

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 5 月 31 日 (31.05.2018)



(10) 国际公布号
WO 2018/094554 A1

- (51) 国际专利分类号:
B64C 39/02 (2006.01) **G05D 1/00** (2006.01)
- (21) 国际申请号: PCT/CN2016/106749
- (22) 国际申请日: 2016 年 11 月 22 日 (22.11.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (71) 申请人: 深圳前海达闼云端智能科技有限公司 (CLOUDMINDS (SHENZHEN) ROBOTICS SYSTEMS CO., LTD.) [CN/CN]; 中国北京市朝阳区望京SOHO塔3A区23层, Beijing 100102 (CN)。
- (72) 发明人: 骆磊(LUO, Lei); 中国北京市朝阳区望京SOHO塔3A区23层, Beijing 100102 (CN)。
- (74) 代理人: 北京新知远方知识产权代理事务所(普通合伙) (IPFUTURE INTELLECTUAL PROPERTY LAW OFFICE); 中国北京市海淀区花园东路10号高德大厦905徐烨, Beijing 100191 (CN)。

KE, KG, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国(除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:
— 包括国际检索报告(条约第21条(3))。

- (81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP,

(54) **Title:** METHOD FOR IMPROVING SECURITY OF UNMANNED AERIAL VEHICLE TRANSPORTATION, AND UNMANNED AERIAL VEHICLE, TERMINAL, SERVER AND COMPUTER PROGRAM PRODUCT

(54) **发明名称:** 提升无人机运输安全的方法、无人机、终端、服务器和计算机程序产品

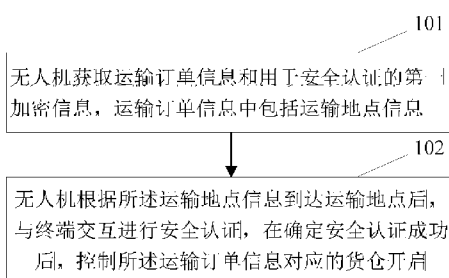


图 1

- 101 An unmanned aerial vehicle acquiring transportation order information and first encryption information for security authentication, wherein the transportation order information comprises transportation place information
- 102 After arriving at a transportation place according to the transportation place information, the unmanned aerial vehicle interacting with a terminal to perform security authentication, and after determining that the security authentication succeeds, controlling the opening of a warehouse corresponding to the transportation order information

(57) **Abstract:** A method for improving the security of unmanned aerial vehicle transportation, comprising: a server delivering encryption information for security authentication to a terminal and/or an unmanned aerial vehicle; and the terminal and the unmanned aerial vehicle performing security authentication according to the encryption information, and executing an unmanned aerial vehicle transportation task only after the security authentication is passed. Encryption information is used for security authentication, thereby reducing the risk of security authentication information being intercepted, also reducing the possibility of a terminal being masqueraded, or of mistaken collection and mistaken delivery, and improving the security of unmanned aerial vehicle transportation. Also provided are an unmanned aerial vehicle, a terminal, a server and a computer program product.

(57) **摘要:** 提升无人机运输安全的方法, 包括服务器向终端和/或无人机下发用于安全认证的加密信息, 终端和无人机根据加密信息进行安全认证, 只有在安全认证通过后才执行无人机运输任务, 由于采用加密信息进行安全认证, 降低了安全认证信息被截获的风险, 也降低了终端被冒充, 或者错取、错送的可能性, 提高了无人机运输的安全性。还提供一种无人机、终端、服务器和计算机程序产品。

WO 2018/094554 A1

提升无人机运输安全的方法、无人机、终端、服务器和计算机程序产品

技术领域

5 本发明涉及物流运输领域，特别涉及提升无人机运输安全的方法、无人机、终端和计算机程序产品。

背景技术

 随着物流业的发展和自动化的发展，采用无人机送货的方式已经初露端倪。然而，实验性质和大规模商用还有较远的距离，比如细化到取货送货的安全性方面，当前的方案还考虑的比较少，无法应对送货时冒领等事件。

10

发明内容

 本发明实施例提出了提升无人机运输安全的方法、无人机、终端、服务器和计算机程序产品，有助于提高无人机在进行货物运输时的安全性。

 本发明实施例提供的第一种提升无人机运输安全的方法，包括：

15 无人机获取运输订单信息和用于安全认证的第一加密信息，所述运输订单信息中包括运输地点信息；

 无人机根据所述运输地点信息到达运输地点后，将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并接收所述终端发来的反馈信息，根据所述反馈信息确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启；或，

