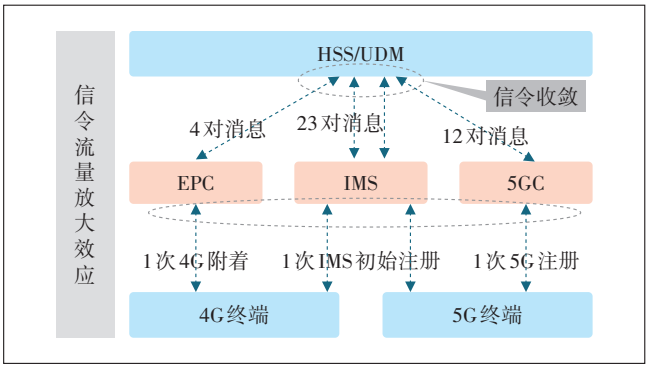

图1　前后端信令流量放大效应

2.2 端到端流控方案

为避免信令流量放大效应引发后端网元过载进而出现雪崩效应，已针对信令风暴产生的原因、特征和危害制定了核心网端到端流控方案，如图2所示。其原则如下。

a）在EPC/5GC/IMS前端网元部署精准流控消减信令浪涌首冲击。

b）在端到端网元部署分级流控保障信令冲击发生时正常用户不掉线。

c）在端网间部署终端重试引导和管控策略保障过载拥塞不扩散。

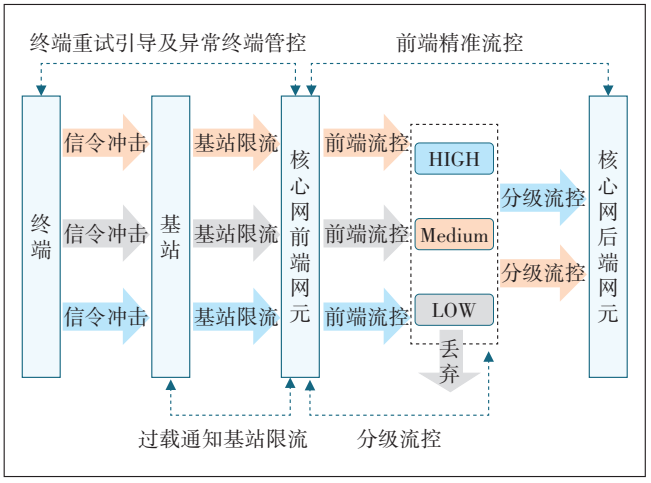

图2　端到端流控方案示意

d）在无线和核心网间部署协同流控，保障极端场景下信令风暴可收敛。

3 EPC/5GC/IMS前端精准流控部署策略

当注册信令冲击发生时，为保障后端网元不过载，应根据HSS/DUM处理能力，在入口网元MME/AMF/SBC上部署前端精准流控策略，拦截核心网各域内已无法处理的增量业务请求，使经入口网元放通的注册请求均能有效处理，百分百利用后端网络资源，有序消化信令冲击。运营商现网网络架构复杂，为在前端网元部署精准流控，需制定以下4个流控模型：前后端信令放大效应模型、后端网元能力分摊模型、前端网元精准流控模型和DRA精准流控模型。

运营商各本地网需根据EPC/5GC/IMS网络信令流程和网络功能开启情况制定适用于本地网的前后端信令放大效应模型和后端网元能力分摊模型；进而根据本地网业务量、组网架构、网元处理能力、放大效应模型和后端网元能力分摊模型推导出前端网元精

准流控模型。

针对不同的流控场景，可将前端网元精准流控模型细分为常规部署模型和应急处置模型，其中常规部署模型兼顾常规故障场景下的流控能力和用户上线能力；应急处置模型适用于在无法有效平抑信令冲击时应急开启。同时，为避免常规部署模型在极端场景下引发HSS/UDM过载，另部署DRA精准流控模型为HSS/UDM提供入向流控保护。前端精准流控模型示意如图3所示。

