



XXXX

基于MWAB组网的低空智联通信网端到端安全研究与验证

白景鹏¹, 薄明霞², 沈军¹

(1. 中国电信研究院, 广东 广州 510000;

2. 中国电信股份有限公司, 北京 100000)

摘 要: 3GPP Release 19定义的支持无线接入回传的移动性基站(本文称为MWAB)具有动态部署、精准覆盖、高度集成的特性,支持与低空飞行器一体化部署,在传统地面蜂窝网络和天基卫星网络的基础上,面向低空域层构建机动性、标准化、低成本的通信网络。但MWAB设备在网络边缘移动部署,物理环境开放可达,易遭受攻击劫持和非法使用,安全风险由边缘网络渗透至核心网络,而现有低空智联通信网络架构的安全能力难以阻断安全渗透威胁。本文针对低空智联通信网络架构开展端到端脆弱性、攻击威胁及安全风险分析,提出了以三道安全防线为思路、三级协同安全监测能力为关键技术的端到端安全方案,通过现网和实验室环境协同测试充分验证了安全方案的有效性和可推广性,并提出标准化推进思路。

关键词: 纵深防御; 网络安全; 低空智联网

中图分类号: TN929.5

文献标志码: A

doi: 10.11959/j.issn.1000-0801.

Research and Validation on the E2E Security of Low-altitude Intelligent Connected Communication Networks Based on Mobile Wireless Access Backhaul node

BAI Jingpeng¹, BO Mingxia², SHEN Jun¹

1. China Telecom Research Institute, Guangzhou 510630, China

2. China Telecom, Beijing 100000, China

Abstract: The Mobile Base Station supporting wireless Access Backhaul defined in 3GPP Release 19 (referred to as MWAB in this paper) is an NG-RAN node composed of User Equipment (MWAB - UE) and Base Station Equipment (MWAB - gNB). It features dynamic deployment, precise coverage, and high - level integration. Based on traditional terrestrial cellular networks and satellite-based networks, it supports the construction of a mobile, standardized, and low-cost communication network for the low-altitude domain layer. However, MWAB nodes are deployed at the edge

收稿日期: 2026-02-09; 修回日期: 2026-03-19

通信作者: 白景鹏, baijp@chinatelecom.cn

基金项目: 移动信息网络国家科技重大专项(2025ZD1301500)

Foundation Items: Mobile Information Networks-National Science and Technology Major Project (2025ZD1301500)



of the network and are exposed to an open physical environment, making them vulnerable to attacks, hijacking, and illegal use. Security risks can penetrate from the edge network to the core network, and the security capabilities of the existing low-altitude communication network architecture are difficult to prevent security threats. This report conducts an E2E vulnerability, attack threats, and security risk analysis of the low-altitude intelligent connected communication network. An E2E security solution is proposed, which takes three security lines of defense as the concept and three-level collaborative security monitoring capabilities as the key technology. The effectiveness and scalability of the security solution are fully validated through coordinated testing in the live network and laboratory environments. Also, ideas for promoting standardization are put forward.

Key words: Defense-in-Depth, Network Security, Low-altitude Intelligent Connected Communication Networks

0 引言

随着移动通信、卫星互联、无人飞行器技术快速发展与交叉融合,低空经济已渗透至经济生产、城市治理、应急保障等多领域,低空智联网作为核心支撑基础设施,其安全稳定运行成为关键挑战^[1]。低空智联网包括通信网、感知网、导航网、气象网和算力网,为低空1000米以下空域应用提供“通、监、导、气、算”一体化服务的综合网络体系^[2]。其中,低空智联通信网络是低空智联网的核心组成部分,聚焦通信能力构建,涵盖地面蜂窝、天基卫星及低空移动节点的通信链路。

当前业界研究的低空智联通信网络主要包括低空网络、地面网络和卫星网络三部分^[4-5],其中在150-600米低空域层存在覆盖成本高、灵活性不足等问题^{[1][3]},而3GPP Release 19定义的移动性无线接入回传节点(MWAB, Mobile Wireless Access Backhaul)技术凭借其灵活组网特性,可快速填补覆盖盲区,适配临时性、移动性通信需求。但MWAB设备边缘部署的物理开放性、多域协同的网络复杂性,使其面临独特安全风险,而现有安全方案仅关注空口安全,缺乏端到端网络安全防护手段。基于此,本文聚焦MWAB组网的低空智联通信网安全问题,开展风险分析、方案设计与验证,为低空经济安全发展提供支撑。

1 研究进展

1.1 基于MWAB技术的低空智联通信网架构

3GPP TS 23.501^[6]定义了支持MWAB特性的5G系统架构,如图1所示。其中,MWAB作为NG-RAN节点之一,由MWAB-UE(Mobile Wireless Access Backhaul User Equipment)组件和MWAB-gNB(Mobile Wireless Access Backhaul gNode B)组件构成,MWAB-UE通过NR Uu协议和PDU会话,为MWAB-gNB与5G网络中的实体(如AMF、UPF、其他gNB及OAM服务器)之间提供IP连接承载回程链路(Backhaul link)。MWAB-UE提供的IP连接既可通过MWAB-gNB服务的同一PLMN/SNPN实现,也可通过不同的PLMN/SNPN建立,可以基于实际场景需求采用不同的部署和组网方案,机动性构建低空通信网络,与地面网络、卫星网络形成一体化协同组网模式。

MWAB-gNB具备3GPP TS 38.300^[7]和TS 38.401^[8]标准规定的完整的gNB功能实现,可安装于移动车辆、低空飞行器上,能够为车辆内外的UE、低空飞行器自身、低空飞行器邻近范围内的多类型终端设备提供蜂窝网络服务。此外,MWAB节点自身具备移动性、实时回传等特点,还能够提供跟踪式、临时性扩展覆盖能力。基于MWAB节点接入回传一体化的组网能力,具有动态部署、精准覆盖、高度集成的特性,支持在传

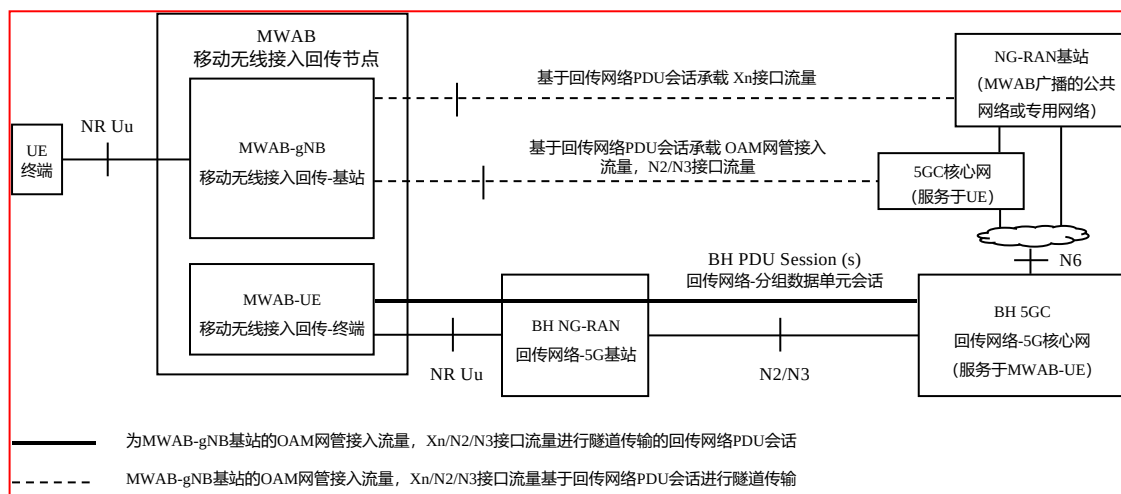


图1 支持移动性基站(MWAB)特性的5G系统架构

统地面蜂窝网络和天基卫星网络的基础上，面向低空域层构建机动性、标准化、低成本的通信网络，可分为3种典型组网方式。

1) 组网方式1：基于“地面蜂窝网络+MWAB接入回传一体”