20

 无人机根据所述运输地点信息到达运输地点后，接收所述运输订单信息对应用户账户登录的终端发来的第二加密信息，无人机对所述第一加密信息和第二加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启；或，

所述无人机进一步接收用于安全认证的第三加密信息，无人机根据所述运输地点信息到达运输地点后，将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并接收所述终端发来的针对所述第一加密信息的反馈信息，以及，接收所述终端发来的第二加密信息，无人机对所述第三加密信息和第二加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启。

本发明实施例提供的第二种提升无人机运输安全的方法包括：

终端根据用户的账户信息从服务器获取运输订单信息和用于安全认证的第四加密信息；

所述终端在与所述运输订单信息对应的无人机进行通讯时，将所述第四加密信息发送给所述无人机，并接收所述无人机发来的反馈信息，根据所述反馈信息确定安全认证是否成功，并显示安全认证是否成功的信息；或，

所述终端在与所述运输订单信息对应的无人机进行通讯时，接收所述无人机发来的第五加密信息，所述终端对所述第四加密信息和第五加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，并显示安全认证是否成功的信息；或，

所述终端进一步从服务器获取用于安全认证的第六加密信息，所述终端在与所述运输订单信息对应的无人机进行通讯时，将所述第四加密信息发送给所述无人机，并接收所述无人机发来的反馈信息，以及，接收所述无人机发来的第五加密信息，所述终端对所述第五加密信息和第六加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，并显示安全认证是否成功的信息。

本发明实施例提供的第三种提升无人机运输安全的方法包括：

为无人机生成运输订单信息，所述运输订单信息中包括运输地点信息；

生成用于安全认证的第一加密信息，或生成用于安全加密的第二加密信

息和第三加密信息；

将所述生成的运输订单发送给所述无人机，并将所述生成的加密信息发送给所述无人机，或发送给所述运输订单对应的用户账户登录的终端。

本发明实施例提供的第一种无人机，包括通信单元、处理单元和存储单元，其中通信单元和存储单元均通过总线与处理单元通讯；

所述通信单元用于处理单元通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元用于根据处理单元的指令存储信息；

所述处理单元用于通过所述通信单元接收运输订单信息和用于安全认证的第一加密信息，所述运输订单信息中包括运输地点信息，并存储至存储单元；以及，

在确认所述无人机到达运输地点后，读取存储单元中的第一加密信息，通过通信单元发送给所述运输订单信息对应用户账户登录的终端，并通过所述通信单元接收所述终端发来的反馈信息，根据所述反馈信息确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令；

或者，在确认所述无人机到达运输地点后，通过通信单元接收所述运输订单信息对应用户账户登录的终端发来的第二加密信息，读取所述存储的第一加密信息，并将所述第一加密信息和第二加密信息分别解密和进行对比，根据对比结果确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令；或，

或者，所述通信单元进一步用于通过通信单元接收用于安全认证的第三加密信息，在确认所述无人机到达运输地点后，从存储单元中读取所述第一加密信息，通过通信单元将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并通过通信单元接收所述终端发来的针对所述第一加密信息的反馈信息，以及，通过通信单元接收所述终端发来的第二加密信息，

将所述第三加密信息和第二加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令。

5 本发明实施例提供的第一种终端，包括通信单元、处理单元、存储单元和显示单元，其中通信单元、存储单元和显示单元均通过总线与处理单元通讯；

所述通信单元用于处理单元通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元用于根据处理单元的指令存储信息；

10 所述显示单元用于根据处理单元的指令显示信息；

所述处理单元用于通过通信单元从服务器获取运输订单信息和用于安全认证的第四加密信息，并存储至存储单元；以及，

在通过通信单元与所述运输订单信息对应的无人机进行通讯时，读取存储单元中的所述第四加密信息，通过通信单元将所述第四加密信息发送给所述无人机，并通过通信单元接收所述无人机发来的反馈信息，根据所述反馈信息确定安全认证是否成功，指示显示单元显示安全认证是否成功的信息；
15 或，

在通过通信单元与所述运输订单信息对应的无人机进行通讯时，通过通信单元接收所述无人机发来的第五加密信息，读取存储单元中存储的第四加密信息，将所述第四加密信息和第五加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，并指示显示单元显示安全认证是否成功的信息；或，
20

所述处理单元进一步用于通过通信单元从服务器获取用于安全认证的第六加密信息，以及在通过通信单元与所述运输订单信息对应的无人机进行通讯时，读取存储单元中存储的第四加密信息，通过通信单元将所述第四加密信息发送给所述无人机，并通过通信单元接收所述无人机发来的反馈信息，
25

