基于平战结合的极端场景网络通信保障研究

Research on Network Communication Support for Extreme Scenarios Based on the Combination of Peacetime and Wartime

胡　悦[1]，刘　怡[2]，何建炜[3]，朱　斌[1]（1. 中国联通研究院，北京 100048；2. 中讯邮电咨询设计院有限公司，北京 100048；3. 航天科工空间工程发展有限公司，北京 100000）

Hu Yue[1], Liu Yi[2], He Jianwei[3], Zhu Bin[1]（1. China Unicom Research Institute, Beijing 100048, China; 2. China Information Technology Designing & Consulting Institute Co., Ltd., Beijing 100048, China; 3. CASIC Space Engineering Development Co., Ltd., Beijing 100000, China）

摘　要：

极端场景对网络安全应急通信能力提出的新要求，保障极端场景下的网络安全应急通信能力是重要议题。梳理了网络极端场景类型需求及痛点以及近年网络战争带来的新型网络极端场景趋势；提出一种“平战结合”的通信网络保障技术理论模型，该模型能够充分协调平时与战时的活动和要素，以平时准备提升危机应急的反应速度和处置能力，也通过应对危机来促进平时的准备工作。

关键词：

平战结合；极限场景；应急业务；通信保障

doi：10.12045/j.issn.1007-3043.2025.08.011

文章编号：1007-3043（2025）08-0051-07

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：

The new requirements for network security emergency communication capability in extreme scenarios make it an important issue to ensure the network security emergency communication capability in extreme scenarios. It analyzes the requirements and pain points of extreme scenarios on the Internet, as well as the trend of new extreme scenarios brought by cyber warfare in recent years. It proposes a theoretical model for communication network support technology that combines peacetime and wartime, which can fully coordinate activities and elements in peacetime and wartime, improve crisis response speed and disposal capabilities through peacetime preparation, and promote peacetime preparation work by responding to crises.

Keywords：

Combination of peacetime and wartime; Extreme scenarios; Emergency services; Communication support

引用格式：胡悦，刘怡，何建炜，等. 基于平战结合的极端场景网络通信保障研究[J]. 邮电设计技术，2025(8)：51-57.

1　概述

现代社会已经高度信息化，网络通信技术渗透到各个领域，为人们的生活、工作和学习提供了便利。然而，在自然灾害、战争冲突、技术故障等极端场景下，传统的网络通信系统常常无法满足人们的需求[1]。因此，如何保障网络通信在极端场景下的正常运行，已成为一个亟待解决的问题。近年来，我国自然灾害频发，国际局势对极端场景网络安全应急通信能力提出新要求。在此背景下，像汶川地震救援、北京奥运会保障、神舟十三号返回通信支持、国防交通保障及国际冲突应对等场景，通信网络和应用技术发展要更贴合其通信保障需求，同时强化极端场景通信保障能力。

我国高度重视网络空间基础安全和网络应急保障能力建设。二十大报告明确指出：“推进国家安全体系和能力现代化，坚决维护国家安全和社会稳定。”同时强调，“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障”[2]。此外，国务院、应急管理部陆续下发了《“十四

基金项目：国家重点研发计划资助项目（2022YFB2902503）

收稿日期：2025-07-20

五”国家应急体系规划》《智慧应急“十四五”规划》《地方应急管理信息化2022年任务书》等一系列应急管理规划文件[3-4],强调了要加强现场应急通信保障能力[5]。

随着我国网络基础设施建设的逐步完善,5G网络的基础能力得到快速提升。5G网络能够根据应急客户需求提供大上行、高可靠、低时延、高精度同步和定位、广域漫游、二次认证、网络切片和能力开放等30余项差异化的关键能力,赋能于应急通信领域[6],这使得应急通信具有更好的适应性,在配置及应用上更加灵活,能够减少对周边环境因素的依赖。整体上可提高抢险救灾效率,争取宝贵时间,提升通信应急服务保障的质量和用户体验[7-8]。随着卫星通信高通量、低时延等新技术的快速发展,卫星通信在速率和时延方面已可以满足大多数5G业务场景的需求[9]。卫星通信网络与5G地面通信网络在技术上也已具备融合的基本条件,并逐步朝着不同轨道多卫星系统融合、通信遥感导航卫星融合、地面与卫星系统协同融合等方向发展[10]。通过构建架构、功能、接口、流程一体化的5G天地一体化网络,能够实现覆盖融合、系统融合、网络融合和业务融合,在提高网络资源利用率的同时,为用户提供全球全域无缝连接、业务连续性和通信服务保障,支持丰富多样的通信业务和应用,为灾害现场应急通信提供了有力支撑[11]。