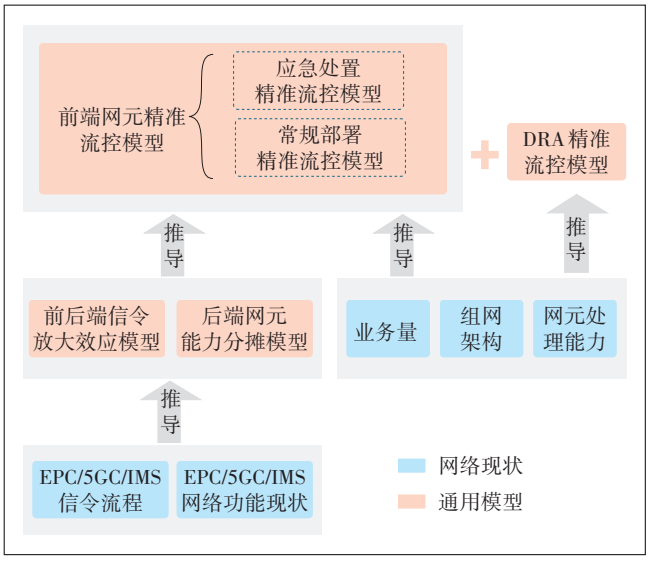

图3　前端精准流控模型示意

3.1 前后端信令放大效应模型

4G附着、5G注册、IMS初始注册因运营商各本地网络的个性化部署策略，对后端HSS/UDM网元的消息放大效应呈现显著差异，如VoLTE AS或HSS未开启集合下载时，HSS的diameter消息放大效应翻倍。因此，需充分评估本地网络各类典型策略部署情况，制定前后端信令放大效应模型，模型样例如表1所示。

3.2 后端网元能力分摊模型

因4G附着、5G注册、IMS初始注册对后端消息的放大效应不同，3类场景对HSS/UDM的资源消耗存在较大差异。另外，云化UDM存在2种组网架构：UDM的EPC和IMS信令处理单元共用虚机，5GC信令处理单元占用独立虚机；UDM的EPC信令、IMS信令和5GC信令处理单元共用虚机。综合3类业务场景的信令放大模型及HSS、UDM的组网架构，制定后端网元能力分摊模型如表2所示。

3.3 前端网元精准流控模型

网元容灾倒换、网络故障恢复等场景导致大量4G、5G用户同时向核心网发起初始注册形成注册浪涌，注册浪涌对不同网元的冲击规模与故障场景、4G和5G用户的规模和比例密切相关。运营商现网中常见的承载网故障后恢复、资源池故障后恢复、单DC故障容灾倒换等容易引发信令冲击场景，发起注册的用户通常分布在省内多台UDM、HSS设备上，为保障此场景下后端网元不发生过载且保障掉线用户可以迅速登网恢复业务，制定了常规部署的前端网元精准流控模型。常规部署的精准流程模型要点如下：

a）根据HSS、UDM网元的活动用户占比情况，推导出大量终端同时登网场景下，后端网元的上线能力最短板。

b）根据前后端消息放大效应模型，分别推导出前端网元MME、AMF、SBC的总上线能力。

c）以VoLTE渗透率较高时，4G和5G附着成功后均发起IMS初始注册为原则（EPC上线能力+5GC上线

表1　前后端信令放大效应模型

业务场景	参数名称	消息放大系数	消息放大系数说明
EPC附着	$W1$	2	2对S6a口消息
EPC附着（开启通知）	$W1$	4	2对S6a口/2对通知消息
5GC注册	$W2$	12	6对N8、N12口/6对N10口消息
IMS初始注册（关闭esrvcc、开启集合下载）	$W3$	10	5对Cx口/5对Sh口消息
IMS初始注册（开启esrvcc、开启集合下载）	$W3$	13	5对Cx口/5对Sh口/3对esrvcc注册消息
IMS初始注册（开启esrvcc、关闭集合下载）	$W3$	23	5对Cx口/5对Sh口/3对esrvcc注册/10对补充业务消息

