1. **项目简介（200字以内）**

无人机与微基站的结合，使快速且安全地恢复通信成为可能。

本项目利用波形特异性实现了人机、机机间的无感知认证；利用聚合消息验证码实现了人、机轻量级、高速安全接入与密钥协商；利用时间触发一致性控制技术实现了通信链路抗毁；利用自组网技术实现快速部署、提供安全通信网络。本项目的实施将有效提升应急抢险场景下，通信快速恢复、通信安全保障的能力，进一步提升应急抢险的能力。

1. **项目相关研究现状及发展动态（不少于200字）**

**1.研究现状**

近年来，在自然灾害如地震、海啸、洪水等的救援善后工作中，应急通信的需求增长迅速。由于受灾地域通常面临着通信基础设施损毁的情况，给灾后救援、重建等工作造成了极大的障碍。因此应急通信系统对于灾后各项工作至关重要，如何更加有效地恢复受灾地区的通信信号，这一问题引起了很多人的关注。

目前主要的实施方案有固定翼无人机方案和系留式无人机方案，本项目基于这两种方案提出一种新的基于无人机蜂群的组网方案，下面主要介绍一下现有的两种方案和本方案的现状及发展动态。

1. **固定翼无人机方案**

现有的固定翼无人机方案主要由宏站、无人机平台、安全网关、机载基站、回传终端、SP-GW（ServingPDN-GateWay）组成。该系统结构中，回传终端、机载基站均部署在上飞机设备中，作为数据传输和网络覆盖工具，分别与用户终端和宏站建立连接，形成信号传输路径。在此种方案[1]中，固定翼无人机体积庞大，对机场、通用航空管制、经费等条件要求较高，部署周期长；电池电量有限，导致可持续时间受限；因覆盖范围有限而无法完全覆盖受灾地区；由于其信号在覆盖范围内是无差别覆盖，会导致人流量密集的地区出现通信堵塞的情况。

具体场景如图1所示：

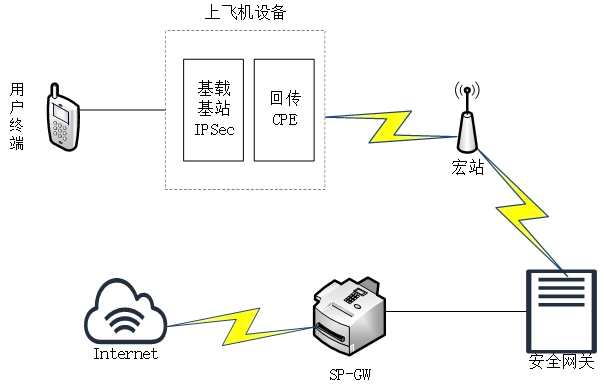


图1 固定翼无人机方案场景示意图

1. **系留式无人机方案**

现有的系留式无人机方案主要由现网、地面应急车、通信卫星、卫星便携站、起降平台、系留电缆组成，是指将无人机和系留线缆结合起来实现的无人机系统，它通过系留线缆来供应电能，可以使无人机不受电能限制而长时间滞留在空中。虽然此种方案[2]避免了固定翼无人机可持续时间有限这一缺点，但因系留线缆导致滞空高度有限进而影响了其信号有效的覆盖范围并存在高密度用户聚集地通信质量受损等相关的问题。

具体场景如下图2所示：

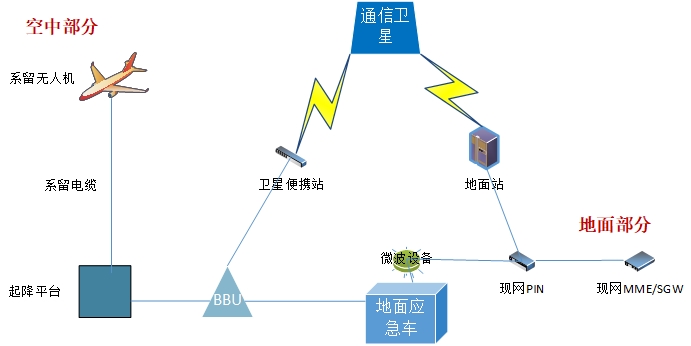


图2 系留式无人机方案场景示意图

**3）本方案**

本项目提出了基于无人机蜂群的应急通信方案，通过无人机搭载微型基站，利用自组网技术，形成机间安全通信链路，有效覆盖受灾地区，进而快速恢复受灾地区的信号，满足应急通信的需求。