以及，通过通信单元接收所述无人机发来的第五加密信息，对所述第五加密信息和第六加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，并指示显示单元显示安全认证是否成功的信息。

5 本发明实施例提供的第一种服务器，包括：通信单元、处理单元和存储单元，其中通信单元和存储单元均通过总线与处理单元通讯；

所述通信单元用于处理单元通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元用于根据处理单元的指令存储信息；

10 所述处理单元用于为无人机生成包括运输地点信息的运输订单，并生成用于安全认证的第一加密信息，或生成用于安全认证的第二和第三加密信息，并通过通信单元将所述生成的运输订单发送给所述无人机，以及通过通信单元将所述生成的加密信息发送给无人机或所述运输订单对应的用户账户登录的终端。

15 本发明实施例提供的第二种无人机，包括存储器、一个或多个处理器；以及一个或多个模块，所述一个或多个模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行上述第一种提升无人机运输安全方法中各个步骤的指令。

20 本发明实施例提供的第二种终端，包括显示器，存储器，收发器，一个或多个处理器；以及一个或多个模块，所述一个或多个模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行上述第二种提升无人机运输安全方法中各个步骤的指令。

25 本发明实施例提供的第二种服务器，包括：存储器，收发器，一个或多个处理器；以及一个或多个模块，所述一个或多个模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行杉树第三种提升无人机运输安全方法中各个步骤的指令。

本发明实施例还提供了一种与无人机结合使用的计算机程序产品，包括

计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述第一种提升无人机运输安全方法中各个步骤的指令。

5 本发明实施例还提供了一种与电子设备结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述第二种提升无人机运输安全方法中各个步骤的指令。

本发明实施例还提供了一种与服务器结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述第三种提升无人机运输安全方法
10 中各个步骤的指令。

通过上述第一种提升无人机运输安全方法、各种无人机，和与无人机结合的计算机程序产品的方案中，无人机获取加密信息，并根据加密信息与终端交互进行安全认证，只有在安全认证通过后才开启货仓完成运输任务，由于采用加密信息进行安全认证，降低了安全认证信息被截获的风险，也降低
15 了终端被冒充，或者错取、错送的可能性，提高了无人机运输的安全性。

通过上述第二种提升无人机运输安全方法、各种终端，和与电子设备结合的计算机程序产品的方案中，终端根据用户账户信息获取加密信息，并根据加密信息与无人机交互进行安全认证，以及将认证结果信息通知给用户，由于采用加密信息进行安全认证，降低了安全认证信息被截获的风险，降低
20 了无人机被冒充或者错收、错发货物的可能性，提高了无人机运输的安全性。

通过上述第三种提升无人机运输安全方法、各种服务器，和与服务器结合的计算机程序产品的方案中，服务器生成加密信息并下发给用户账户登录终端和/或无人机，使得后续可以通过加密信息进行运输安全认证，从而降低了安全认证信息被截获的风险，降低了无人机被冒充或者错收、错发货物的
25 可能性，提高了无人机运输的安全性。

附图说明

下面将参照附图描述本发明的具体实施例，其中：

图1示出了本发明实施例提供的第一种提升无人机运输安全的方法的流程示意图；

图2示出了本发明实施例提供的第二种提升无人机运输安全的方法的流程示意图；

图3示出了本发明实施例提供的第二种提升无人机运输安全的方法的流程示意图；

图4示出了本发明实施例提供的第一种无人机的结构示意图；

图5示出了本发明实施例提供的第一种终端的结构示意图；

图6示出了本发明实施例提供的第一种服务器的结构示意图；

图7示出了本发明实施例提供的第二种无人机的结构示意图；

图8示出了本发明实施例提供的第二种终端的结构示意图；

图9示出了本发明实施例提供的第二种服务器的结构示意图；

图10示出了本发明一种较佳的无人机取货实施方式的流程示意图；

图11示出了本发明另一种较佳的无人机取货实施方式的流程示意图；

图12示出了本发明一种无人机送货方法的具体实施方式的流程示意图；

图13示出了无人机送货方法的另一种具体实施方式的流程示意图；

图14示出了无人机送货方法的再一种具体实施方式的流程示意图；

图15示出了本发明无人机的一个示例性实施方式的结构示意图；

图16示出了图15所示的无人机的示例性实施方式的一种具体实现方案的结构示意图；

图17示出了本发明无人机的再一种实施方式的结构示意图；

图18示出了本发明一种终端实施方式的结构示意图；

图19示出了本发明一种服务器实施方式的结构示意图。

25 具体实施方式

为了使本发明的技术方案及优点更加清楚明白，以下结合附图对本发明

的示例性实施例进行进一步详细的说明，显然，所描述的实施例仅是本发明的一部分实施例，而不是所有实施例的穷举。并且在不冲突的情况下，本说明中的实施例及实施例中的特征可以互相结合。

