#### 设计、发明的目的和基本思路、创新点、技术关键和主要技术指标

在水灾、飓风和地震等灾害发生后，分布式传感器网络和蜂窝网络等用于支持通信的设备都无法发挥作用。如在2021年7月，河南省郑州市遭受洪水灾害而导致的基站受损，进而导致没有信号现象的出现；在2022年9月，四川省雅安市石棉县发生地震，造成了大面积的建筑倒塌、信号丢失的现象。

受灾后由于自然灾害等因素造成大多数的基站受损，而剩下少量的可运行基站，由于电线断裂导致断电这一原因，无法给在受灾地区中依旧可以运行的基站供电，进而导致无法恢复信号。在自然灾害恶劣的天气条件下，再加上道路受损、不通等困难情况，会导致无法及时顺利展开修复救灾地区的电线等供电设备，同时也不利于专业人员对基站的修复，进而导致基站无法顺利运作，信号缺失这一现象，对灾后搜救工作造成了极大的影响，不利于尽快救出受困人员，也不利于灾区群众与外界的联系。

现有的固定翼无人机方案，对机场、通用航空管制、经费等条件要求都比较高，影响了应用的广泛性。系留式无人机的方案受制于其高度和载重问题，其飞行高度仅在100米左右，无法实现大范围、多功能的应急通信保障需要。

考虑到现有方案的局限性，所以我们提出一种新型解决方案，即利用旋翼无人机进行辅助通信，由于旋翼无人机体积小，且价格便宜，因此该方案具有灵活性高、机动性强、结构简单、造价低廉等特点。

我们的创新点在于：

利用旋翼式无人机自组网技术，以搭载小型基站为基础，构建无人机机群，从而形成有效的通信链路，覆盖受灾地区，进而达到最大限度地缩短恢复当地信号所需时间，为搜救受困人员提供有力的支撑。

技术关键和主要技术指标：

本方案实现的关键在于通信安全协议的设计，为保证通信的安全性，同时考虑到灾情之下时间紧迫这一特性，应采取轻量级的加密协议，该协议也保证了信息基本的机密性、完整性、认证和不可否认性这四个特点如图1所示。

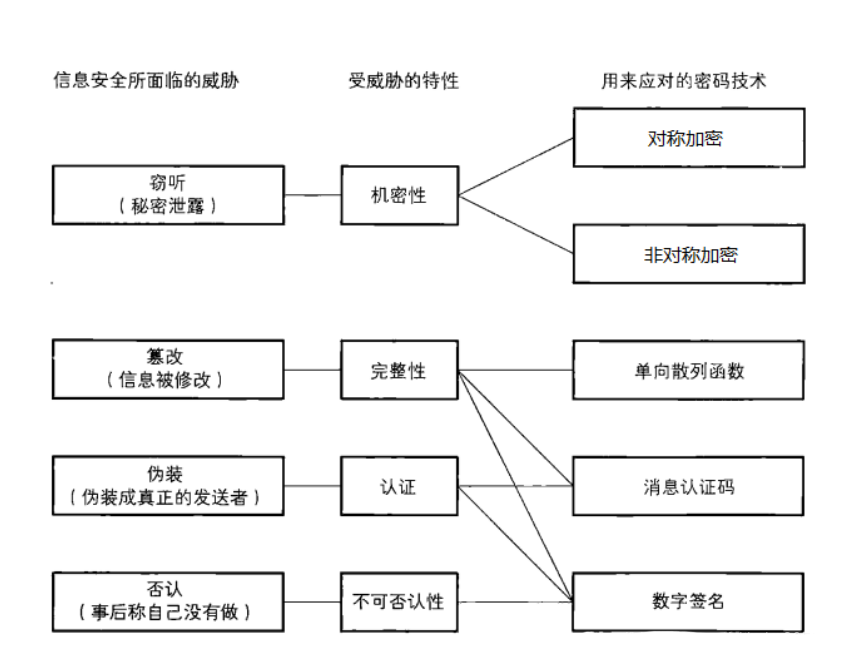


图1

对称加密算法因计算量过大，不适合无人机轻量级的通讯，所以我们设计的协议使用的是对称式加密算法。本方案中的多个协议主要基于无人机起飞前的预置秘钥进行协议加密，协议主要是关于：