2 网络极端场景定义及发生趋势

2.1 极端场景的定义及范围

通信网络极端场景是指在网络通信过程中可能出现的严重状况,这些状况会导致网络通信无法正常进行或无法达到预期效果。这些极端场景主要包括以下几个方面。

a) 自然灾害。地震、洪水、飓风等自然灾害可能会对网络通信基础设施造成严重破坏,导致通信中断或网络瘫痪[1]。

b) 战争冲突。在战争冲突地区,网络可能会遭到敌方的干扰或破坏,从而无法正常通信[2]。

c) 技术故障。网络通信设备或软件出现技术故障,如遭受病毒攻击、系统崩溃等,可能会导致网络通信无法正常进行,具体而言,技术故障又可以包括以下几项。

(a) 网络设备故障:网络设备(如路由器、交换机、服务器等)可能出现硬件故障、软件故障或网络连接问题,致使网络无法正常运行。

(b) 网络攻击:网络可能会遭受各种形式的攻击,如拒绝服务攻击、病毒、木马、网络钓鱼等,这些攻击可能导致网络瘫痪、数据泄露或被篡改[2]。

(c) 网络拥堵:由于网络流量过大等原因,网络可能会变得非常缓慢或拥堵,导致用户无法正常访问网络资源。

(d) 网络配置错误:网络配置可能出现问题,如IP地址冲突、路由错误、DNS解析错误等,导致网络无法正常通信。

(e) 网络断线:由于线路故障、信号干扰、设备故障等各种原因,网络连接可能会中断,导致用户无法正常访问网络资源。

(f) 电磁干扰:电磁干扰可能会对网络通信设备或信号产生影响,导致通信质量下降或通信中断。

d) 地理环境因素。在高山、峡谷等地理环境中,由于地形复杂、遮挡物多等因素,可能会影响网络通信的覆盖和质量。

e) 人为破坏。人为破坏可能会导致网络通信设备损坏或通信线路被切断,从而影响正常的网络通信[12]。

这些网络极端场景可能对网络通信的可靠性和稳定性产生严重影响。

2.2 网络战带来严重极端场景隐患

近年来,随着国际局势不断复杂演化,我国网络空间安全面临的外部形势严峻。网络战争已成为现代战争不可或缺的一部分[2],它是国家间地缘政治、军事、经济斗争的延续,旨在攻击、破坏、干扰敌军战场信息网络,造成严重的极端网络场景。网络战争的攻击范围广泛,涵盖了国家关键基础设施、工业互联网、网络通信、重要数据、天地一体化、软硬件供应链等多个方面。具体而言,主要包括以下几个方面。

a) 网络攻击关键基础设施成为常态,覆盖范围包括金融、通信、交通、能源、政务网络等领域,近年来部分国家的燃油管道管理系统和输电网络都遭受过网络攻击或非法入侵。

b) 在网络战中,对通信网络基础设施的打击、大规模的DDOS攻击、流量劫持等,都会导致网络通信中断,使网络服务资源的可用性受损[2]。

c) APT攻击、恶意数据窃取或擦除软件在网络战中频繁被使用,是获取情报、引导舆论和破坏重要信息系统的重要手段[2]。

d) 在俄乌战争中,欧洲数以千计的卫星网络遭到黑客攻击,导致乌克兰依赖KA-SAT卫星的客户出现网络中断的情况,这说明天地一体化的卫星网络也成为了网络战所打击的对象。

e) 在俄乌战争中,西方对俄罗斯实施了芯片断供、Github限制开源软件和Oracle停服等多种制裁手段,这说明基础软硬件的供应链也可以武器化,干扰敌对国家的军事行动和经济发展[2]。

3 平战结合定义及网络保障实现机制

3.1 平战结合的定义

“平战结合”这一理念最初是在国防建设领域中提出的,它强调军事发展的各个方面应同时考虑和平时期和战争时期的需要,实现军民融合、相互促进,进而推动国防建设与经济发展相结合[1]。

从系统的观点出发,该理念不仅关注非战时紧急状态的需求,也充分考虑战时紧急状态的需求,实现应急与应战的一体化,以便在战时与非战时紧急状态下都能够迅速整合各种可动员的资源,提高国家经济与社会发展的整体抗逆水平[13-14]。

