(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 108062107 A
(43)申请公布日 2018.05.22

(21)申请号 201711237927.7

(22)申请日 2017.11.30

(71)申请人 中国航空工业集团公司沈阳飞机设计研究所
地址 110035 辽宁省沈阳市皇姑区塔湾街40号

(72)发明人 王兴龙 张世辉 白清源 李思凝 赵兴梅

(74)专利代理机构 北京航信高科知识产权代理事务所(普通合伙) 11526
代理人 高原

(51)Int.Cl.
G05D 1/10(2006.01)

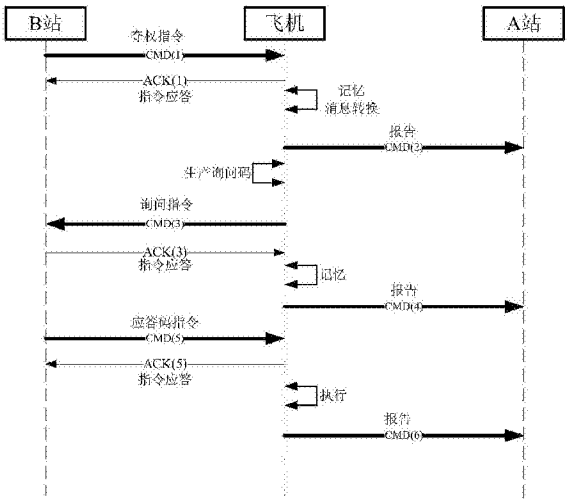
权利要求书1页 说明书4页 附图2页

(54)发明名称

一种无人机控制权变更方法

(57)摘要

本发明涉及一种无人机控制权变更方法，其包括：1)夺权--新控制方向无人机发送夺权指令，无人机接收到夺权指令后返回夺权询问验证，新控制方根据夺权密码算法以及相关验证逻辑计算夺权应答码并发送至无人机，无人机对应答码后对相同的算法及逻辑校验新控制方发送的应答码是否匹配，若匹配则新控制方取得无人机的控制权，否则，夺权失败；2)控制权正常交接--新控制方通过无人机向原控制方发送控制权申请指令，原控制方收到控制权申请指令后校验新控制方的相关信息，若符合要求则让出控制权，否则保持控制权。本发明的无人机控制权变更方法可显著提高了无人机的安全可靠性、生存概率和任务执行效率，并降低了无人机被诱骗、被干扰的风险。



CN 108062107 A

1.一种无人机控制权变更方法，其特征在于，所述无人机控制权变更方法包括：

第一：原控制方不能正常控制无人机，新控制方需要重新对无人机进行控制即为夺权

新控制方向无人机发送最高等级的夺权指令，无人机接收到夺权指令后向新控制方发起夺权询问验证，新控制方根据夺权密码算法以及相关验证逻辑计算夺权应答码并发送至无人机，无人机对应答码后对相同的算法及逻辑校验新控制方发送的应答码是否匹配，若匹配则新控制方取得无人机的控制权，否则，夺权失败；

第二：原控制方能够正常控制无人机且原控制方能够与新控制方进行通信的情况下，无人机控控制权正常交接

新控制方通过无人机向原控制方发送控制权申请指令，原控制方收到控制权申请指令后校验新控制方的相关信息，若控制方信息在控制方库集里，则原控制方同意出让无人机控制权于新控制方，否则原控制方保持对无人机的控制权。

2.根据权利要求1所述的无人机控制权变更方法，其特征在于，所述夺权密码算法采用Diffie-Hellman Key Exchange算法，夺权密码计算流程为：

a)首先新控制方向无人机发出夺权指令时，在信息中会协议约定一个质数p和一个数字g；

b)新控制方选择一个随机的秘密数字x，并计算a＝g^x mod p；

c)无人机在接收到夺权指令后，也同样选择一个随机的秘密数字y，并计算b＝g^y mod p和s＝a^y mod p，其中s值为参与夺权密码计算的随机密钥；在应答新控制方的夺权指令时，将b值与夺权询问码同步发送至新控制方；同时利用随机密钥以及夺权计算算法得到夺权密码；

d)新控制方收到应答消息后，取出b值，先计算s'＝b^x mod p，s'值与无人机计算出来的s值一样；再利用随机密钥以及夺权密码算法得到本次夺权的夺权密码；

e)通过Diffie-Hellman Key Exchange算法使无人机和新控制方在随机密钥s值不传输的前提下，实现了随机密钥的同步确认，从而实现了夺权密码的计算。