表2　后端网元能力分摊模型

UDM组网架构	参数名称	参数算法公式	参数定义
EPC/IMS处理单元共虚机 5GC处理单元单独虚机	$X1$	$W1/(W1+W3)\times100\%$	EPC附着占用HSS/UDM-HSS虚机能力比例
	$X2$	$W3/(W1+W3)\times100\%$	4G用户IMS注册占用HSS/UDM-HSS虚机能力比例
	$X3$	100%	5GC注册占用UDM-5GC虚机能力比例
	$X4$	0	5G用户IMS注册占用UDM-5GC虚机能力比例
EPC/IMS/5GC处理单元共虚机	$Y1$	$W1/(W1+W3)\times100\%$	EPC附着占用UDM虚机能力比例
	$Y2$	$W3/(W1+W3)\times100\%$	4G用户IMS注册占用UDM虚机能力比例
	$Y3$	$W2/(W2+W3)\times100\%$	5GC注册占用UDM虚机能力比例
	$Y4$	$W3/(W2+W3)\times100\%$	5G用户IMS注册占用UDM虚机能力比例

能力≤IMS上线能力，否则将导致IMS注册失败），根据SBC的上线能力与4G/5G用户的比例，进一步校准EPC、5GC的总流控阈值。

根据以上原则，定义相关参数并制定常规部署的前端网元精准流控模型如表3、表4所示。

表3　定义模型相关参数

参数名称及定义	应用条件
A(*N*)=HSS(*N*)主用FE处理能力（TPS）	EPC和IMS共享HSS处理能力
B(*N*)=UDM(*N*)的HSS虚机主用FE处理能力（TPS）	UDM-HSS与UDM-5GC信令处理单元独立虚机
C(*N*)=UDM(*N*)的5GC虚机主用FE处理能力（TPS）	UDM-HSS与UDM-5GC信令处理单元独立虚机
D(*N*)=UDM(N)虚机主用FE处理能力（TPS）	UDM-HSS与UDM-5GC信令处理单元共虚机
E(*N*)=HSS/UDM(N)4G附着用户占本省全量4G附着用户比	通用
F(*N*)=UDM(N)4G和5G注册用户占本省全量注册用户比	通用
G(*N*)=UDM(N)5G注册用户占本省全量5G注册用户比	通用
H(*N*)=UDM(N)4G注册用户占本网元注册用户比	通用
K(*N*)=UDM(N)5G注册用户占本网元注册用户比	通用
U=本省4G附着用户占本省总注册用户比	通用
V=省内5G注册用户占本省总注册用户比	通用
*T*1=本省MME套数	通用
*T*2=本省SBC套数	通用
*T*3=本省AMF套数	通用

极端故障场景下，常规部署的综合考虑削减信令冲击和用户上线速率的精准流控方案已无法有效平抑信令冲击并保护后端网元，需针对不同的故障场景制定应急部署的精准流程模型，在网元出现拥塞时及时手动开启。应急部署的精准流程模型要点如下：

a）提前评估各类故障场景对应的后端网元处理能力最短板，以及相应场景下前端网元的台套数。

b）根据前后端消息放大效应模型，推导出各类应急场景下，前端网元MME、AMF、SBC的流控阈值。在故障发生时结合故障场景和流控效果应急开启。

根据以上原则，制定应急部署的前端网元精准流控模型样例如表5所示，现网部署时需结合故障场景提前制定多套应急部署流控模型。

3.4 DRA精准流控模型

因常规部署的精准流控模型在特殊故障场景下仍存在引发后端HSS/UDM过载的风险，因此需在DRA上针对本地网内所有HSS、UDM本局处理能力分局向部署流控策略。每个局向分接口的流控参数根据后端网元能力分摊模型推导确定，即：S6a口流控阈值=*A*(*N*)×*X*1，Cx/Sh口流控阈值=*A*(*N*)×*X*2。

DRA精准流控可保障在极端故障场景下，超过HSS、UDM处理能力的信令冲击提前在DRA侧拦截，避免在应急处置精准流控参数配置前即发生HSS、UDM网元过载。

4 EPC/5GC/IMS的分级流控部署策略

前端精准流控的部署保障了大量终端同时发起EPC/5GC/IMS初始注册时，后端网元可全量有效处理经前端网元放通的用户请求。当故障发生时，除因容灾等原因发起初始注册的用户外，仍存在大量未掉线用户发起正常的重注册、短消息、语音和数据业务。一旦未掉线用户发起的业务请求因网元的流控机制被拒绝或丢弃，终端将根据自身失败重试机制发起初始注册用户重新登网业务请求，进一步加大注册信令冲击。