因此,在通信网络领域,“平战结合”借鉴上述思想的阐释。这意味着通信网络保障需要充分协调平时与战时状态下的活动和要素,既要通过平时的准备工作来提升危机应急的反应速度和处置能力,也要通过应对危机来促进平时的准备工作。从而主要实现在平战结合机制下的网络技术与方案,使得用户特定通信业务随时保持通畅[15]。

3.2 平战结合的网络保障模型

通信网络保障的“平战结合”机制是将“平战结合”思想应用于通信网络领域的结果,体现了系统、动态的网络观。本文将“平战结合”机制定义为:以提高网络极限场景下的通信应急能力为目标,“立足战时、着眼平时”,统筹兼顾平时与突发情况下的网络通信需求,制定网络系统应对及实施方案,快速响应情景式的通信网络服务管理模式,保障用户通信业务随时保持通畅[15]。

“平战结合”机制的目标是提高应急能力,必须“立足战时、着眼平时”,围绕应战需求,从平战状态2个阶段的差异性出发,深刻理解机制核心功能的构建要点[13,15]。

“平战结合”机制的核心在于构建一个具有时序性的情景式治理流程。该流程涉及各要素在不同状态下的转换过程或程序,它能够充分融合资源、技术、方法等要素,并按照模块化组装的方式对这些要素进行组合转换,进而形成应急能力[15]。

“平战结合”机制的设计旨在使机制体系中的激励机制、约束机制、反馈机制、评价机制等在非人为操作的情况下自动连续地发挥作用。

按照“平战结合”机制,可分为3种状态:平时状态、战时状态以及平战转换状态。

根据以上3种状态,可延伸出4项内容,它们分别对应由3种状态划分产生的4个不同阶段的网络技术方案及业务(见图1)。

3.2.1 平时状态下的网络容灾及预案

平时是指从一个突发事件结束到新的突发事件发生前的这段时间,它是用于开展准备、预防和减缓风险工作的阶段,需要建立起常态管理机制。这一时期的主要目标是尽量将风险消灭在萌芽状态,提升抗风险能力。

在平时备战状态下,要防范各类可能的网络风险,增强网络安全防护能力。可采用跨大区容灾、5G信令安全解决方案、创新网络安全架构等技术方案来降低网络安全隐患,提升网络健壮性。同时,考虑将手机直连卫星互联网作为网络备灾的打底方案[9]。制定针对战时、灾时和平时的网络应急预案,健全能够应对各类突发事件以及各种重大活动任务的科学、规范、高效的应急通信保障组织机构和工作机制[3-4]。

3.2.2 平转战状态下的网络快速配置和业务管理

平战切换期是突发事件即将发生时或发生时,减缓风险和进入应急响应状态的阶段,需要建立起转换机制[13,15]。这一时期强调由“平时”状态快速切入“战时”状态,它以增强抗风险能力和应急处置能力为目标。

在平战转换状态下,可采用不同于常规的事后应急通信机动方案,该方案内嵌在业务流程中,可实现自动切换的实时快速业务保通及配置。如网络协同链路管理技术,可通过自适应分流聚合,实现多种接入协议融合转换以及不同维度策略的分流/并流传输能力,动态调整保障通信网络畅通;智能应急业务控制技术,可对特定用户进行接入限制、策略调度及关键业务管控,实现对用户业务的动态管控。