MWAB设备可部署于低空飞行器（无人机、eVTOL），采用“地面蜂窝网络+MWAB接入回传一体”的组网方式（图2），MWAB-UE通过NR Uu协议与地面网络建立IP连接，为MWAB-gNB与5GC、其他gNB的稳定通信提供回程链路。MWAB-gNB可同时为飞行器自身、周边多类型终端（如巡检设备、物流传感器）提供网络服务。这种组网方式能够适配应急救援、郊区传感采集、郊区物流与巡检等应用场景。

2) 组网方式2：基于“天基卫星网络+MWAB接入回传一体”

MWAB设备可部署于低空飞行器（无人机、eVTOL），采用“天基卫星网络+MWAB接入回传一体”的组网方式（图3），MWAB-UE通过NR Uu协议接入天基卫星网络，并通过馈电链路和信关站与地面核心网建立IP连接，为MWAB-gNB与地面/星载核心网、其他gNB的稳定通信提供回程链路。

MWAB-gNB可同时为飞行器自身、周边多类型终端（如救援设备、移动终端、无人机）提供网络服务。这种组网方式支持通过MWAB将卫星接入与回传能力转换为蜂窝网络扩展覆盖能力，接入MWAB-gNB的终端无需支持卫星互联网协议，能够适配应急通信、海上运输、山区搜救等应用场景。

3) 组网方式3：基于“地面蜂窝网络+天基卫星网络+MWAB接入回传一体”

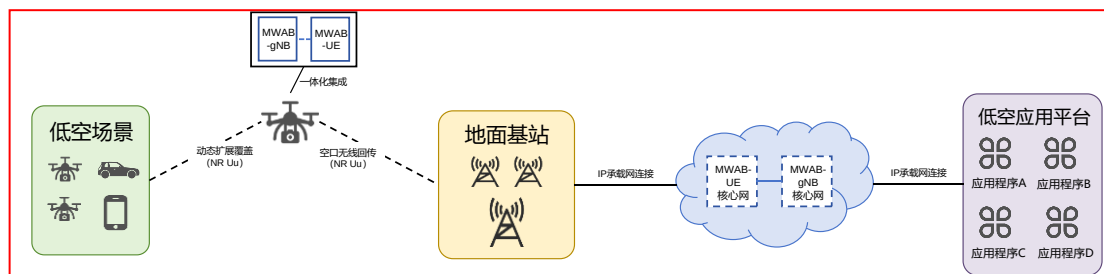


图2 基于“地面蜂窝网络+MWAB接入回传一体”的低空通信组网方式

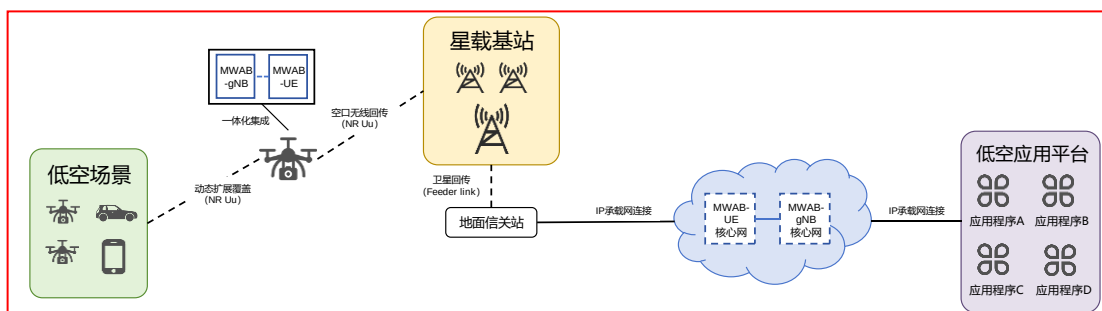


图3 基于“天基卫星网络+MWAB接入回传一体”的低空通信组网方式

MWAB 设备可部署于低空飞行器（无人机、eVTOL），采用“地面蜂窝网络+天基卫星网络+MWAB接入回传一体”的组网方式（图4），是组网方式1和2的融合组网。MWAB-UE可采用双接入的方式，通过NR Uu协议同时接入地面蜂窝网络和天基卫星网络，为MWAB-gNB与地面/星载核心网、其他gNB的稳定通信提供回程链路。此外，MWAB-UE也可以采用单一接入的方式，基于不同的移动性策略在接入地面蜂窝网络和天基卫星网络等两种接入方式之间切换^[9]。

1.2 低空智联通信网安全技术研究现状

构建安全防护体系是保障低空智联通信网稳定运行的关键要素。相关研究表明，无人机等低空飞行器作为低空经济核心终端载体^[10]，其主机系统面临攻击面多、资源受限、安全机制薄弱等问题^[11]，针对低空智联网的攻击呈现跨域渗透化（空天地跨层渗透）、目标战略化（重点针对关键基础设施）等趋势^[4]。基于MWAB的低空通信组网方式在实现空地协同覆盖的同时，也面临攻击

威胁由边缘网络渗透至核心网络的安全风险。现有的低空智联网安全技术研究主要聚焦在安全体系架构梳理，针对通信网络层安全分析仅关注无线电干扰、中间人攻击、重放攻击等空口安全威胁^[8-9]，缺少对端到端网络域的安全风险分析和跨域渗透攻击防护能力研究。

3GPP Release 20 阶段，TR 33.724^[14]研究了支持MWAB功能的5G网络安全架构与安全需求、潜在被攻破的MWAB节点的安全影响，以及针对任何被攻破的MWAB节点的防御措施要求，包括信令面、数据面和管理面的回传接口安全，以及MWAB节点安全检测与防护。本文的第二章将针对基于MWAB的低空通信网络进行端到端风险分析，聚焦接入域、回传域、核心域、管理平台域等网络域，第三章将基于风险分析提出安全防护体系与关键能力，第四章将针对端到端安全能力进行现网和实验室协同的测试验证，第五章将基于测试验证效果，提出3GPP、ITU-T安全标准化推进思路。