5 本发明实施例中，在取货时，通过用户在线物流订单生成时刻的时间戳和无人机被指派取货时刻的时间戳两个信息进行双向验证，或基于其中至少一个时间戳进行单向验证，无人机要验证的是用户是否为物流订单的真实申请方，用户要验证的是无人机是否为约定取货的正确无人机，以防止误取件或者恶意冒充无人机骗取用户物品。

10 在送货时，一种实施方式中，无人机采用语音问答的方式，以用户的答案和物流订单信息进行比对验证，以确定确实为收件人，同时拍照或录像。

15 另一种实施方式中，与取货类似，也可以通过在线物流订单生成时刻的时间戳和无人机被指派取货时刻的时间戳两个信息进行双向验证，或基于其中至少一个时间戳进行单向验证，无人机要验证的是用户是否为正确的收货人，收货人要验证的是此无人机是否为约定送货的无人机，以防止他人冒充用户骗收物品，或无人机错送，用户错收他人物品。

本发明中的无人机可以是无人飞行器，也可以是无人驾驶汽车或其他无人驾驶的运输工具，后续各较佳实施方式中，均是以无人飞行器执行运输任务的场景所描述的，在应用于其他无人驾驶等场景中时，除具体的运输方式不同外，其余涉及订单交互和认证的流程均相同。

20 较佳地，如图 1 所示，本发明实施例提供的第一种提升无人机运输安全的方法，包括：

步骤 101、无人机获取运输订单信息和用于安全认证的第一加密信息，所述运输订单信息中包括运输地点信息；

25 步骤 102、无人机根据所述运输地点信息到达运输地点后，将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并接收所述终端发来的反馈信息，根据所述反馈信息确定安全认证是否成功，在确定成功后，

控制所述运输订单信息对应的货仓开启；或，

无人机根据所述运输地点信息到达运输地点后，接收所述运输订单信息对应用户账户登录的终端发来的第二加密信息，无人机对所述第一加密信息和第二加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，

5 在确定成功后，控制所述运输订单信息对应的货仓开启；或，

所述无人机进一步接收用于安全认证的第三加密信息，无人机根据所述运输地点信息到达运输地点后，将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并接收所述终端发来的针对所述第一加密信息的反馈信息，以及，接收所述终端发来的第二加密信息，无人机对所述第三加密信息和第二加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启。

较佳地，上述针对所述第一加密信息的反馈信息包括：对所述第一加密信息验证是否通过的信息；

15 或者，针对所述第一加密信息的反馈信息包括：所述第一加密信息解密后的信息；则接收所述反馈信息后进一步包括：将所述第一加密信息解密后的信息发送给服务器，并接收服务器反馈的针对所述加密后的信息验证是否通过的信息；则所述根据反馈信息确定安全认证是否成功包括：根据所述服务器反馈的验证是否通过的信息确定安全认证是否成功。

20 较佳地，所述发送给终端的第一加密信息包括：用所述运输订单对应用户账户的公钥加密的信息；

所述第二加密信息包括：用所述无人机的公钥加密的信息；

所述无人机解密的第一加密信息或第三加密信息包括：用所述无人机的公钥加密的信息。

25 所述运输订单为取货订单或送货订单；较佳地，

各加密信息中被加密的信息均可以包括：所述运输订单生成时刻的时间

戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

较佳地，如图 2 所示，本发明实施例提供的第二种提升无人机运输安全的方法包括：

步骤 201、终端根据用户的账户信息从服务器获取运输订单信息和用于安全认证的第四加密信息；

步骤 202、所述终端在与所述运输订单信息对应的无人机进行通讯时，将所述第四加密信息发送给所述无人机，并接收所述无人机发来的反馈信息，根据所述反馈信息确定安全认证是否成功，并显示安全认证是否成功的信息；或，

所述终端在与所述运输订单信息对应的无人机进行通讯时，接收所述无人机发来的第五加密信息，所述终端对所述第四加密信息和第五加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，并显示安全认证是否成功的信息；或，