3.2.3 战时状态下的应急网络及业务实现

战时指的是突发事件发生后的一段时间,属于应急响应阶段,需要建立动员机制[13]。这一时期的主要

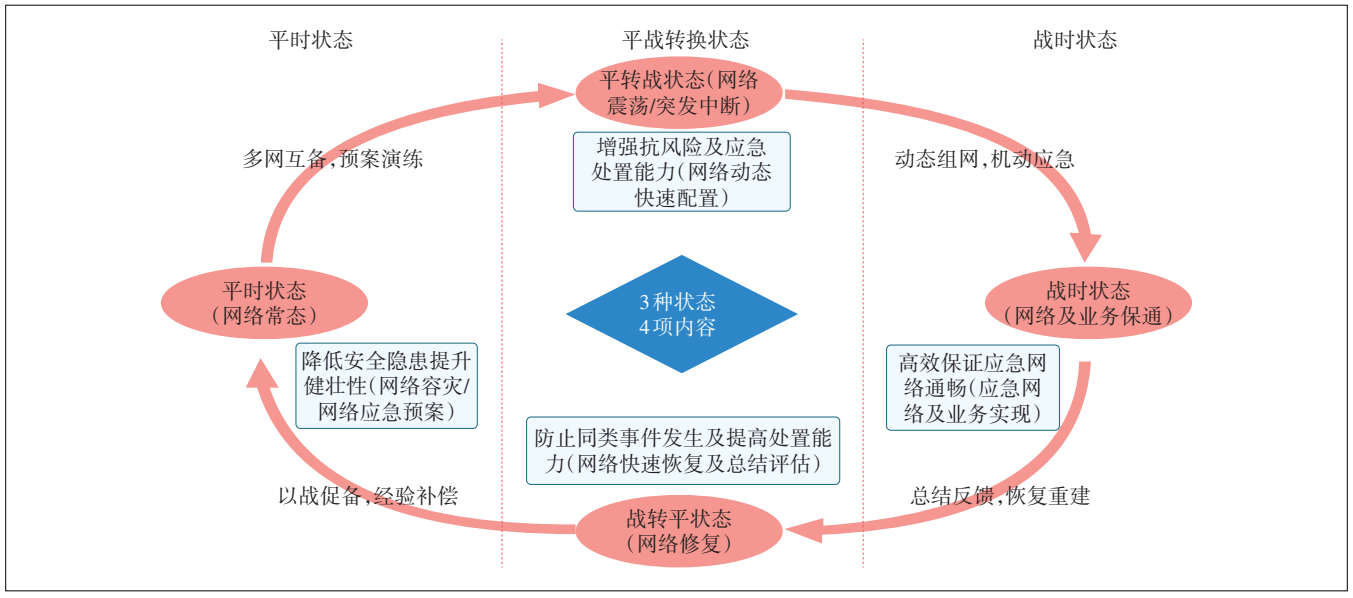

图1　平战结合的网络保障模型

目标是科学、高效、妥善地处置突发事件。

在战时状态下，采用基于天地一体化的用户业务保通和网络补盲方案来保障应急网络畅通，这些方案包括手机直连卫星业务方案、卫星中继应急网络及业务方案、卫星网络漫游方案、自由空间光通信融合网络方案等[9]。

3.2.4　战转平状态下的网络修复学习

战平过渡期是突发事件主要处置结束后的一段时间，是响应、恢复与学习并举的阶段，需要建立转换机制[13-15]。这一时期强调由“战时”状态稳妥地过渡到“平时”状态，以恢复正常的生产生活秩序，防止事件再次发生或提高处置同类事件的能力为主要目标。

除与平转战动态具备相同的动态循环技术方案之外，还应具备针对网络及业务突发作战打击后的快速恢复技术方案[11]，以及恢复平时状态后的总结评估、学习记录等能力[13]。

4　面向极端场景的网络保障技术

4.1　平/战时应急专网业务控制技术

在可用网络资源有限的前提下，如何实现战时状态下的应急业务保障，是需要研究的关键技术。通过建设机动的5G应急专网，利用5G通信业务控制系统技术，实现5G网络在应急场景下的快速一体化接入及精准应用和控制。

5G应急通信业务控制系统内部包含UDM、IMS AS和业务控制模块，它对外与5G核心网、IMS核心网和泛在融合能力开放平台对接，从而实现5G应急通信控制相关业务功能。具体实现如下功能。

a）应急专网内部人员间的3G/4G/5G语音通话、短信及数据访问功能。

b）应急专网与外部移动通信网络间的3G/4G/5G语音通话、短信及数据访问功能。

c）应急网络资源编排和分配优化，以实现业务路由智能选择。

d）互联网应用在应急场景的操作优化，解决大网损坏时，APP应用及短信等不能使用的问题。

e）具备集群认证功能，针对特定应急用户群体，增加认证能力。

f）采用快速部署方案，对5G应急专网进行解耦和简化，满足快速与大网互通和随机随时接入的需求。

g）5G消息、短信与应急通信系统的紧密联动及高效精准投送方案。

h）其他运营商增值业务，如语音增强（实时翻译）、NEF能力开放、QoS控制等的融合应用方案。

系统应支持多种组网模式，支持卫星+5G网络各种组合场景的组网方案，包括支持5G网络下虚拟专网、混合专网和独立专网3类网络形态等（实现用户面下沉、控制面及用户面下沉等场景）以及卫星高低轨不同资源组合场景。此外，系统满足接入兼容要求，可同时满足5G公网和5G专网的接入需求。