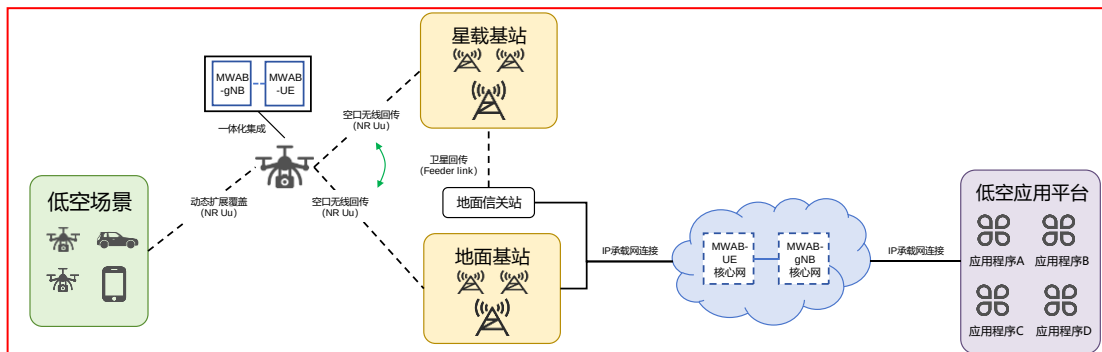


图4 基于“地面蜂窝网络+天基卫星网络+MWAB接入回传一体”的低空通信组网方式

2 端到端安全风险分析

2.1 脆弱性分析

基于网络架构，将从MWAB设备、回程网络（接入网络）、核心网、网管系统等四个部分对基于MWAB的低空通信网络进行端到端脆弱性分析，如图5所示。

1) MWAB设备自身的脆弱性

- 硬件方面：与传统基站设备部署在运营商机房、机柜内不同，MWAB设备部署在不受运营商控制的物理开放环境区域，且在低空场景下具体移动性特点，易遭物理破坏、仿冒、入侵控制和劫持；部分低成本、白盒化MWAB设备的固件容易携带未修复开源漏洞。

- 软件方面：普遍存在弱口令、明文存储敏感信息、软件包完整性校验算法不安全等弱安全配置，容易被破解。

2) 回程网络（接入网络）的脆弱性

- 网络层面：与传统基站设备采用运营商配置的专用IP承载不同，由于大规模MWAB设备处于低空移动状态，灵活采用基于IP连接的地面回传网络和/或卫星回传网络等公共网络接入核心网与网管系统，缺乏安全隔离手段，无法配置访问控制策略，导致核心网、网管系统暴露面增大。

3) 核心网侧的脆弱性

- 网络层面：因公网IP引入暴露面，而且未划分独立DMZ区，在回程网络与核心网络之间

缺乏安全防护缓冲区，安全隔离与监测手段不足。核心网侧未针对MWAB设备回传的低空应用流量实施细粒度的访问控制策略。

- 软件方面：核心网自身安全主要依赖核心网安全域入口的边界防护能力，核心网内部网元层面的安全隔离与监测手段不足。

4) 网管系统侧的脆弱性

- 网络层面：因公网IP引入暴露面，而且未划分独立DMZ区，在回程网络与网管系统之间缺乏安全防护缓冲区，安全隔离与监测手段不足。网管系统侧对MWAB设备回传的流量缺乏细粒度的访问控制策略。

当MWAB-UE和MWAB-gNB属于同一PLMN/SNPN时，上述分析的核心网侧脆弱性指的是MWAB-UE和MWAB-gNB共同归属的核心网。当MWAB-UE和MWAB-gNB属于不同的PLMN/SNPN时，上述分析的核心网侧脆弱性指的是MWAB-gNB归属的核心网。

2.2 攻击威胁分析

基于端到端脆弱性分析结果，对基于MWAB的低空通信网络开展安全威胁分析。基于MWAB的低空通信网络安全威胁的来源主要来自两大方面，一是来自MWAB设备侧的攻击，二是来自公共网络的攻击，如图6所示。针对这两种威胁来源，分析其攻击路径。

1) 来自MWAB设备侧的攻击路径：□ 控制MWAB设备—>通过回程网络渗透至内网—>入侵核心网、低空网络管理平台，此类攻击可结合

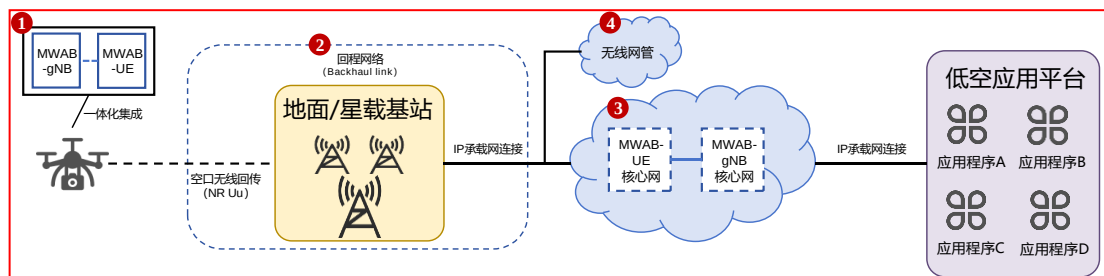


图5 基于MWAB的低空通信网络的脆弱性分布点

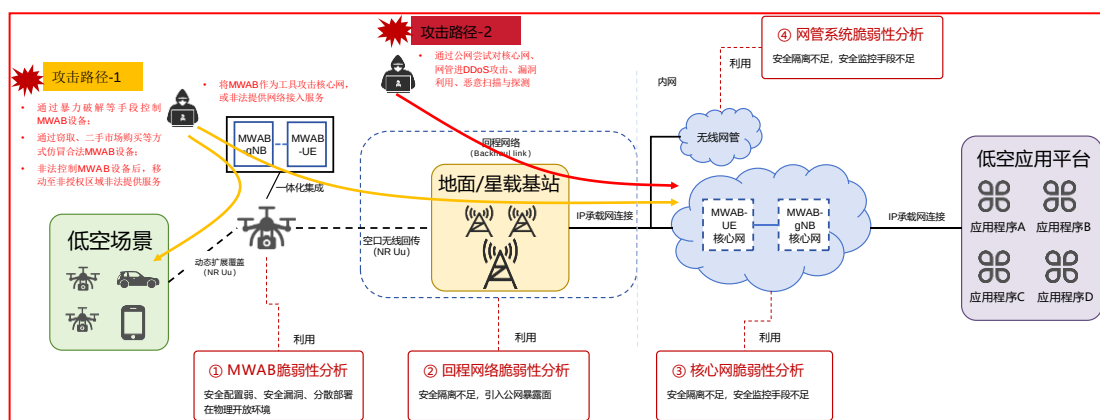


图6 基于MWAB的低空通信网络安全威胁与攻击路径

低空移动、数据采集跨域回传特性，伪装合法节点规避边界检测，发送异常低空应用流量进行渗透攻击；□ 控制MWAB设备—>移动至非授权区域^[13]—>非法提供网络接入、通感服务，或干扰低空智联网的无人机集群定位信号、篡改低空应用数据、实施非法监听，利用低空智联网“通监/感一体化”特性扩大攻击影响，导致空域安全管控失效。

2) 来自公共网络的攻击路径：定位暴露的核心网、网管系统—>利用漏洞入侵核心网、网管系统—>以边界网元为跳板渗透内网的核心网、低空网络管理平台，此类攻击可利用MWAB多域接入回传的特性，通过地面、卫星网络等多链路发起协同攻击。

2.3 安全风险分析

基于以上脆弱性分析、安全威胁分析，对基

于MWAB的低空通信网络关键节点进行风险分析，关键节点威胁利用相应脆弱性导致的安全风险的对应关系如表1所示。

1) MWAB设备被控制（低风险）

MWAB设备位于网络末端，因硬件、软件及管理上的脆弱性，攻击难度低、被控几率较高，其被控制后对局部低空通信服务的中断、干扰，但不足以对整个网络造成重大影响，整体造成的风险为低水平。

2) 非法提供网络接入服务（中风险）

MWAB设备具备移动性特征，一旦被入侵控制，攻击者可能控制MWAB设备移动至非授权区域提供低空通信服务，可能导致局部区域低空应用相关的敏感信息泄露、非法内容传播、终端非法追踪，对网络安全构成较大威胁，整体造成的风险为中水平。