所述终端进一步从服务器获取用于安全认证的第六加密信息，所述终端在与所述运输订单信息对应的无人机进行通讯时，将所述第四加密信息发送给所述无人机，并接收所述无人机发来的反馈信息，以及，接收所述无人机发来的第五加密信息，所述终端对所述第五加密信息和第六加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，并显示安全认证是否成功的信息。

所述针对所述第四加密信息的反馈信息包括：对所述第四加密信息验证是否通过的信息；

或者，针对所述第四加密信息的反馈信息包括：所述第四加密信息解密后的信息；则接收所述反馈信息后进一步包括：将所述第四加密信息解密后的信息发送给服务器，并接收服务器反馈的针对所述加密后的信息验证是否通过的信息；则所述根据反馈信息确定安全认证是否成功包括：根据所述服务器反馈的验证是否通过的信息确定安全认证是否成功。

较佳地，所述发送给无人机的第四加密信息包括：用所述无人机的公钥加密的信息；

所述第五加密信息包括：用所述用户账户的公钥加密的信息；

所述终端解密的第四加密信息和第六加密信息包括：用所述用户账户的公钥加密的信息。

所述运输订单可以为取货订单，或送货订单；较佳地，各加密信息中被加密的信息均可以包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

如图 3 所示，本发明实施例提供的第三种提升无人机运输安全的方法包括：

步骤 301、为无人机生成运输订单信息，所述运输订单信息中包括运输地点信息；

步骤 302、生成用于安全认证的第一加密信息，或生成用于安全加密的第二加密信息和第三加密信息；

步骤 303、将所述生成的运输订单发送给所述无人机，并将所述生成的加密信息发送给所述无人机，或发送给所述运输订单对应的用户账户登录的终端。

所述发送加密信息的步骤后，进一步可以包括：接收所述无人机或所述终端发送的解密信息，并对解密信息进行安全认证，然后向所述无人机或所述终端反馈安全认证结果。

所述发送给无人机的第一加密信息可以包括：用所述用户账户的公钥加密的信息；

所述发送给用户账户登录的终端的第一加密信息可以包括：用所述无人机的公钥加密的信息；

所述第二加密信息和第三加密信息可以分别包括用所述无人机的公钥加密的信息和用所述用户账户的公钥加密的信息。

所述运输订单为取货订单，或送货订单；较佳地，各加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或所述服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

如图 4 所示，本发明实施例提供的第一种无人机，包括处理单元 41、通信单元 42 和存储单元 43，其中通信单元 42 和存储单元 43 均通过总线与处理单元 41 通讯；

所述通信单元 42 用于处理单元 41 通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元 43 用于根据处理单元 41 的指令存储信息；

所述处理单元 41 用于通过所述通信单元 42 接收运输订单信息和用于安全认证的第一加密信息，所述运输订单信息中包括运输地点信息，并存储至存储单元 43；以及，

在确认所述无人机到达运输地点后，读取存储单元 43 中的第一加密信息，通过通信单元 42 发送给所述运输订单信息对应用户账户登录的终端，并通过所述通信单元 42 接收所述终端发来的反馈信息，根据所述反馈信息确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令；

或者，在确认所述无人机到达运输地点后，通过通信单元 42 接收所述运输订单信息对应用户账户登录的终端发来的第二加密信息，读取所述存储的第一加密信息，并将所述第一加密信息和第二加密信息分别解密和进行对比，根据对比结果确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令；或，

或者，所述通信单元 42 进一步用于通过通信单元 42 接收用于安全认证的第三加密信息，在确认所述无人机到达运输地点后，从存储单元 43 中读取所述第一加密信息，通过通信单元 42 将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并通过通信单元 42 接收所述终端发来的针

对所述第一加密信息的反馈信息，以及，通过通信单元 42 接收所述终端发来的第二加密信息，将所述第三加密信息和第二加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令。

5 较佳地，所述针对所述第一加密信息的反馈信息可以包括：对所述第一加密信息验证是否通过的信息；

或者，针对所述第一加密信息的反馈信息也可以包括：所述第一加密信息解密后的信息；则所述处理单元 41 通过所述通信单元 42 进一步用于：通过通信单元 42 将所述第一加密信息解密后的信息发送给服务器，并通过通信
10 单元 42 接收服务器反馈的针对所述加密后的信息验证是否通过的信息；则所述通信单元 42 用于根据反馈信息确定安全认证是否成功包括：所述通信单元 42 用于根据所述服务器反馈的验证是否通过的信息确定安全认证是否成功。