当系统接入5G公网时，与5G公网核心网信令面以及IMS核心网互通。系统对接的5G专网可采用虚

拟专网、混合专网和独立专网等3类网络形态。

虚拟专网组网模式的组网架构如图2所示。其优先级配置和切片等特性满足用户对专网隔离性和性能方面的需求。

混合专网组网模式的组网架构如图3所示，在该模式下，应急通信业务控制系统与大网5GC及IMS对接，负责数据转发的UPF网元下沉，以满足数据不出场和业务隔离等需求。

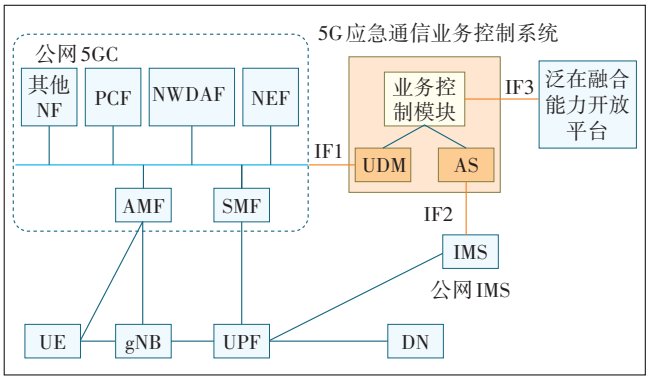

图2　虚拟专网组网模式的应急通信业务控制系统组网架构

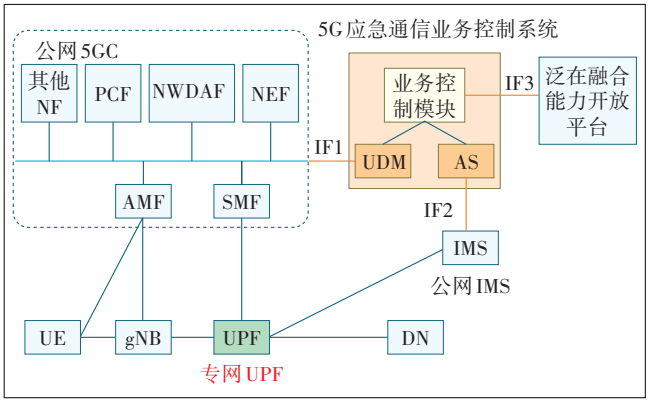

图3　混合专网组网模式的应急通信业务控制系统组网架构

独立专网组网模式的组网架构如图4所示。在该模式下，应急通信业务控制系统与专网5GC及公网或专网IMS对接，如果5GC网元下沉（如AMF、SMF等），UDM未下沉，则系统可与下沉网元进行对接，基础语音业务仍使用大网IMS。如IMS也在专网内独立建设，系统支持与专网IMS对接。