表1 关键节点威胁利用相应脆弱性导致的安全风险的对应关系

关键节点	脆弱性	主要威胁 (攻击复杂度)	影响程度	风险 等级	CVSS 评分
MWAB设备	硬件固件漏洞 弱安全配置 分散部署在物理开放环境，具备移动性，采用公网回传	控制、仿冒合法MWAB设备，攻击复杂度低	MWAB设备被控制，局部通信中断，无敏感数据泄露	低	0.1-3.9
		劫持并非法移动MWAB设备，攻击复杂度中	非法提供网络接入服务，区域业务受扰，部分敏感数据泄露	中	4.0-6.9
		通过MWAB设备的合法隧道渗透攻击内部网络，攻击复杂度高	核心网、低空网络管理平台被控制，核心数据泄露、全网服务瘫痪	高	7.0-10.0
核心网/网管系统	公网暴露面 安全隔离不足 安全监测手段不完善	利用地面/卫星网络回传引入的公网暴露面，恶意嗅探内部网络，从而入侵，攻击复杂度高	核心网、低空网络管理平台被控制，核心数据泄露、全网服务瘫痪	高	7.0-10.0

3) 核心网/网管系统被控制（高风险）

由于 MWAB 设备、回程网络以及核心网/网管潜在的脆弱性问题，攻击者可能通过控制 MWAB 设备作为跳板逐步渗透最终控制核心网或网管系统，尽管攻击难度大，但成功后可能引发大规模低空通信服务中断、低空应用用户隐私泄露和通信数据篡改，导致空域、地域通信管控失效，对网络稳定和用户数据安全构成极大威胁，整体造成的风险为高水平。

3 端到端安全防护体系

3.1 防护思路：基于安全网关的三道安全防线

现有低空智联通信网络安全架构研究主要聚焦在以下几个方面的安全能力构建：□ 低空通信网络终端接入身份认证、抗 DoS 防御^{[4][11]}；□ 低空通信网络轻量化密码算法与公钥基础设施^[11]；□ AI 大模型赋能低空物联网安全^{[4][12]}。这些安全能力能够有效解决低空终端合法性状态监控、低空网络通信链路安全保护、AI 赋能低空通信安全等安全需求，但缺乏对低空通信网络接入回传节点（如 MWAB 设备、终端设备）“设备层面+流量层面”安全风险的有效感知和综合研判能力，无法感知分散在网络边缘的 MWAB 设备、存在公网暴露面的边界网关的安全状态，难以防范攻击者基于低空接入回传节点的合法通信链接发起的跨域渗透攻击，因此有必要提升基于 MWAB 的低空通信网络的精准安全监测与防护能力。

基于低空智联通信网络架构的特点，根据分层解耦、全域覆盖的原则，引入安全网关作为安全隔离与异常监测能力的关键节点，部署在 MWAB-gNB 归属核心网的边界入口 DMZ 区处，MWAB-gNB 基于 MWAB-UE 提供的 IP 连接与安全网关进行双向认证、建立 IPSec 隧道。以安全网关所在的 DMZ 区作为安全锚点划分三道安全防线，如图 7 所示。

1) 第一道防线：MWAB 设备到网关所在 DMZ 区入口边界。防止非法控制 MWAB 设备，确保 MWAB 设备和边界网关之间的安全通信。

- MWAB 设备安全：基于轻量化安全监测能力，保护 MWAB 设备免受物理攻击、暴力破解、未授权访问、非法劫持移动等威胁。

- 回程网络（接入网络）安全：基于 NDS/IP 安全机制，边界安全网关对 MWAB 设备进行合法性验证，并确保 MWAB 设备与边界安全网关之间的通信安全，防止数据泄露或篡改。

2) 第二道防线：网关所在 DMZ 区入口到出口。确保关卡作用，收敛公网暴露面，前置安全监测和防护，防止非法流量进入内网。

- 边界网关安全：基于轻量化安全监测能力，保护网关设备安全，防止外部攻击渗透到内部网络。

- DMZ 区安全：基于安全网关划分安全域，在网关与内网之间设置隔离区，收敛公网暴露面，防范通过控制 MWAB 设备发起基于协议栈

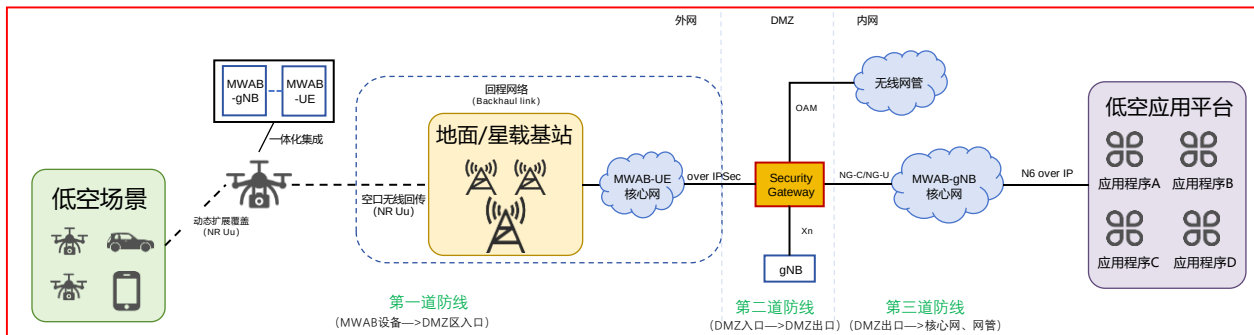


图7 基于MWAB的低空通信网络的三道安全防线



的异常流量攻击，防止外部攻击直接进入核心网络。

3) 第三道防线：DMZ 区出口边界到核心网、网管边界。防止通过 MWAB 边缘网络攻击威胁渗透到内网，保护核心网和网管系统安全。

- 网管域安全：加强访问控制安全，保护网管系统，防止未授权访问和恶意操作。集中监测 MWAB 设备、边界网关安全状态及风险告警。

- 核心网域安全：加强访问控制安全，确保核心网关键信息基础设施的安全，防止关键数据和服务受到攻击。

基于三道安全防线思路形成端到端安全能力体系，共 21 项安全能力，包括：MWAB 设备安全、接入网安全、边界网关安全、DMZ 安全、网管侧安全、核心网侧安全等六个安全面，以及设备安全、接入安全、网络安全、信令安全、管理安全等五个安全分层，如图 8 所示。

3.2 防护体系：三级协同安全监测

针对攻击链特点分析，在三道安全防线和端到端安全能力体系的基础上，基于 NDS/IP 安全

机制、异常流量检测、设备安全状态监测等 3 项关键技术，构建覆盖边缘接入域、边界网关域、核心网络域的分级协同安全监测与防护体系，如图 9 所示。

1) NDS/IP 安全机制

基于 3GPP TS 33.210^[15]定义的 NDS/IP (Network Domain Security/IP layer security，网络域安全/IP 层安全机制)，为属于不同安全域的 MWAB 设备和安全网关提供基于合法证书或 USIM 的双向认证机制，基于认证结果建立 IPSec 隧道进行密钥协商、更新和维护，对应端到端安全能力体系中第一道、第二道安全防线的安全能力 2、3、7、8、14、15，保障 MWAB 设备回传通信安全。MWAB 设备和安全网关之间传输的：□ 信令面：NG-C 接口信令、Xn 接口信令，□ 数据面：NG-U 接口流量，□ 管理面：OAM 接口流量均通过 IPSec 隧道进行基于 ESP 模式的传输保护，能够防范针对 MWAB 设备回传接口的仿冒、窃听和篡改攻击。