**2.发展动态：**

无人机由于具备高速、机动、灵活等优点，在抗震救灾、应急抢险等场景下优势明显，结合通信链路抗毁、密钥协商、无感知认证等技术，有助于快速实现应急通信。在无人机蜂群的辅助下，将迅速的部署通信链路、实现应急通信，帮助救援指令进行高效传达，实现灾区情况实时采集，进而将推动救援行动的高效展开、有效缓解灾区人民焦躁情绪，提升了应急抢险能力。

具体场景如图3所示：

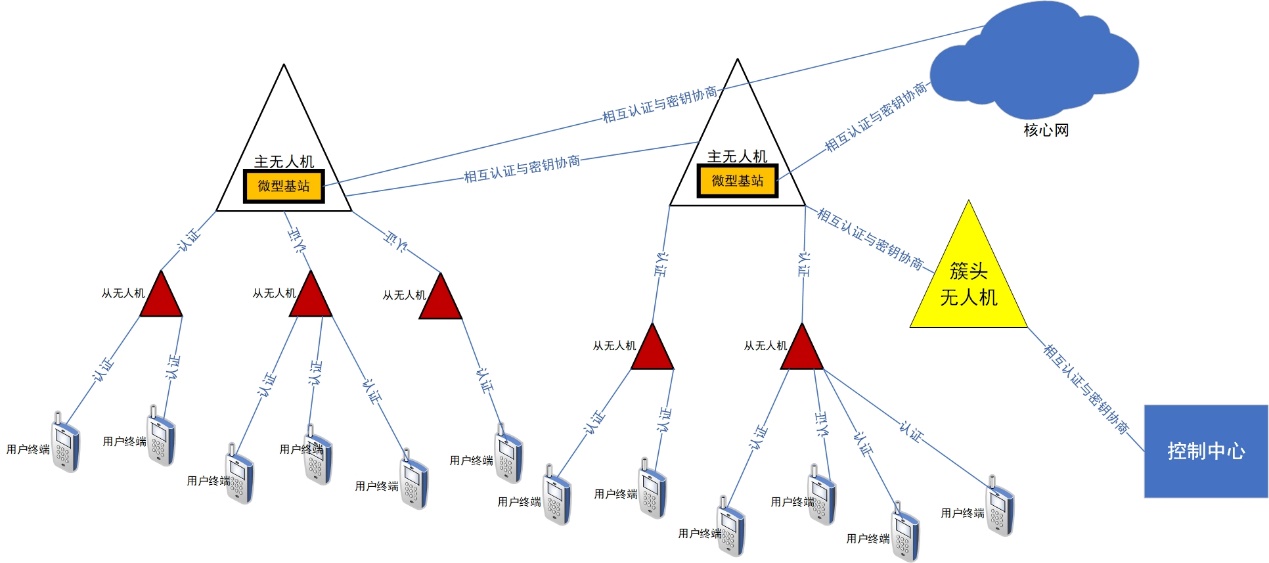


图3 旋翼无人机方案场景示意图

**文献引用：**

[1]代海刚.5G基站环境下固定翼无人机应急通信覆盖能力研究[J].电声技术,2022,46(01):113-116+125.DOI:10.16311/j.audioe.2022.01.032.

[2]吴鹏,王黎阳.系留式多旋翼无人机在应急通信中的应用[J].中国信息化,2018(12):60-61.

1. **项目实施的目的、意义（不少于200字）**

**1.目的**

在水灾、地震等自然灾害发生后，受灾地区往往会有基础设施损坏。而当通信基站受灾损坏后，当地通信设备无法再通过基站进行信息的发送与接收，从而导致无法与外界进行通信。

灾区内与救援人员的信息不互通会对救灾造成极大阻碍，导致救灾人员、资源无法得到恰当调配，影响救灾效率。如果能通过某种方式临时恢复灾区通信，在救灾过程中，灾区内外信息能够相互流通，那么这将对救灾工作带来极大便利，有效保障灾区居民生命与财产安全。