较佳地，所述发送给终端的第一加密信息包括：用所述运输订单对应用户账户的公钥加密的信息；

15 所述第二加密信息包括：用所述无人机的公钥加密的信息；

所述处理单元 41 解密的第一加密信息或第三加密信息包括：用所述无人机的公钥加密的信息。

所述运输订单可以为取货订单，也可以为送货订单；较佳地，各加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。
20

图 5 示出了本发明实施例提供的第一种终端，如图 5 所示，该终端包括通信单元 52、处理单元 51、存储单元 53 和显示单元 54，其中通信单元 52、存储单元 53 和显示单元 54 均通过总线与处理单元 51 通讯；

所述通信单元 52 用于处理单元 51 通过其接收来自外部设备的信息，或
25 向外部设备发送信息；

所述存储单元 53 用于根据处理单元 51 的指令存储信息；

所述显示单元 54 用于根据处理单元 51 的指令显示信息；

所述处理单元 51 用于通过通信单元 52 从服务器获取运输订单信息和用于安全认证的第四加密信息，并存储至存储单元 53；以及，

在通过通信单元 52 与所述运输订单信息对应的无人机进行通讯时，读取
5 存储单元 53 中的所述第四加密信息，通过通信单元 52 将所述第四加密信息发送给所述无人机，并通过通信单元 52 接收所述无人机发来的反馈信息，根据所述反馈信息确定安全认证是否成功，指示显示单元 54 显示安全认证是否成功的信息；或，

在通过通信单元 52 与所述运输订单信息对应的无人机进行通讯时，通过
10 通信单元 52 接收所述无人机发来的第五加密信息，读取存储单元 53 中存储的第四加密信息，将所述第四加密信息和第五加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，并指示显示单元 54 显示安全认证是否成功的信息；或，

所述处理单元 51 进一步用于通过通信单元 52 从服务器获取用于安全认
15 证的第六加密信息，以及在通过通信单元 52 与所述运输订单信息对应的无人机进行通讯时，读取存储单元 53 中存储的第四加密信息，通过通信单元 52 将所述第四加密信息发送给所述无人机，并通过通信单元 52 接收所述无人机发来的反馈信息，以及，通过通信单元 52 接收所述无人机发来的第五加密信息，对所述第五加密信息和第六加密信息分别解密并进行对比，根据对比结
20 果和所述反馈信息确定安全认证是否成功，并指示显示单元 54 显示安全认证是否成功的信息。

较佳地，所述针对所述第四加密信息的反馈信息包括：对所述第四加密信息验证是否通过的信息；

或者，针对所述第四加密信息的反馈信息包括：所述第四加密信息解密
25 后的信息；则所述通信单元 52 进一步用于：将所述第四加密信息解密后的信息通过所述通信单元 52 发送给服务器，并通过通信单元 52 接收服务器反馈

的针对所述加密后的信息验证是否通过的信息；则所述通信单元 52 用于根据反馈信息确定安全认证是否成功包括：所述通信单元 52 用于根据所述服务器反馈的验证是否通过的信息确定安全认证是否成功。

5 较佳地，所述发送给无人机的第四加密信息包括：用所述无人机的公钥加密的信息；

所述第五加密信息包括：用所述用户账户的公钥加密的信息；

所述终端解密的第四加密信息或第六加密信息包括：用所述用户账户的公钥加密的信息。

10 所述运输订单可以为取货订单，也可以为送货订单；较佳地，所述第四加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第五加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

15 所述第六加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

图 6 示出了本发明实施例提供的第一种服务器，如图 6 所示，该服务器包括：处理单元 61、通信单元 62 和存储单元 63，其中通信单元 62 和存储单元 63 均通过总线与处理单元 61 通讯；

20 所述通信单元 62 用于处理单元 61 通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元 63 用于根据处理单元 61 的指令存储信息；

所述处理单元 61 用于为无人机生成包括运输地点信息的运输订单，并生成用于安全认证的第一加密信息，或生成用于安全认证的第二和第三加密信息，并通过通信单元 62 将所述生成的运输订单发送给所述无人机，以及通过
25 通信单元 62 将所述生成的加密信息发送给无人机或所述运输订单对应的用户账户登录的终端。

较佳地，所述服务器的处理单元 61 进一步用于通过通信单元 62 接收所述无人机或所述终端发送的解密信息，并对解密信息进行安全认证，然后通过所述通信单元 62 向所述无人机或所述终端反馈安全认证结果。

较佳地，所述发送给无人机的第一加密信息为：用所述用户账户的公钥加密的信息；

所述发送给用户账户登录的终端的第一加密信息包括：用所述无人机的公钥加密的信息；

所述第二加密信息和第三加密信息分别包括用所述无人机的公钥加密的信息和用所述用户账户的公钥加密的信息。

所述运输订单为取货订单，或送货订单。

较佳地，所述第一加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或所述服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第二加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第三加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