2) 异常流量检测

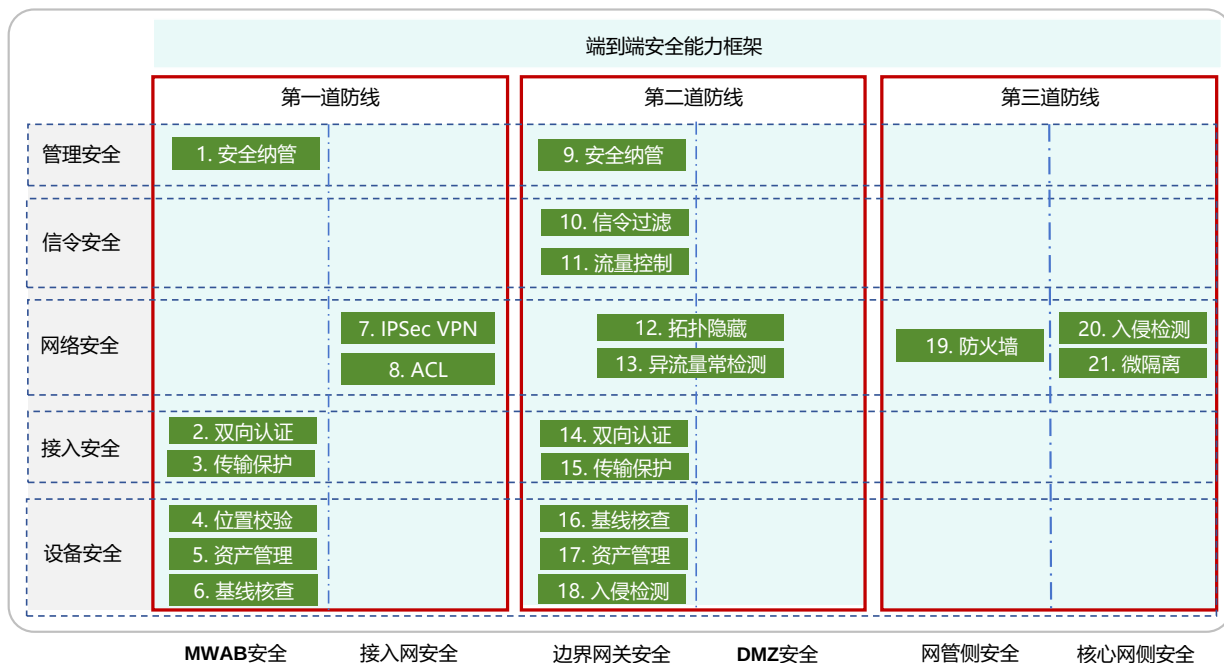


图 8 端到端安全能力体系

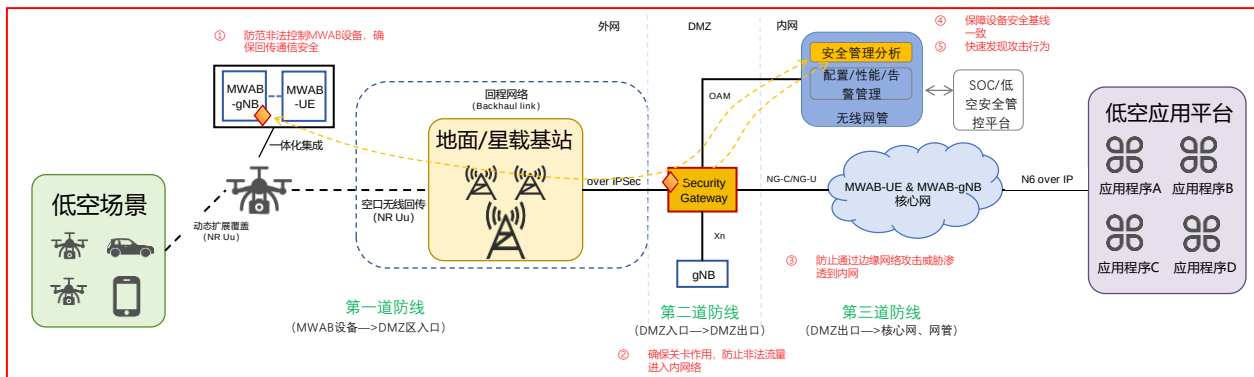


图9 分级协同的安全监测与防护系统

针对 MWAB 设备回传接口的全栈协议特征，包括信令面的 NG-C 和 Xn 接口协议、数据面的 NG-U 接口协议、管理面的 HTTP/TLS/IPSec 接口协议，在 3GPP TS 33.210^[15] 定义的安全网关（SEG，Security Gateway）的基础上增强异常流量检测能力，对应端到端安全能力体系中第二道安全防线的安全能力 10、11、12、13，实现以下防护能力：□ 拓扑隐藏，通过信令代理和地址转换功能对 MWAB 设备隐藏内网拓扑，包括信令面、数据面和管理面；□ 细粒度访问控制（信令过滤），例如基于 NG-C 接口限制 MWAB 设备仅能访问 AMF 网元或特定的 AMF 网元；□ 异常流量拦截，对 IPSec 隧道内的异常协议、泛洪攻击的快速识别与拦截，阻断攻击向核心网渗透。

3) 设备安全状态监测

•MWAB 设备侧安全监测

通过在 MWAB 设备内置或升级支持轻量化安全组件，解决物理暴露场景下资源受限设备的低开销数据采集问题，实现 MWAB 设备安全状态实时监测，对应端到端安全能力体系中第一道安全防线的安全能力 4、5、6，包括资产指纹数据采集与分析、安全配置信息采集与分析、位置合法性校验（基于 IP 地址+设备地理位置+接入回传时延），还可以包括最小化主机入侵数据采集与分析，比如针对暴力破解攻击的检测与告警，防范针对边缘 MWAB 设备的入侵攻击、非法劫

持攻击。

•边界网关侧安全监测

通过在边界安全网关设备内置或升级支持轻量化安全组件，发现并防范来自边缘、公网对安全网关的渗透攻击行为，实现网关设备安全状态实时感知，对应端到端安全能力体系中第二道安全防线的安全能力 16、17、18，包括资产指纹数据采集与分析、安全配置信息采集与分析、主机入侵行为数据采集与分析。

•无线网管侧安全管理分析

通过在无线网管升级支持安全管理分析功能，对部署在 MWAB 设备、边界安全网关内的轻量化安全组件进行安全纳管，对应端到端安全能力体系中第三道的安全能力 1、9。无线网管整合 MWAB 设备安全状态、边界网关安全状态及异常流量检测日志等多源数据，构建跨层级威胁链分析模型，形成基于 IPSec 隧道的信令面、数据面、管理面协议攻击的安全防护策略，支持在无线网管集中监测 MWAB 设备、边界网关安全状态及风险告警，并按需通过安全能力开放接口上报给上级 SOC 平台或低空应用安全管控平台，实现低空通信网络“事前、事中、事后”安全可视、可管控。