本项目通过无人机蜂群在灾区进行组网，形成通信链路，覆盖受灾地区，达到迅速实现应急通信的效果。

**2.意义**

2021年7月17日至21日，河南出现罕见持续性强降水天气，多地突发特大暴雨，其中郑州降雨量达345mm，最大点雨量尖岗884mm。此次暴雨导致郑州292人遇难，47人失踪，直接经济损失达532亿元。暴雨还导致郑州通信基站大面积退服，多条通信光缆受损，通信基础设施受损严重，某些受灾严重区域一度发生通信阻断。据统计，此次特大暴雨共造成河南省6.2万个基站退服，其中郑州市退服基站达3.5万个，光缆受损566条，共1223km，影响固定网用户数14.3万户，移动网用户数38.2万户。河南省及郑州市基站退服率分别达到了13%和45%。

在这种情况下，尽管运营商竭力抢救恢复通信，但仍然很难在短时间内保证各地通信恢复正常。而灾后72小时是救援黄金时期，仅凭公网修复无法保证救灾时期的通信正常。灾区居民无法与外界进行有效联系，对救灾工作造成重重阻碍。在灾后地面公网恢复周期内，社会秩序的恢复也需要移动互联网通信网络业务的维持，大范围基站退服、脱网问题直接影响到了社会的正常运行。

幸运的是我们还有临时恢复通信的手段。针对地面公网通信瘫痪问题，运营商紧急部署无人机实现了快速回复局部区域通信，借助卫星构筑天地通信链路，为地面公网提供补充与完善，为公众提供临时互连网络业务。

目前随着无人机技术的迅猛发展和日趋成熟，我国已经发展出多种通过无人机临时恢复通信的方案，但是其中以系留无人机为主，系留无人机应急通信系统包含无人机平台和地面系统两大部分。无人机平台包括多旋翼无人机、系留飞行控制系统、机载电源模块和任务载荷。地面系统包括起降平台、发电机、地面站、地面 CPE设备和核心网设备。其可以长时间为一定区域稳定提供通信服务。但是缺点也很明显，系留无人机需通过线缆与地面终端相连，这就限制了无人机飞行的高度与覆盖的范围，无法实现大面积通信的恢复。

为解决上述问题，我们考虑通过无人机域内组网的方案扩大无人机覆盖的范围。无人机具备高速、易操控的优点。无人机蜂群携带微型基站，形成通信链路，恢复灾区通信，通过无人机分层协作，覆盖更大的范围，为更广阔的地区提供通信服务。同时通过域内组网的方案，可以及时调配无人机资源，为居民区等用户多的区域分配更多的无人机，达到合理配置资源的效果，利于救灾指令的传达，为灾后救灾提供巨大的帮助。

1. **项目研究内容和拟解决的关键问题（不少于300字）**

**1. 研究内容**

本项目将对基于无人机蜂群的救灾应急通讯系统进行研究。在水灾、飓风和地震等灾害发生后，大部分基站受损，剩余的基站因无法承受大流量的数据，导致广大地区通信服务缺失，分布式传感器网络或宏蜂窝网络等都无法最大限度地发挥作用，这将不利于救灾工作的进行。考虑到现有技术如固定翼无人机和系留式无人机方案的局限性，本项目提出一种新型解决方案，利用无人机蜂群进行应急通信的解决方案，本方案中主要由无人机、控制中心、核心网、微型基站这四个实体组成，基于分层组网，将无人机划分为：簇头无人机、主无人机、从无人机。方案的核心在于恢复通信的基础上，保障用户通信的安全性和完整性，保障基于无人机蜂群的通信链路的强健性。

当无人机电量充足并且搭载的微型基站可以正常工作时，无人机向控制中心和地面站发送认证请求，通过认证后，无人机将获得专属密钥，分别认证成功后接入到无人机网络完成无人机组网，在一切准备就绪后，无人机根据控制中心传来的控制信令飞到相应的位置，并与附近无人机进行身份认证，以便于相互之间传递信息，这样便形成了一个密集的信号交通网。接着无人机搭载的微型基站开始准备接入用户设备，在此过程中，为了保证通信安全，在用户接入微型基站时，需要进行身份认证与密钥协商，通过认证后，微型基站利用消息漫游将用户信息发送到核心网，并把得到的处理结果反馈给用户，进而实现用户与外界的通信。当同时有大量用户通信设备接入无人机的基站时，自动通过流量均衡算法对通信负载进行分摊均衡。当无人机电量不足时，根据调度算法自动发送信息给控制中心，控制中心将派送新的无人机去替换此电量不足的无人机，当新的无人机到达时，新的无人机通过认证后接入到无人机网络完成无人机群组的更新，而电量不足的无人机可以返回到控制中心，进行充电或者更换电池，等待再次被使用。无人机蜂群在灾区上空巡飞，以维持区域通信的可靠、稳定，此时会出现因无人机移动带来的信号覆盖范围改变的问题，不在原本无人机的信号覆盖范围内的用户需要通过认证与密钥协商后接入切换到在信号范围覆盖内的相应无人机。无人机群组具备一定的通信链路抗毁能力，当无人机遇到极端恶劣天气等情况，导致受损无法继续执行任务时，会由控制中心派送新的无人机接入对其进行更新。