3.根据权利要求2所述的无人机控制权变更方法，其特征在于，在夺权过程中设有门限，所述门限包括夺权时间门限及夺权次数门限。

4.根据权利要求1所述的无人机控制权变更方法，其特征在于，在正常交接过程中，验证新控制方的所述相关信息包括ID地址、控制等级。

5.根据权利要求4所述的无人机控制权变更方法，其特征在于，在正常交接过程中设有应答时限。

一种无人机控制权变更方法

技术领域

[0001] 本发明属于航空技术领域，尤其涉及一种无人机控制权变更方法。

背景技术

[0002] 随着计算机、信息技术、自动驾驶技术和遥控遥测技术的进步，无人机领域也得到了极大的发展。到目前为止无人机的作用也已经超越了早期的侦察、通信中继、反辐射等作战支援任务，开始逐渐承担更为重要的任务，如攻击。但在世界范围内，经常会出现正在执行任务的无人机被非正常控制方诱骗及控制的示例，无人机被非控制方控制极度危险。

[0003] 在现有的无人机被诱骗及控制过程中，主要有以下几个原因：

[0004] a)无人机系统对于自身控制权变更的保护安全措施不到位；

[0005] b)无人机系统对它的控制方没有强有力的身份验证措施。

[0006] 伴随着现在的无人机飞行距离越来越远，其有可能超出原控制方的控制距离(如几百公里范围)，这时需要将无人机的控制权转交给距离无人机较近的控制方进行控制。原控制方在控制无人机过程中，若出现通信故障，则会失去对无人机的控制，无人机会出现丢失、坠毁等事故。在无人机控制中，若出现上述情况，一般情况下无人机则自动返航，避免上述事故的发生。为了让无人机继续完成任务，则需要对无人机控制权的变更，实现对无人机的控制以便继续完成任务。

发明内容

[0007] 本发明的目的是提供一种无人机控制权变更方法，用于解决上述问题。

[0008] 为达到上述目的，本发明采用的技术方案是：一种无人机控制权变更方法，其包括：

[0009] 第一：原控制方不能正常控制无人机，新控制方需要重新对无人机进行控制即为夺权

[0010] 新控制方向无人机发送最高等级的夺权指令，无人机接收到夺权指令后向新控制方发起夺权询问验证，新控制方根据夺权密码算法以及相关验证逻辑计算夺权应答码并发送至无人机，无人机对应答码后对相同的算法及逻辑校验新控制方发送的应答码是否匹配，若匹配则新控制方取得无人机的控制权，否则，夺权失败；

[0011] 第二：原控制方能够正常控制无人机且原控制方能够与新控制方进行通信的情况下，无人机控控制权正常交接

[0012] 新控制方通过无人机向原控制方发送控制权申请指令，原控制方收到控制权申请指令后校验新控制方的相关信息，若控制方信息在控制方库集里，则原控制方同意出让无人机控制权于新控制方，否则原控制方保持对无人机的控制权。

[0013] 进一步的，所述夺权密码算法采用Diffie-Hellman Key Exchange算法，夺权密码计算流程为：

[0014] a)首先新控制方向无人机发出夺权指令时，在信息中会协议约定一个质数p和一

个数字g；

[0015] b)新控制方选择一个随机的秘密数字x，并计算a＝g^x mod p；

[0016] c)无人机在接收到夺权指令后，也同样选择一个随机的秘密数字y，并计算b＝g^y mod p和s＝a^y mod p，其中s值为参与夺权密码计算的随机密钥；在应答新控制方的夺权指令时，将b值与夺权询问码同步发送至新控制方；同时利用随机密钥以及夺权计算算法得到夺权密码；

[0017] d)新控制方收到应答消息后，取出b值，先计算s'＝b^x mod p，s'值与无人机计算出来的s值一样；再利用随机密钥以及夺权密码算法得到本次夺权的夺权密码；

[0018] e)通过Diffie-Hellman Key Exchange算法使无人机和新控制方在随机密钥s值不传输的前提下，实现了随机密钥的同步确认，从而实现了夺权密码的计算。

[0019] 进一步的，在夺权过程中设有门限，所述门限包括夺权时间门限及夺权次数门限。

[0020] 进一步的，在正常交接过程中，验证新控制方的所述相关信息包括ID地址、控制等级。

[0021] 进一步的，在正常交接过程中设有应答时限。

[0022] 本发明的无人机控制权变更方法在无人机控制领域首次提出基于正规流程及智能加密算法的无人机控制权变更方法，显著提高了无人机的安全可靠性、生存概率和任务执行效率，并降低了无人机被诱骗、被干扰的风险。