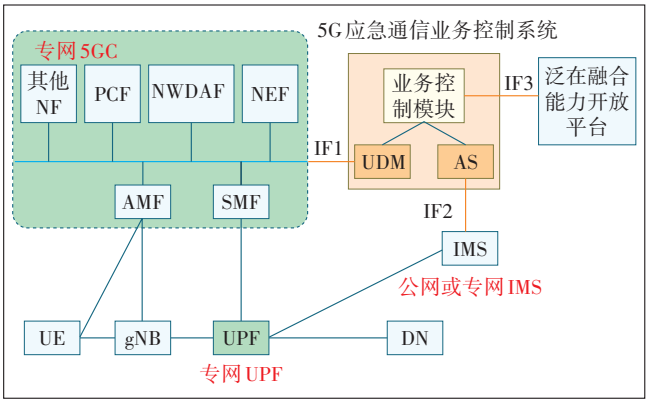

图4　独立专网组网模式的应急通信业务控制系统组网架构

应急通信业务控制系统的关键功能模块如图5所示，具体功能实现如下。

a）业务控制管理模块。提供面向管理员的网站，实现系统管理、网络访问权限控制、基础能力编排与处理、策略调用控制的可视化管理与配置。

（a）系统管理：支持对管理员账号、管理员角色/权限的管理与分配，以及系统/管理员操作日志的记录

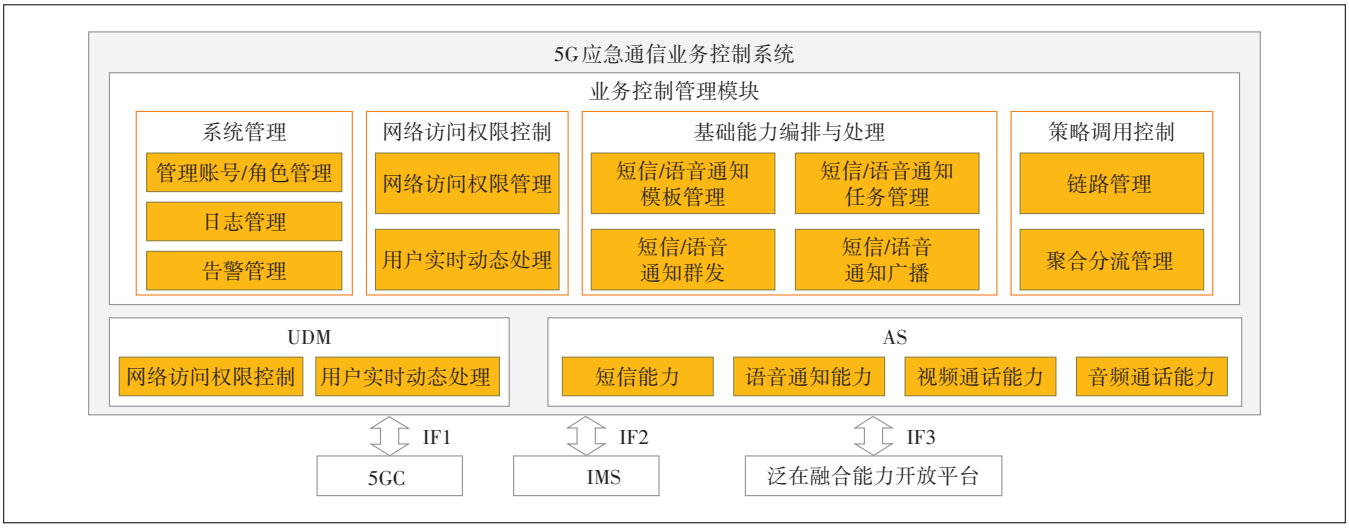

图5　应急通信业务控制系统关键功能模块

和查询能力。同时，允许通过告警管理模块来监测系统告警和运行情况。

（b）网络访问权限控制：提供针对用户、用户组、用户号码段的网络访问权限控制功能，并能进行在线用户的实时动态处理。

（c）基础能力编排与处理：支持短信/语音通知能力模板的创建和管理，以及相应群发/广播任务的创建与执行。

（d）策略调用控制：允许管理员进行链路通道的增删改操作，并具备聚合分流策略的配置管理功能。

b）UDM。接收来自业务控制管理模块的网络访问权限控制信息，并通过IF1接口与公网/专网5GC进行消息交互，从而实现控制功能及用户实时动态处理。

c）AS。与IMS网络对接，实现短信、语音通知、音频通话、视频通话等基础业务能力，并向业务控制管理模块提供相应能力接口供其使用。

4.2 平战转换动态协同组网技术

协同接入配置模块是平战转换的动态协同组网技术的关键功能实体，也是实现该技术的关键网元。它能够实现平战转换期间动态调整地面及低轨卫星、中高轨卫星资源，按需合理分配使用的目标。具体功能设计及技术点如下。

4.2.1 网络部署位置

协同接入配置模块的部署逻辑架构如图6所示，其在网络中部署位置包含以下2个位置。

a）接入侧：位于5G基站和不同卫星网络用户站之间。在上行方向，将来自5G基站的流量通过不同的策略路由到不同的卫星链路进行传输。在下行方向，能够接收不同卫星链路流量并汇聚传输到5G基站。

b）网络侧：位于不同卫星网络信关站和5G核心网之间。在上行方向，将不同卫星的信关站数据汇聚并传输到外部核心网，在下行方向，能将核心网下发的流量根据不同的策略路由到不同的信关站进行传输。