此外，还需在网管侧防火墙部署针对 MWAB 设备回传的管理面流量的细粒度访问控制策略，在核心网侧针对 AMF、UPF 等与 MWAB 设备通



信的网元升级支持入侵检测、微隔离等安全能力。

4 端到端安全能力验证

端到端安全能力验证的目标是测试基于MWAB的低空通信网络三道防线、安全能力方案的有效性、可行性与可复制性，评估安全能力方案的功能、性能指标。

4.1 验证测试方案

验证测试环境包括现网环境与实验室环境，共同开展协同测试。实验室测试通过模拟攻击的方式验证安全能力有效性，现网测试侧重于验证安全能力的稳定性。实验室模拟攻击测试包括三个部分：攻击被测MWAB设备、攻击被测安全网关、利用被控MWAB设备攻击内网，攻击示意图如图10所示，实验室测试设备和系统信息如

表2所示。

1) 攻击被测MWAB设备：在MWAB设备侧模拟弱配置、非法劫持移动设备等风险操作，模拟攻击者利用弱配置对MWAB设备进行入侵控制，同步在无线网管监测被攻击MWAB设备的安全状态及风险项告警。

2) 攻击被测安全网关：在边界安全网关侧模拟弱配置等风险操作、主机入侵攻击行为，在无线网管监测被攻击安全网关的安全状态及风险项告警。

3) 利用被控MWAB设备攻击内网：□ 在MWAB设备侧模拟发送超过阈值的流量，在安全网关侧监测MWAB设备速率并验证熔断机制；□ 在MWAB设备侧利用工具、仪表，模拟信令、数据、管理面协议栈的异常流量攻击，封装在IPSec隧道向安全网关发送，在无线网管查看安

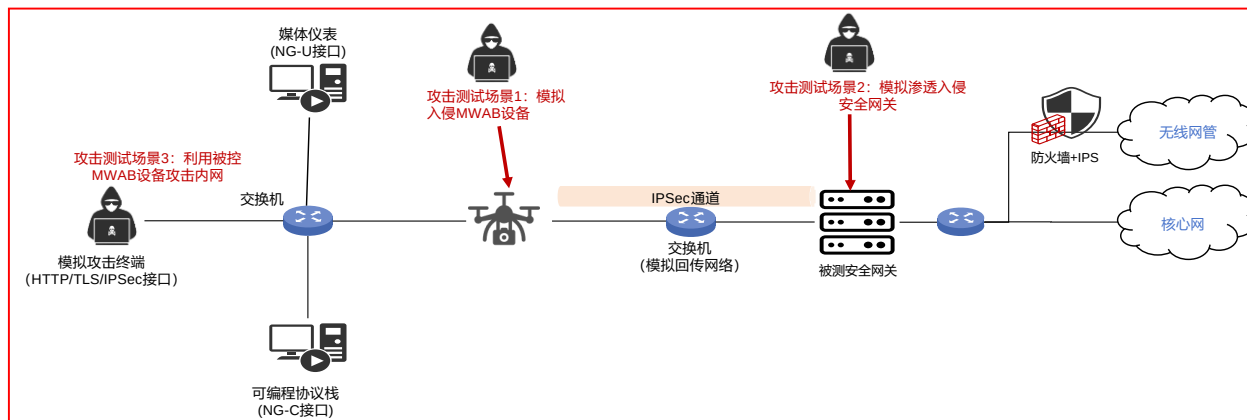


图10 模拟攻击测试逻辑架构图

表2 实验室测试设备和系统信息

设备/环境/工具	厂家	数量	型号/版本/作用
N3接口仪表	厂家C	1	•dotouch xpro-ns v5.1.1
N2接口仪表	厂家C	1	•dotouch xproFlexStack 2.0.0
模拟攻击终端	自编程工具	1	•生成异常HTTP/TLS/IPSec流量
MWAB设备	厂家A	1	•设备型号：CTIBS5421
接入网络交换机	厂家B	1	•设备型号：H3C S6520X-54QC-EI
边界安全网关	厂家A	1	•设备型号：CTAGW5000
模拟攻击工具	自编程工具	1	•发起hydra（暴力破解），MobaXterm（非法下载，webshell上传，异常登录）
DMZ区防火墙	厂家B	1	•设备型号：H3C T5000
无线网管	厂家A	1	•版本：V5.3.9

全网关的安全日志告警，抓包分析异常流量检测和拦截机制。

4.2 验证测试结果

攻击测试场景1（攻击被测MWAB设备）针对MWAB设备的3个攻击环节进行了14项风险操作测试，验证MWAB设备轻量化安全监测能力支持在网管集中监测MWAB设备安全状态及风险告警，包括支持13类资产指纹数据采集与异常识别（含位置合法性校验）、支持13项安全弱配置检查及风险提示，安全组件运行时对MWAB设备的CPU占比0.9%、内存占用25.83M、带宽占用率1.3%，对低空应用业务的资源占用影响低，如表3所示。

攻击测试场景2（攻击被测安全网关）针对安全网关进行风险操作、入侵攻击测试，验证安全网关轻量化安全监测能力支持在网管集中监测安全网关安全状态及风险告警，包括支持13类资产指纹数据采集与异常识别、支持13项安全弱配

置检查及风险提示、支持10类系统入侵攻击检测与告警，安全组件运行时对MWAB设备的CPU占比0.29%、内存占用28.71MB、带宽占用率1.75%，对低空应用业务的资源占用影响低，如表4所示。

攻击测试场景3（利用被控MWAB设备攻击内网）控制MWAB设备向核心网、网管系统发送异常攻击流量进行测试，验证安全网关支持5类异常流量拦截，覆盖信令、数据、管理面协议栈。其中，控制面、管理面异常流量拦截响应平均时延为50~95ms，如表5所示。

4.3 验证效果分析

1) 有效性验证

基于对MWAB低空通信网络端到端脆弱性的分析，梳理24类典型攻击及安全风险，并在验证测试过程中模拟24类攻击威胁，验证三道安全防线、分级协同安全监测能力的防护效果，端到端安全能力部署前仅能够防护3类攻击威胁，端

表3 攻击测试场景1的安全能力测试结果

模拟攻击威胁	测试分类	验证安全能力项	功能、性能指标
非法入侵控制、仿冒合法MWAB设备	验证MWAB设备登录环节风险点检测覆盖：共测试7项风险操作	- 资产识别与弱配置检查 - 口令长度配置 - 口令复杂度配置 - 口令过期时间配置 - 限制用户su到root配置 - 限制SSH登录失败重试次数 - 限制root用户远程登录 - 使用SSH协议进行远程维护	- 功能：支持在网管集中监测MWAB设备安全状态及风险告警，包括13类资产指纹采集与异常识别、13项安全弱配置检查及风险提示 - 性能：支持资源占有率上限配置，现网运行时，安全组件资源占用低，CPU：0.9%、内存：25.83M、带宽：1.3%
	验证尝试获取MWAB设备控制权环节的风险点检测覆盖：共测试4项风险操作	- 资产识别与弱配置检查 - 配置用户最小授权 - 配置文件与目录缺省权限控制 - 删除或锁定无关账号 - 建立多账号组，分配不同权限	
	验证控制MWAB设备后实施违规操作风险点检测覆盖：共测试4项风险操作	- 资产识别与弱配置检查 - 关闭不必要的服务和端口 - 启用Syslog日志审计 - 配置日志文件安全权限 - 基于“IP地址+地理位置+时延”的合法性校验	