附图说明

[0023] 此处的附图被并入说明书中并构成本说明书的一部分，示出了符合本发明的实施例，并与说明书一起用于解释本发明的原理。

[0024] 图1为夺权流程示意图。

[0025] 图2为控制权交接过程示意图。

具体实施方式

[0026] 为使本发明实施的目的、技术方案和优点更加清楚，下面将结合本发明实施例中的附图，对本发明实施例中的技术方案进行更加详细的描述。

[0027] 无人机控制权是指有控制权的控制方可以通过数据链路向无人机平台发送指令，无人机能够正常响应，同时还能接收无人机通过数据链路下传的数据信息。本发明的目的是通过规范流程及密钥算法验证提高无人机控制权变更的保护安全以及对控制方身份的强力验证，使无人机控制权变更从使用流程、无线传输、信息过滤、握手原则、校验机制、异常处理等整个流程进行了详细的设计，给出了一套完整的无人机控制权变更方法，从而解决或减少无人机被诱骗或反控制问题。

[0028] 本发明的无人机控制权变更主要包括两种情况，分别为是夺权和正常交接两种方式。

[0029] 一、夺权(原控制方不能正常控制无人机，新控制方需要重新对无人机进行控制即为夺权)

[0030] 1.1夺权流程

[0031] 如图1所示，在夺权过程中，首先夺权方(新控制方)向无人机发送最高等级的夺权

指令，无人机发出询问码，夺权方(新控制方)以询问码为种子，按照约定算法计算出验证码，并将验证码发送给无人机，无人机确认后，将新控制者进栈，服从新控制者的指控，图中A站为原控制方控制X机，B站为夺权方发起夺权操作。

[0032] 上述最高等级指的是控制权变更的相关指令，此外还有其他的等级，如重要和一般等级，重要等级一般为起飞、着落、返航等指令，一般指令为高度保持、左右遥调等指令。

[0033] 2.2夺权密码计算

[0034] 夺权密码在计算过程中需要无人机和新控制方使用相同的随机密钥以及相同的计算算法。但由于数据在无线传输过程中都有被截获及被破解的几率，为了确保夺权密码的绝对安全，使用Diffie-Hellman Key Exchange算法计算每次夺权时的随机密钥，再按照夺权计算算法，使用计算出来的随机密钥来得出最终的夺权密码。

[0035] Diffie-Hellman Key Exchange算法使用流程：

[0036] a)首先新控制方向无人机发出夺权指令时，在信息中会协议约定一个质数p和一个数字g，这两个数是基本公开的，即使该消息被截获破解也没有问题；

[0037] b)新控制方选择一个随机的秘密数字x，并计算a＝g^x mod p，这个a在信息传输时公开的；

[0038] c)无人机在接收到夺权指令后，也同样选择一个随机的秘密数字y，并计算b＝g^y mod p和s＝a^y mod p，这个b在信息传输时也是公开的，但s值是真正参与夺权密码计算的随机密钥；并在应答新控制方的夺权指令时，将b值与夺权询问码同步发送至新控制方；同时利用随机密钥以及夺权计算算法得到夺权密码；

[0039] d)新控制方收到应答消息后，取出b值，先计算s＝b^x mod p(无人机与控制方之前约定的公式，第三方无法获得)，该s值与无人机计算出来的s值一样；再利用随机密钥以及夺权计算算法得到本次夺权的夺权密码；

[0040] e)通过Diffie-Hellman Key Exchange算法使无人机和新控制方在随机密钥s值不传输的前提下，实现了随机密钥的同步确认，从而实现了夺权密码的计算，保证了夺权过程的安全可靠。

[0041] 1.3过程异常处理

[0042] 夺权过程中，由于信息都是使用无线传输，故存在信息丢失等情况，该情况下，为了不影响无人机的正常使用，设定每次夺权终止时间门限以及同一ID同一时间连续申请夺权门限次数，以确保不影响无人机的正常任务执行。上述时间门限及次数门限可根据需要进行设定。

[0043] 二、控制权正常交接

[0044] 图2所示双站控制权交接流程，控制权交接是原控制方A、新控制方B和无人机三方顺序交互的过程，其中双控制方为主动方，无人机为被动接收方。控制权正常交接的双控制方，必要都是在无人机的控制方库集里，否则无人机不受理正常交接请求。约定当控制权交接流程开始后，如果在应答时限60S内无人机未收到过程中消息，则自动退出控制权交接过程，恢复至控制权交接之前的状态。