为避免在线用户业务失败恶性循环引发网络雪崩，需要在核心网各域网元中部署分级流控策略，对业

表4　前端网元精准流控模型——常规部署

网元	流控模型	模型公式
MME流控阈值	EPC域HSS、UDM能力（TPS）	MIN{MIN[*A*1/*E*1，*A*(*N*)/*E*(*N*)，*B*1/*E*1，*B*(*N*)/*E*(*N*)]×*X*1，MIN[*D*(1)×*H*(1)/*E*(1)，*D*(*N*)×*H*(*N*)/*E*(*N*)]×*Y*1}
	MME总流控阈值（CAPS）	MIN{EPC域HSS、UDM能力/*W*1，SBC总流控阈值×*U*}
	单套MME流控阈值（CAPS）	MME总流控阈值/（*T*1-1）
SBC流控阈值	IMS域HSS、UDM能力（TPS）	MIN{MIN[*A*1/*E*1，*A*(*N*)/*E*(*N*)，*B*1/*F*1，*B*(*N*)/*F*(*N*)]×*X*2，MIN[*D*(1)/*F*(1)，*D*(*N*)/*F*(*N*)]×*Y*4}
	SBC总流控阈值（CAPS）	IMS域HSS、UDM能力/*W*3
	单套SBC流控阈值（CAPS）	SBC总流控阈值/（*T*2-1）
AMF流控阈值	5GC域UDM能力（TPS）	MIN{MIN[*C*1/*G*1，*C*(*N*)/*G*(*N*)]×*X*3，MIN[*D*1×*K*1/*G*(1)，*D*(*N*)×*K*(*N*)/*G*(*N*)]×*Y*3}
	AMF总流控阈值（CAPS）	MIN{5GC域UDM能力/*W*2，SBC总流控阈值×*V*}
	单套AMF流控阈值（CAPS）	AMF总流控阈值/（*T*3-1）

表5　前端网元精准流控模型——应急部署

网元	流控模型	模型公式
MME流控阈值	EPC域HSS、UDM能力(TPS)	MIN{MIN[$A1/E1$,$A(N)/E(N)$,$B1/E1$,$B(N)/E(N)$]×$X1$,MIN[$D(1)\times H(1)/E(1)$,$D(N)\times H(N)/E(N)$]×$Y1$}
	MME总流控阈值(CAPS)	MIN{EPC域HSS、UDM能力/$W1$,SBC总流控阈值×U}
	单套MME流控阈值(CAPS)	MME总流控阈值/$T1$
SBC流控阈值	IMS域HSS、UDM能力(TPS)	MIN{MIN[$A1/E1$,$A(N)/E(N)$,$B1/F1$,$B(N)/F(N)$]×$X2$,MIN[$D(1)/F(1)$,$D(N)/F(N)$]×$Y4$}
	SBC总流控阈值(CAPS)	IMS域HSS、UDM能力/$W3$
	单套SBC流控阈值(CAPS)	SBC总流控阈值/$T2$
AMF流控阈值	5GC域UDM能力(TPS)	MIN{MIN[$C1/G1$,$C(N)/G(N)$]×$X3$,MIN[$D1\times K1/G(1)$,$D(N)\times K(N)/G(N)$]×$Y3$}
	AMF总流控阈值(CAPS)	MIN{5GC域UDM能力/$W2$,SBC总流控阈值×V}
	单套AMF流控阈值(CAPS)	AMF总流控阈值/$T3$