1.簇头与控制中心之间的相互认证与密钥协商；

2. 簇头与节点之间的相互认证与密钥协商，

3. 控制中心与节点之间的相互认证与密钥协商；

4.节点之间的相互认证与密钥协商；

5.群组节点的更新；

6.节点与子节点之间的相互认证与密钥协商；

7. 节点与用户设备之间相互认证与密钥协商；

具体场景如图2所示。

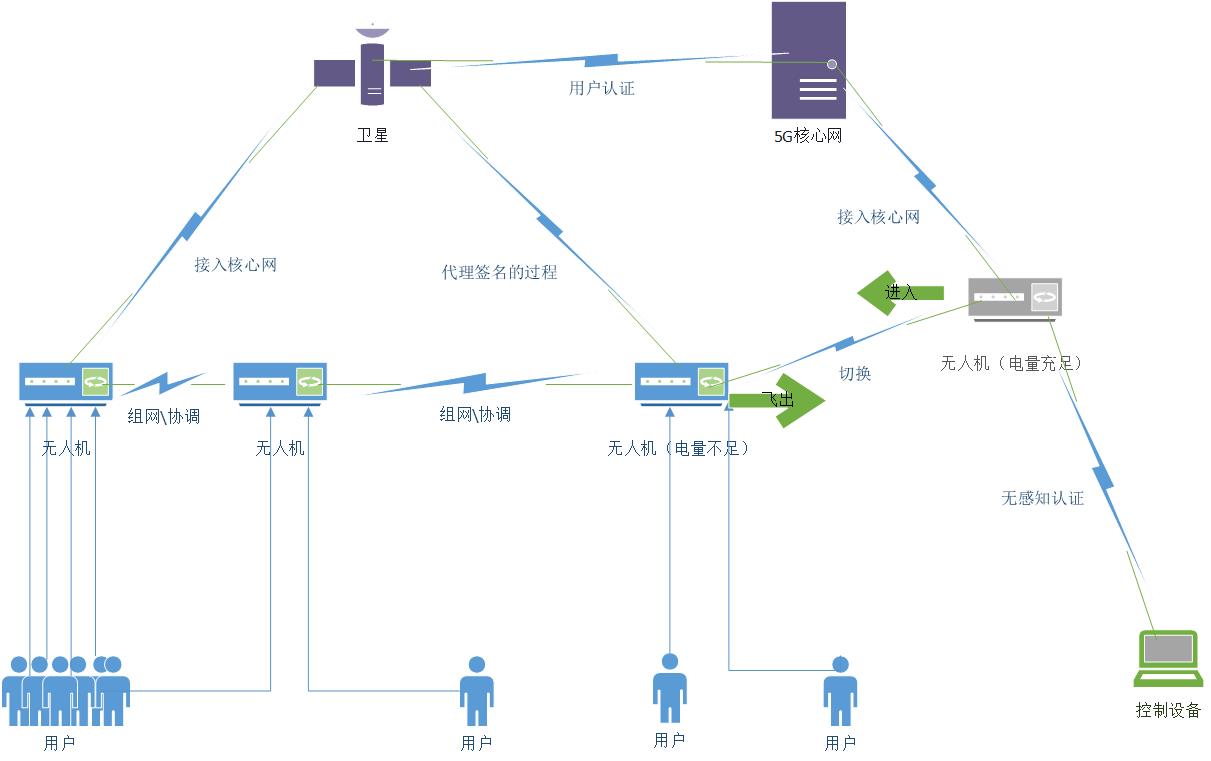


图2

我们目前已实现簇头与控制中心之间的相互认证与秘钥协商协议的代码，协议内容如下：



具体步骤如下：

1. AS(控制中心)首先发起认证请求，包含新生成的时间戳T1以及随机数r1;
2. 簇头收到消息后，如果确认T1是新鲜的，返回响应消息，即IDL,IDAS, T2, r2,MACL，其中MACL=hash(K，IDL,IDAS, T2, r2,r1),其中T2为新生成的时间戳，r2为随机数,K为控制中心与簇头之间的预置密钥；
3. AS检查T2的新鲜性与MACL是否正确。检查通过则返回认证确认消息IDAS, IDL,T3, r3,MACAS，其中MACAS=hash(K，IDAS,IDL, T3, r3,r2),其中T3为新生成的时间戳，r3为随机数。
4. 簇头检查T3的新鲜性与MACAS是否正确。检查通过返回认证结果，并开始衍生密钥。
5. AS根据认证结果决定是否衍生密钥。如果认证成功，AS及时广播簇头的ID。（括号主要取决于设定里究竟是否节点能与AS之间信号强度是否支撑通信，是则簇头的主要目的是减少信令数目，否则兼具中继功能）12345678 CK=1234 IK=5678

**余下6个协议的具体内容如下：**

## 节点与控制中心之间的相互认证与密钥协商



1. 节点i依据控制中心广播的簇头ID,发送认证请求消息IDL,IDi,ti,ri,MACi，其中MACi=hash(Ki, IDL,IDi,ti,ri), 其中ti为新生成的时间戳，ri为随机数,K为节点i与AS之间的预置密钥；
2. 收到多个节点的认证请求后，簇头检查新鲜性后，按照MAC=MAC1⊕MAC2⊕…⊕MACn的方式聚合消息中的MAC值，并发送聚合认证请求IDAS, IDL,{(ID1,t1, r1),(ID2,t2, r2),…,(IDn,tn, rn)},MAC,MACL,其中MACL=hash(IK, IDAS, IDL,{(ID1,t1, r1),(ID2,t2, r2),…,(IDn,tn, rn)},MAC)，其中IK为上一阶段簇头与控制中心衍生的密钥;