[0045] 本发明的无人机控制权变更方法，可实现以下效果：

[0046] 1)控制权变更方法可大大降低无人机被诱骗、被干扰的风险；

[0047] 2)可实现多控制方实现对多无人机协同控制的无缝衔接及切换，提高任务执行效

率；

[0048] 3)在当前控制方出现故障不能实习对无人机有效控制时，可通过该方法让新控制方取得对无人机的控制权，提高了无人机的生存概率。

[0049] 本发明的无人机控制权变更方法在无人机控制领域首次提出基于正规流程及智能加密算法的无人机控制权变更方法，显著提高了无人机的安全可靠性、生存概率和任务执行效率，并降低了无人机被诱骗、被干扰的风险。

[0050] 以上所述，仅为本发明的最优具体实施方式，但本发明的保护范围并不局限于此，任何熟悉本技术领域的技术人员在本发明揭露的技术范围内，可轻易想到的变化或替换，都应涵盖在本发明的保护范围之内。因此，本发明的保护范围应以所述权利要求的保护范围为准。

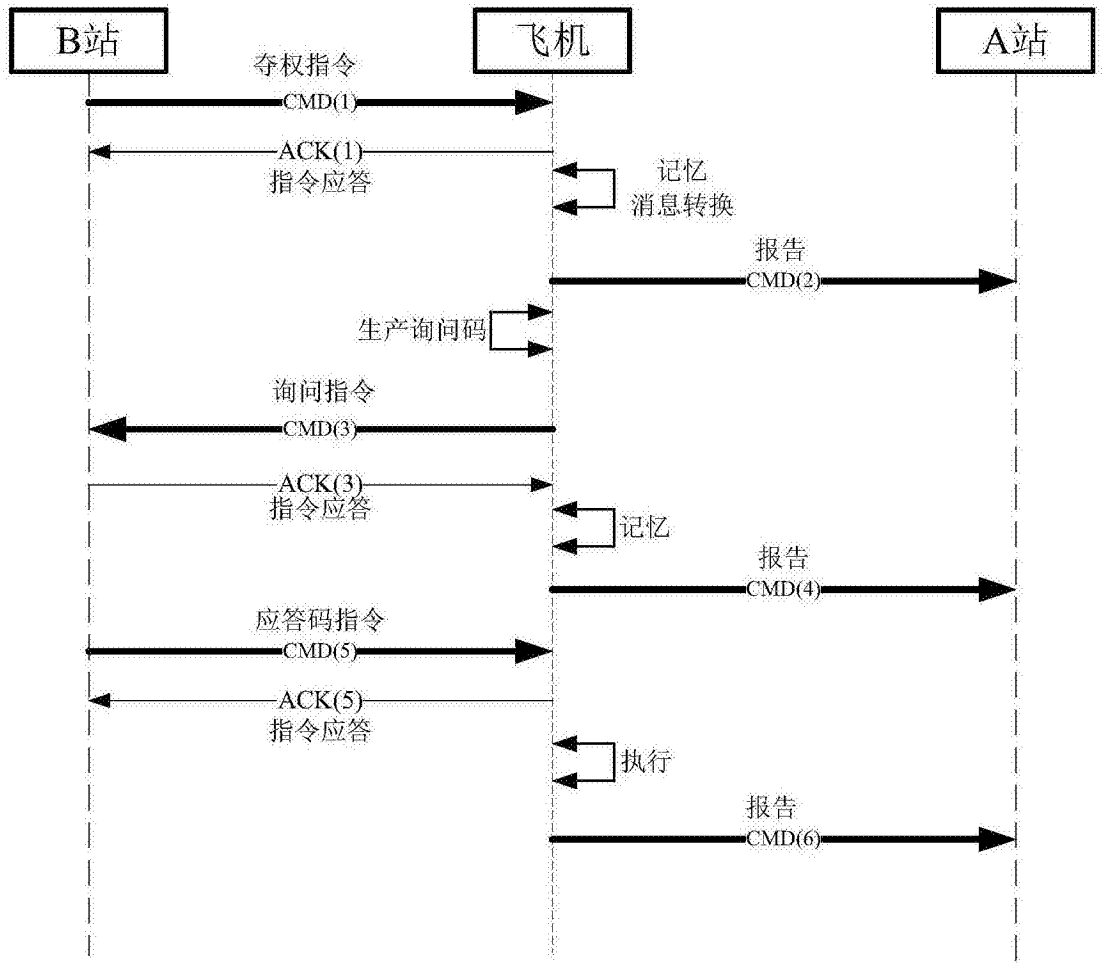

B站
飞机
A站
夺权指令
CMD(1)
ACK(1)
指令应答
记忆
消息转换
报告
CMD(2)
生产询问码
询问指令
CMD(3)
ACK(3)
指令应答
记忆
报告
CMD(4)
应答码指令
CMD(5)
ACK(5)
指令应答
执行
报告
CMD(6)