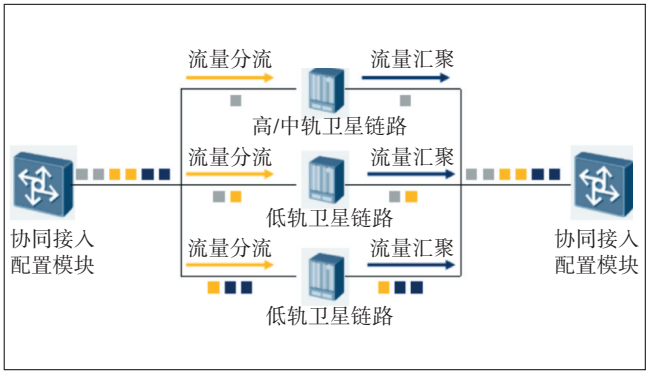

图6　协同接入配置模块的部署逻辑架构

协同接入配置模块处理的流量可包含5G N1、N2、N3、N9以及SNMP的网络管理流量。

4.2.2 自适应分流/聚合功能

协同接入配置模块可按照预设的配置时间间隔，动态监控每条连接链路的带宽情况，并根据每个连接的可利用率来分配传输对应数量的数据包。然后，这些数据包经过接收终端的纠错后，被重新合并还原为原始数据。

4.2.3 应用层流量检测和识别功能

当TCP或UDP数据流经过协同接入配置模块时，系统会读取IP数据包内承载的ISO应用层数据并对其进行重组，从而得到整个数据流应用层的内容，然后按照系统定义的管理策略对流量进行管理和监控操作。

4.2.4 可配置策略的分流功能

模块可以根据不同的策略模板，通过手动或远程的方式配置不同的分流策略，便于根据不同成本的链路流量消耗情况或者不同的卫星传输特性，有针对性地进行设置和调节。例如，有些用户希望优先使用4G网络，其次选择卫星提供的网络链路（基于成本因素）；或者优先采用高轨卫星传输信令面数据（因其稳定）及低轨卫星传输用户面数据（因其高效），其次选择使用高轨卫星传输用户面数据。

策略场景举例如下。

场景1：协同接入配置模块能够根据配置的策略，选择将信令面流量通过高轨卫星用户站进行传输，将用户面流量通过低轨卫星用户站进行传输。

场景2：协同接入配置模块能够根据配置的策略，选择将信令面和用户面流量都通过低轨卫星进行传输。

场景3：协同接入配置模块能够根据配置的策略，选择按照一定比例将流量分别通过低轨卫星+高轨卫星进行传输。

4.2.5 传输链路检测功能

模块能够根据不同的策略快速检测当前配置的卫星链路状态，并能实时维护各条链路状态。其检测功能逻辑如图7所示，当检测到某条卫星链路故障后，模块能自动将该链路置入故障状态。当该链路恢复

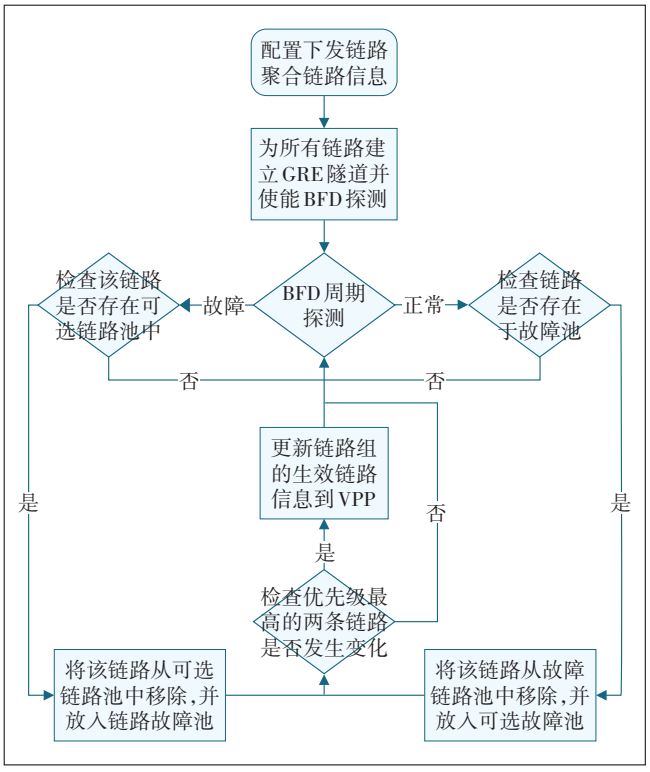

图7　传输链路检测功能逻辑

后，模块能够根据策略或者实时检测结果，自动将其从故障状态切换到可用状态。

4.2.6　自动切换链路功能

当目前正在传输中的链路出现故障时，模块能够自动选择其他可用的链路进行传输。如当前是通过高轨卫星链路进行传输，当检查到高轨卫星链路出现故障时，模块能够按照策略自动选择其他可用的高轨卫星链路或者低轨卫星链路进行传输。