务类型和信令消息类型区分优先级队列进行调度。分级流控模型如表6所示。配置模型原则为：

a）前端流控已放通的会话的后续中间消息高优先级执行，保障网络资源不浪费。

b）网元间的心跳检查消息最高优先级放通，保障网元通信不中断。

c）区分业务场景分级调度，放通重注册/注册更新保障老用户不掉线；流控初始注册，控制新用户接入。

5 流控模型效果验证

为验证核心网前端精准流控和分级流控的效果，在实验室搭建5GC和IMS网络模拟环境，模拟20万5G SA注册用户因网络故障下线，在故障恢复后大量终端同时登网冲击5GC、IMS、UDM网元的场景。观测在故障恢复后的1 h内，UDM收到的信令冲击量变化情况（根据放大系数折算为caps）。

场景1：仅部署自保流控。在核心网未部署前端精准流控和分级流控，仅开启设备自保流控的情况下，随着大量下线终端登网，UDM受到的信令冲击量持续增加，直至触发设备自保流控并丢弃无法处理的信令。因单用户的5GC注册和IMS注册会放大为25对与UDM交互的信令，部分中间消息被丢弃导致用户注册失败重试。UDM的自保流控无法有效消化注册浪涌冲击，导致网元持续过载，故障恢复1 h后用户仍无法登网注册。

表6　分级流控模型

分级模型	队列优先级	判断原则	EPC/5GC业务类型	IMS业务类型
高优先级	1	消息类型	中间消息	中间消息
高优先级	1	消息类型	心跳消息	心跳消息
高优先级	2	业务类型	紧急呼叫	紧急呼叫
普通优先级	3	业务类型	VoLTE语音业务	重注册
普通优先级	4	业务类型	注册更新请求/TAU请求	VoLTE呼叫/短信
普通优先级	5	业务类型	初始注册请求/附着请求	初始注册
低优先级	6	业务类型	数据业务	订阅

场景2：部署前端精准流控。在核心网AMF/SBC根据前端精准流控模型部署流控策略情况下，故障恢复后，大量终端同时发起注册请求，当注册请求达到AMF/SBC网元配置的精准流控门限值后，AMF/SBC对超过阈值的注册请求直接回复失败响应，不再占用后端UDM网元的处理资源，UDM可有效处理被AMF/SBC放通的用户注册信令，用户在15 min内完成登网注册，未发生网元过载问题。在12 min后，少部分被AMF/SBC流控的终端根据重试定时器再次发起注册并成功登网，全量用户业务恢复。

场景3：同时部署前端精准流控和分级流控。当核心网网元部署前端精准流控但未部署分级流控情况下，AMF/SBC放通了注册的首消息，但后续鉴权、响应等消息同样存在被流控的风险，导致已被放通注册首消息的用户登网失败。在部署分级流控场景下，可保障被放通注册首消息的用户的后续请求和响应均能被有效处理；同时放通刷新注册、呼叫等高优先级业务，保障在线用户不因网元流控而掉线。根据实验室模拟分析，部署分级流控可更有效提升用户的上线速率，用户在5~10 min内即基本完成登网注册，因流控而延时重试的终端数量明显减少，保障故障发生后全部用户业务迅速恢复。

6 核心网重试机制引导及异常终端管控方案

网元通过部署前端精准流控和分级流控完成对超出网络处理能力的终端接入请求限流，因限流导致

业务请求失败的终端频繁登网重试将加剧对网络资源的消耗。核心网需根据终端在过载流控场景的业务特点和行为部署针对性的解决方案，解决方案包括对于被流控终端重试机制的引导和对于不遵守网络侧引导机制的终端的异常行为管控。

6.1 终端重试机制引导方案

a）EPC/5GC终端重试引导方案：3GPP TS 24.301、3GPP TS 24.501分别定义了MME和AMF针对终端注册场景，网络侧通过回复拒绝消息（原因值#22 Congestion）并携带Backoff Timer信元实现EPC/5GC流控的功能。该信元指示请求消息重复尝试的延迟时长，使终端延迟并离散接入，减轻终端频繁注册对网络侧的资源消耗。

b）IMS终端重试引导方案：3GPP TS 24.229定义了IMS可通过回复500/503等失败响应码并携带Retry-After头域拒绝终端的注册请求，入口网元通过拦截响应通知终端根据网络侧指示在离散时间重试，消减注册失败用户频繁重试对网元的信令冲击。