3. 控制中心核验MAC，如果检查通过，则返回IDL, IDAS,{(ID1,T1, R1,MACAS\_1),(ID2,T2, R2,MACAS\_2),…,(IDn,Tn,Rn,MACAS\_n)},MACAS-L，其中MACAS\_i=hash(Ki, IDi,Ti, Ri,ri)，MACAS\_L=hash(IK,IDL, IDAS,{(ID1,T1, R1,MACAS\_1),(ID2,T2, R2,MACAS\_2),…,(IDn,Tn,Rn,MACAS\_n)}),T1T2……Tn为新生成的时间戳,R1R2……Rn为随机数。
4. 簇头收到消息后核验MACAS\_L，核验通过后将认证回应分发给相应的节点；
5. 节点i核验MACAS\_i,核验通过后开始衍生密钥。

* 依靠簇头(簇头的选取依靠广播消息)，但不与簇头进行身份认证与密钥协商
* 聚合认证请求MAC=MAC1⊕MAC2⊕…⊕MACn
* MACAS\_i=hash(Ki, IDi,Ti, Ri,ri),
* MACAS\_L=hash(IKAS\_L,IDL, IDAS,{(ID1,T1, R1,MACAS\_1),(ID2,T2, R2,MACAS\_2),…,(IDn,Tn,Rn,MACAS\_n)})(没加随机数不知道会不会安全性分析出问题)
* 簇头在这里的作用为转发消息
* 簇头的更新依靠AS的广播（或者加密）消息

对簇头的一些合理设定：1.减少认证的信令开销；2.减少AS处控制信令的信令开销2.减少数据传输的信令开销（某些节点采集的数据数据不一定要连续发送，可以采集一段时间集中发送（而节点存储空间不够，所以先加密簇头，可能是与AS的密钥，也可能是与簇头的密钥））

## 节点与簇头之间的相互认证与密钥协商



1. Nodei首先发起认证请求，包含新生成的时间戳T1以及随机数r1;
2. 簇头收到消息后，如果确认T1是新鲜的，返回响应消息，即IDL,IDi, T2, r2,MACL，其中MACL=hash(K，IDL,IDi, T2, r2,r1),其中T2为新生成的时间戳，r2为随机数,K为节点i与簇头之间的预置密钥；
3. Node i检查T2的新鲜性与MACL是否正确。检查通过则返回认证确认消息IDi, IDL,T3, r3,MACi，其中MACi=hash(K，IDi,IDL, T3, r3,r2),其中T3为新生成的时间戳，r3为随机数。
4. 簇头检查T3的新鲜性与MACAS是否正确。检查通过返回认证结果，并开始衍生密钥。
5. Node i根据认证结果决定是否衍生密钥