图1

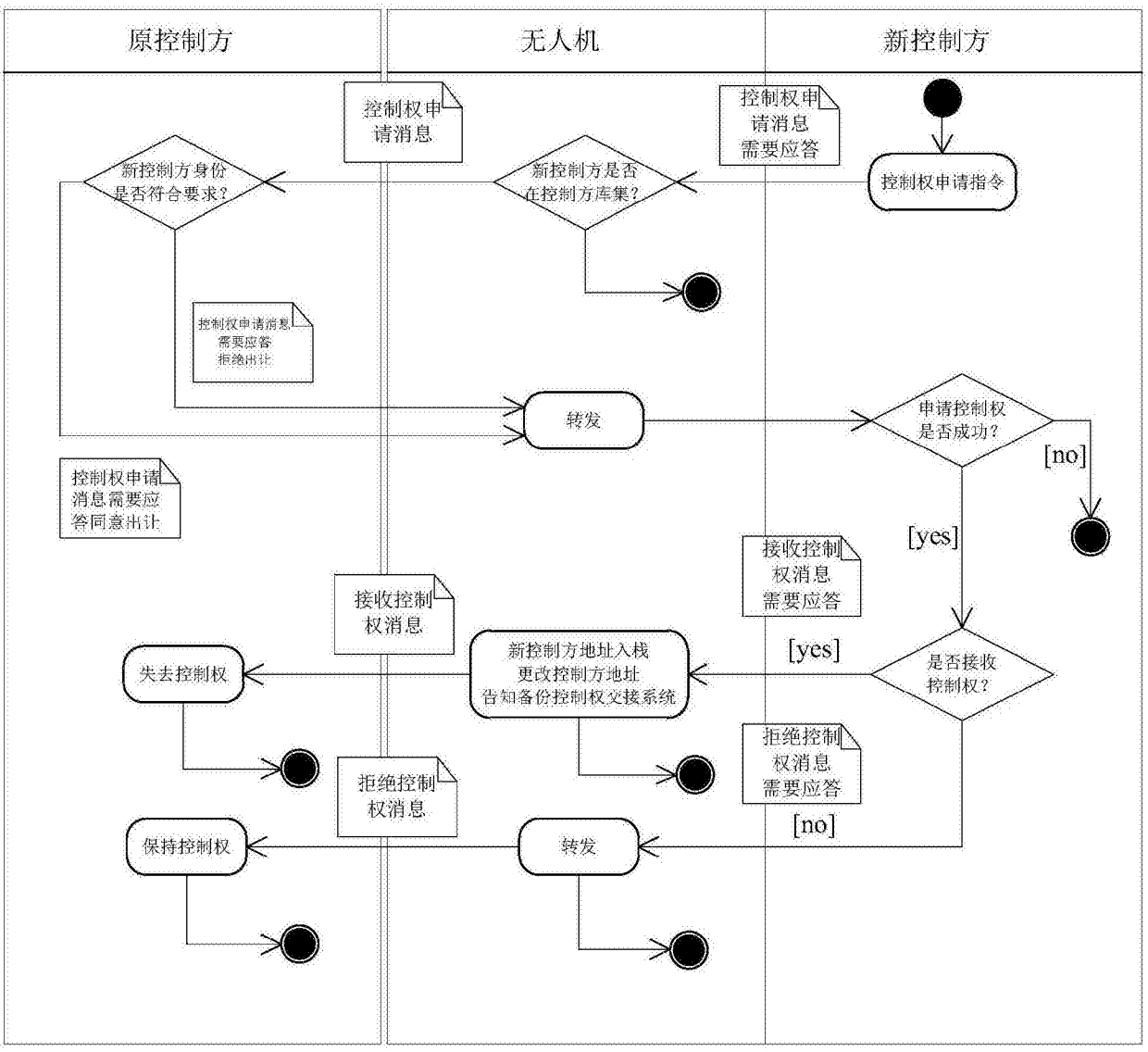

原控制方
无人机
新控制方
控制权申请消息
控制权申请消息需要应答
控制权申请指令
新控制方身份是否符合要求？
新控制方是否在控制方库集？
控制权申请消息需要应答拒绝出让
转发
申请控制权是否成功？
[no]
控制权申请消息需要应答同意出让
[yes]
接收控制权消息需要应答
接收控制权消息
[yes]
失去控制权
新控制方地址入栈更改控制方地址告知备份控制权交接系统
是否接收控制权？
拒绝控制权消息需要应答
拒绝控制权消息
[no]
保持控制权
转发

图2