6.2 异常终端行为管控方案

现网中部分终端收到网络侧下发的重试引导响应时，存在不遵循Backoff Timer和Retry-After时长要求并反复尝试登网情况，终端的无序注册行为使得终端重试机制引导方案难以取得预期效果。需针对不规范终端行为部署异常终端管控方案，以作为重试引导方案的有效补充。

a）EPC/5GC异常终端行为管控方案：MME/AMF部署信令控制功能，MME/AMF基于短时间内用户附着/注册、PDN连接/PDU会话建立、业务请求等消息的频次实施统计测量，当终端业务请求频次超出阈值即被判定为异常用户，在短时间内限制该终端登网。

b）IMS异常终端行为管控方案：SBC部署黑名单管控功能，SBC将频繁注册用户、异常高频呼叫用户临时加入黑名单，丢弃该用户发送的所有报文，削减高频业务请求对网络的信令冲击。

7 MME/AMF过载通知基站限流方案

当极端故障场景下，核心网流控手段已无法在短时间内平抑终端大量业务请求引发的信令冲击。此时，核心网网元需要通知基站侧实施自动限流，减少发往核心网的信令消息量。

需在AMF/MME网元部署过载通知基站限流功能，功能开启后，MME/AMF网元出现过载时，向4G和5G基站发送Overload Start消息，通知基站按比例拒绝终端新建连接，使得终端注册请求终结在无线侧，不再额外消耗核心网资源。当MME/AMF网元状态恢复正常后，向基站发送Overload Stop消息，通知基站允许终端重新接入网络。

8 结束语

网络演进带来的组网架构和业务模型的频繁调整为流控策略的部署带来了挑战。核心网端到端流控方案有助于指导运营商建立完整的核心网信令风暴防护体系，即应用前端精准流控模型随网络演进更新流控参数，确保流控配置的及时性和准确性；应用分级流控、终端重试引导以及协同基站的终端管控方案，从多维度平抑注册浪涌引发的信令冲击，有效提升网络信令风暴防护能力。

参考文献：

[1] 张宁，宫钦，冯涛，等. 基于主动预测的Diameter信令风暴处理方法研究[J]. 山东通信技术，2022，42(3)：40-43.
[2] 丁义文. Diameter信令网信令风暴抑制方案研究[D]. 北京：北京邮电大学，2017.
[3] 魏子然，黄芬，杨兆铭. 信令风暴的防控方法及计算设备：CN202010523137.0[P]. 2021-12-10.
[4] 饶亮. 信令风暴端到端管控方法及应用系统[J]. 电信技术，2018(3)：62-66.
[5] 彭公孚. 信令风暴的预防与抑制方法研究[J]. 信息通信，2017(3)：248-249.
[6] 马冀，田锦. 即时通信类业务仿真评估及优化研究[J]. 信息与电脑(理论版)，2022，34(2)：204-207.
[7] 马骏野，张可，徐宁. 移动物联网安全监测系统研究与应用[J]. 电脑知识与技术：学术版，2019，15(18)：23-27.
[8] 廖智军，李振廷，石胜林，等. LTE/5G双连接关键技术[J]. 移动通信，2018，42(3)：21-26.
[9] 毛柯平. LTE-5G融合组网设计与研究[J]. 科学与信息化，2021(6)：49，51.
[10] 冯征. 5G信令网引入3GPP R16版本的SCP组网研究（上）[J]. 电信工程技术与标准化，2021，34(1)：1-7.

作者简介：
尹永鑫，毕业于北京邮电大学，工程师，硕士，主要从事移动核心网维护管理、网络优化以及语音网技术研究工作；关威，毕业于北京工业大学，高级工程师，硕士，主要从事核心网运营管理、质量优化、安全管理、技术研究等工作；张欣，毕业于西安邮电学院，高级工程师，学士，主要从事移动核心网维护管理、网络优化以及5GC技术研究工作；贺晓博，毕业于北京邮电大学，高级工程师，学士，主要从事核心网项目的规划、设计、咨询及行业标准编制工作。