该方案具有灵活性高、机动性强、结构简单等特点，为灾后救援通信恢复工作提供一种新的想法。利用数量众多的无人机组成密集的信号交通网，形成有效通信的通信链路，达到恢复通信的目的。虽然单个无人机的供电能力有限，但是预备有无人机时刻准备替换电量即将耗尽的无人机，这让无人机蜂群的提供应急通信成为可行方案。

**2. 研究目标**

本项目拟利用无人机蜂群搭载微型基站，通过用户与无人机之间的认证，无人机之间的相互认证以及无人机搭载的微型基站与核心网之间的认证，研究基于无人机群组的救灾应急通讯系统，实现灾区与外界的安全通信。

具体来说，首先所有无人机都与控制中心进行身份认证与密钥协商，确保无人机收到的控制信息均来自控制中心，实现无人机群组的安全组网。随后，用户在接入无人机搭载的微型基站时，要进行认证和密钥协商，最后，为了保证用户的信息在漫游时不被泄露，无人机搭载的微型基站在接入核心网时，将通过自主设计的协议进行认证与密钥协商，实现对用户信息的安全传递。

本项目的科研成果将进一步提升应急抢险的能力，为灾后救援时的安全通信提供有效保障。

**3. 拟解决的关键问题**

无人机蜂群组成的安全通信网涉及到无人机之间的通信认证、无人机覆盖位置变化的动态算法、海量用户接入涉及到的无人机间的工作量分担、当无人机电量不足时的替换方案和突发状况而导致的用户接入断开等情况，下面具体介绍拟解决的三方面关键问题：

1. **无人机构建安全通信网**

现有的应急通信方案部署周期普遍较长，无法快速恢复灾区的通信信号，不匹配救灾场景下时间紧迫这一特性。为此本项目提出分层组网方案，致力于快速形成无人机通信网，满足灾区对快速恢复通信的需求。在此方案中，将无人机划分为簇头无人机、主无人机、从无人机，其中簇头无人机负责与控制中心进行通信，将得到的控制信令转发给相应的无人机，进而实现控制中心对无人机蜂群的控制。主无人机上载有微型基站，微型基站是应急通信网络的核心，用于辅助用户与外界进行通信。在主无人机下方设置有从无人机，从无人机负责收集用户请求信息并转发给主无人机，达到扩大通信网覆盖范围的目的。基于对组网的安全、稳定等方面的考虑，将依据组网需求设计出无人机与控制中心之间的认证协议、无人机与无人机之间的认证协议（完成组网实体间的相互认证与密钥协商），致力于构建安全可靠的通信链路，为应急通信提供安全保障。

1. **用户设备海量并发接入问题**

a)现有的应急通信方案并未考虑到在用户密集区域，海量设备并发接入通信网所带来的通信阻塞、信令风暴等相关影响通信质量的问题。为解决这一问题，本项目致力于设计一种轻量级的接入认证协议，在保障通信安全与稳定的前提下，减少用户设备接入认证所需的信令开销，进而缩短接入认证所需要的时间，达到提升应急场景下通信效率的效果。

b)现有的应急通信方案并未解决负载均衡问题，常常出现某一个无人机接入的用户数量过多、工作量过大，而附近某些无人机接入用户数量较少、工作量未满等情况，不利于资源的合理分配与利用。因此，本项目提出使用流量均衡算法，当某一个无人机负载量过大时，将依据流量均衡算法，自动分摊任务给附近的无人机，致力于解决在用户密度大的区域中通信质量易受影响的问题。