## 节点之间的相互认证与密钥协商



Node A与Leader之间已经建立了加密和完整性保护

1. Node A首先发起认证请求，将会话请求消息（IDA,Enc(IDB,RA),MACA）发送给Leader。其中MACA=hash(IKA，IDA,Enc(IDB,RA))，IKA为NodeA和Leader两者之间的完整性保护密钥
2. Leader核验MACA和检验随机数的新鲜性，检查通过生成随机数RS，将会话通知消息(IDL,Enc(IDB, IDA, RS⊕RA),MACL\_B)发送给Node B，其中MACL\_B=hash(IKB,IDL,Enc(IDB, IDA, RS⊕RA))，IKB为NodeB和Leader两者之间的完整性保护密钥。
3. Node B核验MACL\_B和检验RS⊕RA的新鲜性，检查通过生成随机数RB，计算密钥CK||IK=hash(IDA,IDB,RA⊕RB⊕RS)，将会话通知回复（IDB,Enc(IDA, RB),MACB）返回给Leader。其中MACB=hash(IKB，IDB,Enc(IDA, RB))，IKB为NodeB和Leader两者之间的完整性保护密钥。
4. Leader核验MACB和检验随机数的新鲜性, 检查通过后将会话请求回复（IDL,Enc（IDA,IDB,RB⊕RS)MACL\_A）发送给Node A，其中MACL\_A=hash(IKA,IDL, Enc(IDB, IDA, RS⊕RB))，IKA为Node A和Leader两者之间的完整性保护密钥。

## 群组节点更新

正常情况由AS通过旧簇头将加密的新簇头的ID发送给各个节点，簇头节点损坏的情况重新执行流程

## 子节点与节点之间的相互认证与密钥协商

同（三）

## 用户设备与节点之间相互认证与密钥协商

在不考虑AKA的情况下就是一个普通群组认证。

#### 说明与现有技术相比、该作品是否具有突出的实质性的技术特点和显著进步

无人机空中基站系统是近几年发展起来的一种新型的应急通信保障手段，无人机空中基站投入商用后，除了能够提供应急通信车所能实现的所有功能外，还因覆盖角度可随无人机旋转方向调整，而具有更加有效地实现大面积信号覆盖的优势。

现有无人机通信分为系留无人机、旋翼无人机和固定翼无人机三种类型。其中系留无人机应用较多，目前其作为主要通信恢复式空中基站，但受制于其高度和载重问题，系留无人机尽管可实现24小时应急通信保障需求，但其飞行高度仅在100米左右，载荷约10KG，无法实现大范围、多功能的应急通信保障需要。固定翼无人机已经可以成功应用，在2022年1月21日河南的特大暴雨中，“翼龙”应急救灾型无人机成功恢复周边30多平方千米的手机信号，有效通信恢复时间长达5个小时，但是固定翼无人机也有短板，其对机场、通用航空管制、经费等条件要求都较高，影响了应用的广泛性。

而我们提出的基于旋翼无人机进行组网，其优势在于众多旋翼无人机在灾区组成密集的信号交通网，并且有预备无人机时刻准备替换电量即将耗尽的无人机，众多旋翼无人机搭载在应急救援车上，并且配备相关充电设备，这样机动性、稳定性、持续时间会大大增强，故可以成为恢复应急通讯的可行方案。

#### 作品使用说明以及该作品的技术特点与优势

使用说明及技术特点：本方案的实体主要有子节点无人机、节点无人机、簇头无人机、控制台、基站、核心网。

如图3所示



图3

本方案的核心在恢复通信的基础上，保障用户的通信的安全性和完整性。具体为无人机机群搭载基站，接收用户发来的数据之后发送到卫星上，由此来与外界取得联系。无人机机群的控制主要是通过簇头无人机与控制器之间进行通信，将获得的控制信息转发给相应的无人机，从而实现各个无人机与控制器之间的联系；为了扩大无人机的覆盖范围，我们在主无人机下面设置一些从无人机，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，起到一个ap的作用；当某一个主无人机负载量过大时，将接受到的数据包转发给他附近的其它负载量不是很大的、工作量相对较少的主无人机，让它们代为处理。