表4 攻击测试场景2的安全能力测试结果

模拟攻击威胁	测试分类	验证安全能力项	功能、性能指标
通过MWAB设备或公网暴露面对网关设备尝试远程入侵	验证安全网关登录环节风险点检测覆盖：共测试7项风险操作	•资产识别与弱配置检查 •口令长度配置 •口令复杂度配置 •口令过期时间配置 •限制用户su到root配置 •限制SSH登录失败重试次数 •限制root用户远程登录 •使用SSH协议进行远程维护	•功能：支持在网管集中监测MWAB设备网关安全状态及风险告警，包括13类资产指纹采集与异常识别、13项安全弱配置检查及风险提示、10类系统入侵攻击检测与告警，以及访问控制、安全隔离等策略下发 •性能：支持资源占有率上限配置，现网运行时，安全组件CPU占用率为0.29%，内存占用为28.71 MB、带宽：1.75%
	验证尝试获取安全网关控制权环节的风险点检测覆盖：共测试4项风险操作	•资产识别与弱配置检查 •配置用户最小授权 •配置文件与目录缺省权限控制 •删除或锁定无关账号 •建立多账号组，分配不同权限	
	验证控制网关后实施违规操作风险点检测覆盖：共测试3项风险操作	•资产识别与弱配置检查 •关闭不必要的服务和端口 •启用Syslog日志审计 •配置日志文件安全权限	
	验证对“尝试登录-尝试获取控制权-控制网关后实施恶意行为-攻击成功后反取证操作”四个攻击环节常见攻击行为特征的检测效果，及时发现可疑入侵行为	•主机入侵行为检测 •暴力破解攻击检测 •非法登录攻击检测 •账号权限提升攻击 •文件权限提升攻击检测 •关键文件篡改攻击检测 •反弹shell攻击检测 •webshell攻击检测 •非法文件下载攻击检测 •软连接后门检测 •非法新增用户检测	

到端安全能力部署后能够防护24类攻击威胁，如图11所示，支持在网管集中监测MWAB设备和边界网关的安全状态及风险告警，支持结合MWAB设备安全状态监测结果及MWAB设备回传异常流量检测结果，综合分析研判MWAB设备的安全风险等级，主动对异常MWAB设备进行

行注销下线、释放回传连接、合法追踪等安全响应操作，充分验证端到端安全能力体系在防范低空智联通信网络攻击威胁的优势。

2) 可行性与可推广性

在现网环境测试并试点运行过程中，覆盖MWAB设备、边界网关和无线网管平台等三级安

表5 攻击测试场景3的安全能力测试结果

模拟攻击威胁	测试分类	验证安全能力项	功能、性能指标
通过MWAB设备恶意嗅探内部网络，发送异常流量	使用仪表模拟信令面异常协议的消息包，通过IPSec隧道发送至核心网AMF网元	•信令面异常流量检测与拦截 •N2接口异常协议（重复/翻转字段、篡改长度等） •SI-C接口异常协议（重复/翻转字段、篡改长度等） •异常IKEv2协议交换消息（算法篡改、协商信息篡改） •异常泛洪、分片、TLS攻击包 •信令面ACL过滤 •信令面拓扑隐藏 •过载流量检测与熔断	•功能：支持5类异常协议流量拦截，覆盖信令、数据、管理面，以及访问控制、安全隔离、设备熔断等策略下发 •性能：信令面、管理面异常流量拦截响应平均时延为50~95ms
	使用仪表模拟数据面异常协议的消息包，通过IPSec隧道发送至核心网UPF网元	•数据面异常流量检测与拦截 •N3接口异常协议（篡改GTP flags、长度等） •SI-U接口异常协议（篡改GTP flags、长度等） •数据面ACL过滤 •数据面拓扑隐藏 •过载流量检测与熔断	
	使用仪表模拟管理面异常协议的消息包，通过IPSec隧道发送至网管系统	•管理面异常流量检测与拦截 •land攻击包 •Ping of Death攻击包 •Teardrop攻击包 •管理面ACL过滤 •管理面拓扑隐藏 •过载流量检测与熔断	

关键节点	脆弱性	面临威胁	安全风险	端到端能力部署前	端到端能力部署后	防护成效
MWAB设备	① 硬件固件漏洞 ② 弱安全配置 ③ 分散部署在物理开放环境	仿冒、入侵、控制合法MWAB设备	1. 利用非法设备替换合法MWAB设备实施仿冒攻击 2. 劫持边缘MWAB设备的回传网络接口实施仿冒攻击 3. 窃取合法MWAB设备的预共享密钥信息实施仿冒攻击 4. 利用MWAB设备的弱口令漏洞，尝试非法登录控制设备 5. 利用MWAB设备开放的不安全服务端口，通过暴力破解入侵系统 6. 通过网络嗅探工具截获明文存储/传输的账号口令等数据 7. 非法登录设备后，尝试通过提权安装、运行恶意软件实施攻击 8. 非法登录设备后，尝试通过删除日志执行反取证操作 9. 非法登录设备后，尝试非法移动设备至非授权区域提供低空应用服务	双向认证 传输保护 (MWAB设备<—>核心网网元)	双向认证 传输保护 (MWAB设备<—>边界安全网关)	1. 防范非法控制MWAB设备 • 支持13类资产指纹数据采集与异常识别 • 支持13项安全弱配置检查及风险提示
接入网络	① 公网暴露	通过公网暴露面对内网进行非法扫描、嗅探	10. 利用公网暴露面，非法扫描、嗅探边界安全网关的服务端口	难以防范	IPSec VPN、ACL	2. 形成3种组网模式下的接入网络暴露面收敛，确保MWAB设备与网关之间的安全通信
边界安全网关	① 公网暴露	通过MWAB设备或公网暴露面对网关设备尝试远程入侵或DoS攻击	11. 通过伪基站、接口劫持、鉴权信息窃取等手段仿冒MWAB设备向网关发起攻击 12. 利用MWAB设备的合法IPSec隧道，向网关发送异常IKE协议流量，实施DoS攻击 13. 利用MWAB设备的合法IPSec隧道，向网关发送异常管理面流量，实施DoS攻击 14. 利用安全网关的弱口令漏洞，尝试非法登录控制设备 15. 利用安全网关开放的不安全服务端口，尝试登录、暴力破解入侵系统 16. 非法安全网关设备后，尝试通过提权安装、运行恶意软件实施攻击 17. 非法安全网关设备后，尝试通过删除日志执行反取证操作，非法下载文件 18. 利用公网暴露面，尝试绕过安全网关，非法嗅探、访问、登录核心网网元	难以防范	双向认证 传输保护 异常流量检测、流量控制 资产管理、基础核查 入侵检测、安全纳管	1. 防范非法控制安全网关 • 支持13类资产指纹数据采集与异常识别 • 支持13项安全弱配置检查及风险提示 • 支持10类操作系统入侵行为检测
核心网	① 安全隔离不足 ② 安全监测不完善	通过MWAB设备或从公网恶意嗅探核心网络，实施入侵或DoS攻击	19. 利用MWAB设备的合法IPSec隧道，向核心网发送异常3GPP协议包实施渗透攻击 20. 利用MWAB设备的合法IPSec隧道，向核心网发送异常数据面流量实施渗透攻击 21. 非法控制网关设备后，向核心网发送异常消息包、流量包实施渗透或DoS攻击 22. 利用公网暴露面，尝试绕过网关，非法嗅探、访问、登录网管平台或其它系统 23. 利用MWAB设备的合法IPSec隧道，向网管发送异常管理面流量实施渗透攻击 24. 非法控制网关设备后，向网管发送异常消息包、流量包实施渗透或DoS攻击	难以防范	双向认证 传输保护 异常流量检测、流量控制 资产管理、基础核查 入侵检测、安全纳管 信令过滤、异常流量检测 流量控制 网元微隔离、入侵检测 拓扑隐藏、防火墙、VPN	2. 加强网关的关卡作用，前置安全监测与防护，防止非法流量进入内网 • 检测和拦截控制、用户、管理面异常流量 • 覆盖3GPP N2、N3接口协议，HTTP/TLS/IPSec协议
网管系统	① 安全隔离不足 ② 安全监测不完善	通过MWAB设备或从公网恶意嗅探核心网络，实施入侵或DoS攻击			异常流量检测	3. 形成3种组网模式下的DMZ区防护策略，防范攻击威胁渗透到内网