1. **无人机群组更新问题**

在现有的应急通信方案中，单个无人机电量有限或环境恶劣导致无人机损坏，进而导致应急通信可持续运行时间受限及可能发生部分区域通信中断等问题。为了突破这些问题，本项目目标提出一种无人机群组更新方案，当某个无人机电量不足或发生故障时，控制中心将派送新的无人机去替换此无人机，新的无人机在与控制中心和核心网进行认证后，接入到无人机网络，与原无人机进行工作交接，从而快速且安全地实现无人机群组成员更新，缓解应急通信系统可运行时间受限这一问题，为应急通信的应用提供更加广阔的空间。

1. **项目研究与实施的基础条件（不少于300字）**

**1. 研究与实施基础**

申请者与主要成员已针对“海量设备并发接入认证”，“无人设备组网认证”，“无人机间无感知认证”等技术开展了相应的研究工作。

**2.现有研究条件**

1）申请人以及项目组成员已阅读了大量的相关文献，记录了众多的数据，探讨了该项目需解决的关键问题，分析了所研究课题的国内外研究现状，具有一定的理论基础。

2）网信大楼b255办公室可以提供进行实验操作。

3）申请人、与团队成员为我校网络与信息安全学院的本科学生，在学院领导、老师的指导下，均具备良好的工程实践能力。

4）申请人团队依托于西安电子科技大学网络与信息安全学院，学术积淀深厚。

5）可购买的天线、树莓派、wifi无线模块等现有硬件。

6）我国自主研发创新的一套数据加密处理系列算法可供使用。

7）实验室购买的旋翼无人机以及仿真平台可供使用。

1. **项目实施方案（不少于300字）**

本项目拟设计一种基于无人蜂群的救灾应急通讯系统，通过无人机机群进行组网，恢复灾区通讯信号。项目要实现的主要是五大模块，具体如下：

**1）无人机与控制中心的无感知认证**

无人机在起飞之前的准备工作中需要完成与控制中心之间的无感知认证，本方案基于国密SM4加密算法实现认证和密钥协商，为无人机与控制中心之间的信令传输提供安全保障，建立可信的通信方式。

**2）无人机与无人机之间的密钥认证和组网**

无人机在和控制中心认证完成之后开始无人机蜂群之间的无感知认证，控制中心按照组网方案发送控制信令给无人机，完成无人机蜂群的组网计划，至此各个无人机收到部署方案，同时得知自己即将前往的目的地。

1. **无人机处理海量并发接入问题**

恢复通信不可避免的问题是大量用户并发接入微型基站以及进行信息处理时会对服务器造成巨大的计算压力。解决此问题需从三个方面入手：

a) 采用5G切片技术，将控制信令与通信信令使用的信道分开，如此，即便在通信拥堵的情况下，控制中心发送的控制信令依旧可以被各个无人机准确接收。

b) 大量用户信息的处理问题，需要合适的算法保证服务端有能力处理海量信息，以及准备好当信息量超过服务端处理能力时的应对方案。

c) 在用户密集区域，当出现某一个无人机负载量过大时，将依据流量均衡算法，把接收到的数据包转发给附近的其它无人机，让它们代为处理，解决了在大密度用户区域通信质量易受影响的问题。

1. **无人机群组更新问题**

a）无人机因为故障或电量问题需要新无人机代替：考虑到单个无人机可持续工作时间有限的问题，设计出无人机群组更新的应对方案，当某个无人机电量不足时，根据调度算法自动发送信息给控制中心，控制中心将派送新的无人机去替换此电量不足的无人机，此方案解决了应急通信方案可持续运行时间有限的一大难题;无人机群组具备一定的通信链路抗毁能力，当检测到无人机遭遇极端恶劣天气等因素，导致受损无法继续执行任务时，会由控制中心派送新的无人机接入对其进行更新。

b）无人机更新会带来用户接入切换的问题：出现因无人机更新带来的信号覆盖范围改变的问题，不在原本无人机的信号覆盖范围内的用户要接入切换到在信号范围覆盖内的相应无人机，保证正常通信。

**5）无人机分层协作**

为了扩大无人机的覆盖范围，本方案在主无人机下面设置了从无人机，从无人机只负责对用户的信息进行接收并转发给主无人机，起到分担主无人机收集与转发用户信息的作用；无人机蜂群的控制，主要通过簇头无人机与控制中心之间进行通信，将获得的控制信息转发给相应的主无人机，主无人机转发给从无人机，从而实现各个无人机与控制器之间的联系。