如图4所示

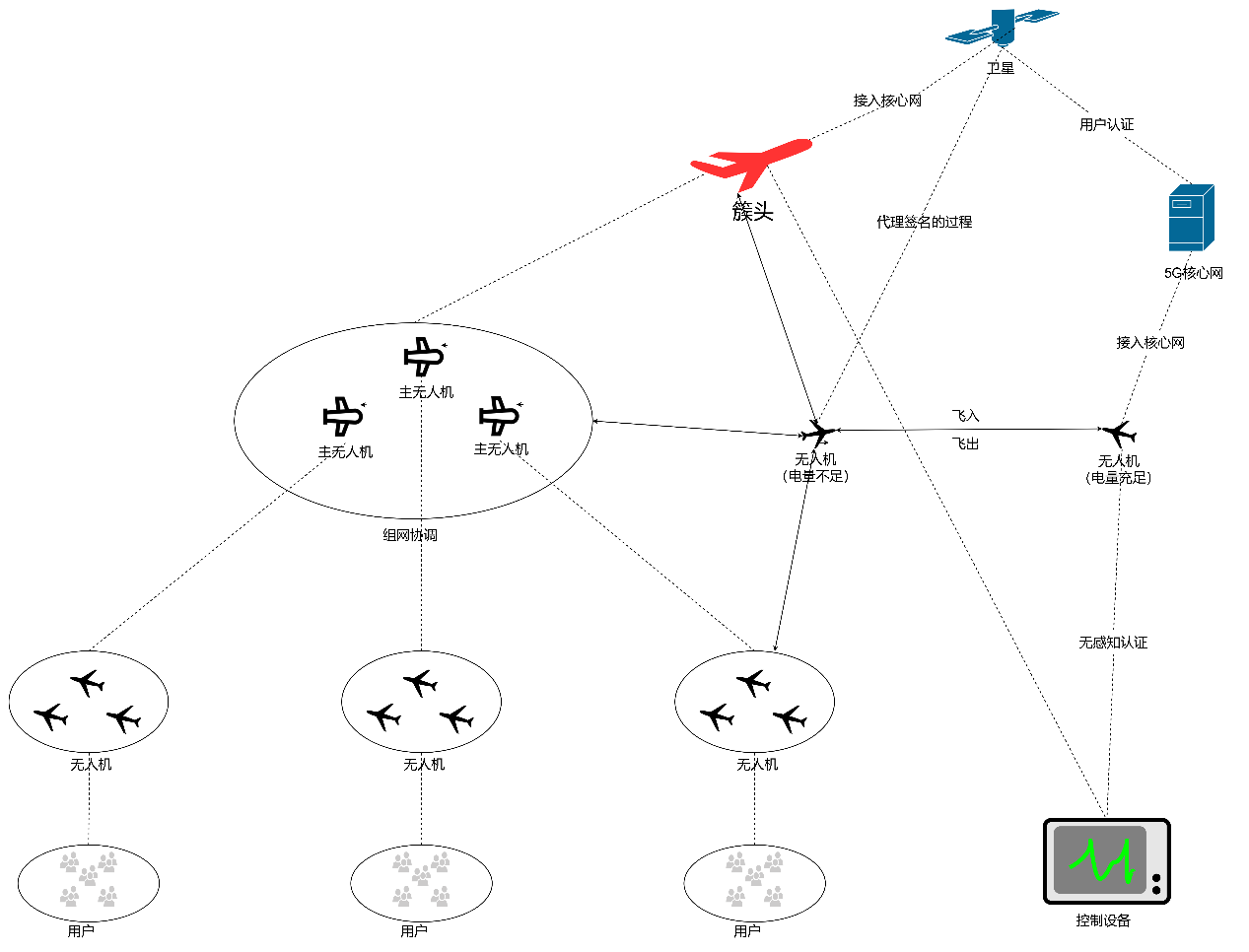


图4

优势：本方案主要具备灵活性高、机动性强、结构简单、造价低廉等特点。