图11 端到端攻击威胁防护效果



全能力协同测试, 验证的端到端安全能力稳定运行30天以上, 覆盖视频回传、传感数据采集等典型低空应用场景, 包括业务闲时、忙时时段, 验证安全能力在不同业务负载环境下的稳定性。

5 标准化推进思路

基于端到端安全能力验证效果, 将分别在3GPP、ITU-T等国际标准组织推动基于MWAB的低空智联通信网络安全技术标准化。

面向3GPP Release20阶段的5G MWAB网络安全项目, 推动NDS/IP安全机制、异常流量检测、设备安全状态感知等安全方案写入TR 33.724^[14]及后续规范性文件。其中, 基于安全网关的NDS/IP安全机制、异常流量检测机制可用于解决TR 33.724^[14]的关键问题1: MWAB-gNB与OAM之间的管理面链路安全、关键问题3: MWAB节点的Xn、N2、N3接口安全、关键问题4: 回程链路承载的MWAB-gNB的信令安全保护, 基于分级协同安全监测的MWAB设备安全状态感知技术可用于解决TR 33.724^[14]的关键问题2: 受入侵的MWAB节点与核心网的安全保护措施。

面向ITU-T SG17的IMT-2020及未来网络安全项目, 推动基于安全网关的三道安全防线体系、三级协同安全监测架构成为低空智联通信网络的安全需求与实施指南, 不仅适用于本文提出的基于MWAB的低空智联通信网络, 也还适用于其它基于无线接入回传一体化技术、无线通感一体化技术构建的面向低空应用的移动通信网络。

6 结束语

本文针对基于MWAB组网的低空智联通信网络开展端到端脆弱性、攻击威胁及安全风险分析, 提出了以三道安全防线为思路、三级协同安全监测能力为关键技术端到端安全方案, 通过

现网和实验室环境协同测试充分验证了安全方案的有效性和可推广性, 并提出3GPP/ITU-T标准化推进思路。

随着5G-A新应用、新场景加速发展, 6G服务及网络架构标准化研究启动, 未来移动通信网络将涌现出越来越多的与MWAB技术类似的基于“无人飞行器+无线接入回传一体化/通感一体化节点”集成的低空智联通信组网架构。在推动低空智联通信架构创新、技术落地与应用实践的同时, 传统以被动防御思路为主的安全体系将不再适用, 需要向以“跨域纵深防御、主动防御”为核心理念的方向转变。不仅能够快速、灵活的根据业务需求提供网络扩展覆盖, 还能高效满足经济性、安全性等网络建设需求, 支撑低空经济高质量发展。

参考文献:

- [1] 中信科移动. 低空智联网络场景和关键技术[R]. 2025.
CICIT Mobile. Scenarios and Key Technologies of Low-Altitude Intelligent Network [R]. 2025.
- [2] 中国信息通信研究院. 低空智联网络发展研究报告(2024年)[R]. 2024.
CAICT. Research Report on the Development of Low-Altitude Intelligent Network (2024) [R]. 2024.
- [3] 曹阳阳, 高松涛, 于一鸣等. 低空覆盖组网技术方案[J]. 电信科学, 2026. CAO YY, GAO ST, YU YM et al. Low-Altitude Coverage Networking Technology Solution. Telecommunications Science, 2026.
- [4] 王云涛, 苏洲, 高源, 巴建乐. 低空智联网络架构、安全与优化关键技术[J]. 电子与信息学报, 2025,
WANG YT, SU Z, GAO Y, BA JL. Key Technologies for Low-Altitude Internet Networks: Architecture, Security, and Optimization[J]. Journal of Electronics & Information Technology, 2025.
- [5] 武燕燕, 吴松. 低轨卫星辅助的低空智联网络架构分析及设计[J]. 电信科学, 2025, 41(3): 27-37.
Wu Y Y, Wu S. Architecture analysis and design for low earth orbit satellite-assisted Low-Altitude Intelligent network[J]. Telecommunications Science, 2025, 41(3): 27-37.
- [6] 3GPP. System architecture for the 5G System (5GS); Stage 2: 3GPP TS 23.501 [S]. 2025.

- [7] 3GPP. NR; NR and NG-RAN Overall description; Stage-2: 3GPP TS 38.300 [S]. 2025.
- [8] 3GPP. NG-RAN; Architecture description: 3GPP TS 38.401 [S]. 2025.
- [9] 陈山枝. 关于低轨卫星通信的分析及我国的发展建议[J]. 电信科学, 2020, 36(6): 1-13.
CHEN SZ. Analysis of LEO satellite communication and suggestions for its development strategy in China[J]. Telecommunications science, 2020, 36(6): 1-13.
- [10] 陈鸿杰, 郭显甫, 吴凡等. 面向低空智联网的无人机网络切片资源管理机制研究[J]. 电信科学, 2025, 41(03): 38-51.
CHEN HJ, GUO YF, WU F, et al. Research on UAV network slicing resource management for low-altitude intelligent network[J]. Telecommunications Science, 2025, 41(03): 38-51.
- [11] 中国移动. 低空智能网联网络与数据安全体系白皮书(2025) [R]. 2025.
CMCC. White Paper on Network and Data Security System of Low-altitude Intelligent Connected Network (2025) [R]. 2025.
- [12] 陈咏涛, 刘颜, 樊聪等. 关于低空黑飞无人机探测技术研究与展望[J]. 电信科学, 2026. CHEN YT, LIU Y, FAN C, et al. Research and Outlook on Detection Technologies for Low-Altitude Illegal Drones[J]. Telecommunications Science, 2026.
- [13] 夏勇, 李晋, 廖晓川等. 场景驱动的低空无人机防御系统部署方案研究[J]. 电信科学, 2025. XIA Y, LI J, LIAO XC, et al. Research on Deployment Schemes for Scene-Driven Low-Altitude UAV Defense Systems[J]. Telecommunications Science, 2025.
- [14] 3GPP. Study on security aspects of WAB nodes for NR: 3GPP TR 33.724 [S]. 2025.
- [15] 3GPP. Network Domain Security (NDS); IP network layer security: 3GPP TS 33.210 [S]. 2025.
- 白景鹏, 1995年, 男, 学士学位, 中国电信研究院云网安全技术研究工程师; 主要研究方向为5G/6G网络安全。;
- 薄明霞, 1978年, 女, 博士学位, 中国电信集团云网安全体系架构研究高级工程师; 主要研究方向为内生安全、AI安全、关键基础设施安全。;
- 沈军, 1976年, 女, 硕士学位, 中国电信研究院云网安全技术研究高级工程师; 主要研究方向为5G/6G网络安全。