1. **项目创新点及特色（不少于300字）**

本项目的创新点及特色主要包括方案设计与技术上的创新，同时其应用场景十分广阔，对社会具有极高的使用价值。

**1.创新与特色**：本项目提出的基于无人机蜂群进行组网，其优势在于，通过无人机携带微型基站，在灾区组成密集的信号交通网络，另外在应急救援车上预备有众多准备替换电量即将耗尽的无人机，同时配备有相关的充电设备，这样本通信方案的机动性、稳定性、可持续时间都将大大增强；考虑到灾情之下时间紧迫这一特性，本项目选择使用国密加密算法中的对称加密算法，此算法效率更高、速度更快，有利于节省时间；采用5G切片技术，将控制信令与通信信令使用的信道分开，如此，即便在通信拥堵的情况下，控制台发送的控制信令依旧可以被各个无人机准确接收；依据流量均衡算法，解决在大密度用户区域通信质量易受影响的问题。

**2.对社会：**本项目设计的应急恢复通信方案，利用分层组网协作，使覆盖范围更加广阔，使用的自组网技术有利于快速实现无人机蜂群的部署，因此本项目更适合广泛应用于生活中所需要进行应急通信的场景，应急通信系统在城市运转遭到突发灾害或事故时，承担着及时、准确、畅通地传递信息的“急先锋”角色，是决策者正确指挥抢险救灾的中枢神经，因此本方案对社会的发展有着极大的帮助。

1. **已有基础（包括与本项目有关的研究积累和已取得的成绩、学校可以提供的条件、尚缺少的条件及解决方法）**

**1.与本项目相关的研究积累：**

1.在应对海量用户并发接入方面，自主设计了基于信誉机制和PUF的适用于大规模设备远程身份认证协议，协议能够有效缓解海量设备并发接入时的网络拥塞问题，高效地实现设备与服务器、设备与设备之间的双向认证与密钥协商。

2. 在设备间认证和通信方面，自主设计了海量D2D通信设备的高效匿名邻近设备发现和批量认证机制，该机制解决了异构接入场景下D2D用户设备的设备发现、高效认证、相互认证和密钥协商和隐私保护等问题，提出的方案可以应用于D2D通信的5G异构接入场景。

3. 在轻量级接入认证方案方面，自主设计了一种新型轻量级安全访问认证方案，该方案包含两种基于切比雪夫访问认证协议，适用于两种类型的3GPP标准移动设备：1）通用用户设备，和2）大规模机器类通信设备，可以高效安全地实现设备的接入认证。

4. 在应对群组成员更新方面，自主设计了一种基于中国剩余定理的安全高效的多播服务组密钥分发和更新过程，可以安全高效地实现群组成员变动时的密钥更新，保证后续通信过程的安全。

**2. 学校可以提供的条件：**

学校开展的关于密码学、机器学习、程序设计的课程，认真听老师讲课，不懂的地方将虚心请教老师，即时解惑，以达到学好这些相关的课程的目的；利用线上、线下的图书馆资源，查阅相关的书籍和文献，通过阅读相关的知识来提升自己；指导老师的支持与帮助，推荐相关的论文、及时纠正我们在方向上的错误，对我们的进步给予巨大的帮助。

**3. 尚缺少的条件：**

目前实验室仅拥有一台旋翼无人机，无法实地进行无人机蜂群组网协作的实验。

**4. 现阶段解决方案：**

暂时进行模拟实验，利用多个系统进行交互得到相关实验数据。

1. **项目研究进度安排及各阶段预期成果(本栏内容为中期检查及结题答辩重要参考)**

**第一阶段**：完成无人机蜂群自组网技术与加密方法的相关调研，配套学习相应的基本学习工作，熟练掌握协议中要使用到的通信原理和加密算法以及后期需要用到的测试方法等重要知识和技能。

**第二阶段**：完成组网设计方案，并根据方案撰写所需协议，后续实现所有协议的代码，同时开展模拟测试，基于模拟结果，做出方案的调整。

**第三阶段**：实现在真实无信号环境下，测试多用户同时接入、无人机之间的安全通信、无人机群组更新、微型基站接入核心网时是否会出现问题，基于测试结果对于相关方案进行改进，并再次进行实验。