图 7 示出了本发明实施例提供的第二种无人机，如图 7 所示，该无人机包括存储器 71、收发器 72、一个或多个处理器 73；以及一个或多个模块，所述一个或多个模块被存储在所述存储器 71 中，并被配置成由所述一个或多个处理器 73 执行，所述一个或多个模块包括用于执行上述第一种提升无人机运输安全方法中各个步骤的指令。

图 8 示出了本发明实施例提供的第二种终端，如图 8 所示，该终端包括显示器 81，存储器 82，收发器 83，一个或多个处理器 84；以及一个或多个模块，所述一个或多个模块被存储在所述存储器 82 中，并被配置成由所述一个或多个处理器 84 执行，所述一个或多个模块包括用于执行上述第二种提升

无人机运输安全方法中各个步骤的指令。

图 9 示出了本发明实施例提供的第二种服务器，如图 9 所示，该服务器包括：存储器 91，收发器 92，一个或多个处理器 93；以及一个或多个模块，所述一个或多个模块被存储在所述存储器 91 中，并被配置成由所述一个或多个处理器 93 执行，所述一个或多个模块包括用于执行上述第三种提升无人机运输安全方法中各个步骤的指令。

本发明实施例还提供了一种与无人机结合使用的计算机程序产品，包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述第一种提升无人机运输安全方法中各个步骤的指令。

本发明实施例还提供了一种与电子设备结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述第二种提升无人机运输安全方法中各个步骤的指令。

本发明实施例还提供了一种与服务器结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述第三种提升无人机运输安全方法中各个步骤的指令。

以下分别通过较佳实施方式对本发明实施例的技术方案进一步阐明。

图 10 示出了一个较佳的无人机取货实施方式，该实施方式中，由发货用户通过登录的终端与无人机进行相互认证，提高运输安全性。该实施方式具体包括如下步骤：

步骤 1001、终端根据用户通过在客户端应用（APP）进行的操作，获取物流订单的相关信息，包括发货人地址、收货人地址，货物信息，联系方式等传统物流信息，并生成物流订单呈现给用户，供用户确认提交至网络侧的服务器。

在替代实现方式中，用户也可以通过物流系统提供的网页等其他常见方

式进行相关的物流操作。

当然，无论是用户通过网页方式操作，或者通过客户端方式操作，用户都需在提交前进行账户登录，终端与网络侧的服务器完成登录交互后，才能提交订单信息。

5 这里网络侧的服务器可以是物流系统的网络侧服务器，用于与用户登录的终端交互物流相关信息、订单信息、指派无人机等。其中，用于与终端交互的物流相关信息、订单信息的服务单元与指派无人机的服务单元可以集成于一个物理的服务器中，也可以分别是独立的物理服务器，也可以利用云计算等技术，通过分布式服务器实现，这些具体的实现方式均为计算机网络领
10 域的通用技术，这里不再赘述。

当然，当本发明应用于除提供物流服务器还提供商品销售服务的网络侧系统时，与终端交互的服务单元也可以与提供商品销售服务的服务器单元集成在一起，指派无人机的服务单元单独设置，同样，这些服务单元也均可以通过云计算等技术，通过分布式服务器实现。

15 步骤 1002、网络侧的服务器在接收到用户物流订单，并确认订单成功后，生成该确认订单成功时刻的时间戳 T1。

步骤 1003、服务器根据用户物流订单，指派进行取货的无人机生成取货订单，并记录无人机被指派时刻的时间戳 T2。

服务器在指派无人机时，会根据用户物流订单生成运输订单，在取货的
20 各个实施例中，为清楚起见，将其称为取货订单，并在指派指令中将取货订单信息发送给无人机，该取货订单信息中至少包括运输地点信息，在取货的各个实施例中，将其称为发货人地址信息。另外，本实施例和本发明的其他实施例中，若无人机专用于取货或专用于送货，则服务器发送给无人机的取货订单信息或送货订单信息中无需包括运输类型信息（用于标识该运输任务
25 时取货或送货的信息）；若无人机即用于取货又用于送货，则服务器发送给无人机的取货订单信息或送货订单信息中还包括运输类型信息。