5　总结及展望

本文基于“平战结合”思想，开展通信网络保障和技术方案研究，使通信网络保障能够充分协调平时与战时状态下的活动和要素。一方面，通过平时的准备工作来提升危机应急的反应速度和处置能力，另一方面，借助应对危机来促进平时的准备工作。从而主要实现在平战结合机制下的网络技术与方案，使得用户特定通信业务随时保持通畅。

随着网络技术的持续发展和国际局势的复杂多变，网络极端场景愈发频繁出现，对网络通信保障的需求愈发迫切。该研究内容为运营商提升网络通信的稳定性和可靠性具有重要意义，尤其在极端环境下，能为确保网络通信的正常、高效、自动进行，提供重要的参考模型和技术方案建议。

参考文献：

[1]　齐占军. 关于特大自然灾害中应急通信保障的探讨[J]. 今日消防，2021，6(12)：38-40.
[2]　国家互联网应急中心. 解读国内外网络战形势[EB/OL]. [2025-07-10]. https://www.isccc.gov.cn/xwdt/xwkx/04/253384.shtml.
[3]　白银市应急管理局. 加快智慧应急建设 助力安全水平提升[EB/OL]. [2025-07-10]. https://www. baiyin. gov. cn/bysyjglj/gzdt/art/2024/art_0e2004c82c9643d88f2585582f9e89c1.html.
[4]　河南省应急管理厅. 许昌市应急指挥部组织开展“四位一体”应急保通实战练兵活动[EB/OL]. [2025-07-10]. https://yjglt.henan.gov.cn/2025/04-03/3144464.html.
[5]　工业和信息化部等十四部门. 关于加强极端场景应急通信能力建设的意见[EB/OL]. [2025-07-10]. https://www. gov. cn/zhengce/zhengceku/202501/content_7000295.htm.
[6]　邓涛，张晓军，贾昆，等. 5G定制网应急通信保障解决方案[J]. 长江信息通信，2023，36(5)：211-214.
[7]　中国民航网. 海南空管分局全面升级应急通信保障体系[EB/OL]. [2025-07-10]. http://www. caacnews. com. cn/1/3/202505/t20250515_1387347.html.
[8]　中国电信集团. “汛”练有“速”！安徽公司打好防汛备汛“主动仗”[EB/OL]. [2025-07-10]. http://www.chinatelecom.com.cn/news/03/202505/t20250527_88015.html.
[9]　吕智勇. 6G网络中的卫星通信[J]. 数字通信世界，2020(1)：27-28.
[10]　黄韬，霍如，刘江，等. 未来网络发展趋势与展望[J]. 中国科学(信息科学)，2019，49(8)：941-948.
[11]　中国集群通信网. 极端环境下，如何保障受灾区域与外界通讯？[EB/OL]. [2025-07-10]. https://pttcn. net/plus/m_view. php? aid=33868.
[12]　马爱平. 三项首创为极端灾害场景筑起“防护墙”[EB/OL]. [2025-07-10]. https://www. stdaily. com/Web/gdxw/2025-07/02/content_363811.html.
[13]　董建坤，邢以群，张大亮. 备而有用，用而有备：应急管理的“平战结合”模式研究[J]. 中国应急管理科学，2020(12)：37-47.
[14]　王宏伟. 公共危机管理中的平战结合——应急与应战的一体化[J]. 军事经济研究，2007，28(8)：44-47.
[15]　田文华，赵岩. 超大型城市公共卫生治理“平战结合”的概念模型及其机制研究[J]. 上海交通大学学报(哲学社会科学版)，2022，

作者简介：
胡悦，毕业于西安电子科技大学，高级工程师，硕士，主要从事5G核心网络及业务研究、天地一体化新技术跟踪及创新业务产品研究工作；刘怡，毕业于重庆邮电大学，工程师，主要从事5G网络能力开放、天地一体化新技术、智能客服大模型及创新业务产品研究工作；何建炜，毕业于天津科技大学，高级工程师，硕士，主要从事卫星通信导航遥感一体化研究、天地一体化新技术跟踪及创新业务产品研究工作；朱斌，毕业于北京邮电大学，高级工程师，硕士，主要从事5G网络及能力开放研究、天地一体化新技术跟踪及创新业务产品研究工作。