本步骤中，无人机被指派时刻的时间戳，也即取货订单生成时刻的时间戳。

步骤 1004、服务器采用非对称加密方式，将时间戳 T1 用所指派的无人机的公钥加密，将时间戳 T2 用上述用户账户的公钥加密，然后分别将加密后的时间戳 T1 和加密后的时间戳 T2 发送给所指派的无人机和上述用户登录的终端。

本步骤，下发给无人机的加密时间戳可以随同对无人机的指派指令一同下发，也可以通过专门的消息另行下发。下发给用户登录的终端的信息，可以通过单独的消息下发，也可以随同该流程执行过程中的其他与终端的消息一同下发。

在替代实施方式中，也可以将时间戳 T1 和时间戳 T2 进行调换，即 T1 用用户账户的公钥加密，T2 用无人机的公钥加密，只需在认证过程中也同样进行调换即可。

较佳地，本实施方式和本发明的其他各实施方式中，在用户通过终端上的客户端应用或者网页注册至服务器时，或者无人机注册至上述服务器时，服务器均可以为用户账户或无人机配置和保存公钥私钥对，并将为用户账户配置的私钥发送给用户注册的终端和后续登录的终端，将为无人机配置的私钥发送给对应的无人机。

步骤 1005、所指派的无人机按照物流订单中的地点信息和时间信息至取货地点取货，并将自身的位置信息反馈给服务器，同时服务器在用户通过登录的终端发起无人机位置查询时，将无人机的位置、时间信息发送给用户当时登录的终端。

本实施方式和本发明的其他各实施方式中，无人机上可以携带 GPS 或其他专门的定位模块，或者也可以通过无线通信网络进行定位，以获取自身的位置信息。

步骤 1006、无人机到达取货地点后，将自身中加密后的时间戳 T2 传送给

用户登录的终端，同时用户通过登录的终端将自身中加密后的时间戳 T1 传送给无人机，并分别根据接收到的加密时间戳进行身份认证。

具体地，本步骤中，在无人机到达取货地点后，无人机开始拍照或录像，用户登录的终端从无人机获取订单号信息，验证该到达的无人机是否是为该用户相应订单指派的无人机。

终端在验证无人机成功后，将加密后的时间戳 T1 传送给无人机，同时无人机将加密后的时间戳 T2 传送给终端。

终端和无人机在收到对方发来的加密时间戳后，利用自身的私钥解密接收的加密时间戳，并将其与解密后的来自服务器的相应时间戳进行比对，如果一致，则对方通过身份验证。

即，终端用自身的私钥解开自己之前从服务器得到的 T2 信息和刚刚接收到的 T2 信息并进行比对，如果时间戳相同，则认为此无人机就是指派给该终端的无人机。同时，无人机用自己的私钥解开自己之前从服务器得到的 T1 信息和刚刚接收到的 T1 信息并进行比对，如果时间戳相同，则认为此用户就是此物流订单的发起人。如果终端验证 T2 不通过，则判定此无人机并非系统指派无人机，很可能为其他人的无人机恶意骗取，在步骤 1008 结束取货流程；如果无人机验证 T1 不通过或终端提供不了 T1 信息，则判定此终端并非此订单发起终端，此时不应取货，也在步骤 1008 结束取货流程。

较佳地，本步骤中，终端和无人机的之间的通信可以通过各种无线通信方式完成。在本实施方式中，较佳地，可以采用蓝牙、非接触式射频识别(NFC)方式，或者通过扫描识别编码（如二维码或条形码）等直接交互方式，其相对于通过无线网络进行通信可以进一步提升安全性。

步骤 1007、双方身份验证通过后，则无人机自动解锁并开启该运输订单信息对应的货仓，由用户将物品放入指定空间位置，确认完成放入后，锁闭货仓，取货完成。

本步骤中，若无人机只有一个货仓，则指开启该货仓，若存在多个货仓，

且分别对应不同的运输订单，则只开启该运输订单信息对应的货仓。

本步骤中，取货完成后无人机可以飞往物流集散点、下一个取货点，或者在判断出目的地同城且距离较近时，可直接送货。

步骤 1008、若双方身份验证未通过，结束取货流程。

- 5 本步骤中，若终端验证 T2 不通过，将不通过的信息反馈给服务器，并等待正确的无人机到达；若无人机验证 T1 不通过或未接收到来自终端的加密 T1 信息，则无人机将验证失败信息反馈给服务器，并根据服务器反馈的指令飞回物流集散点、飞往下一个取货点，或者原地等待。

10 以上本实施方式以及本发明其他实施方式中，涉及到物流订单操作，以及无人机指派等相关物流处理的流程可以采用现有的任意实现方式，本发明中对其不进行限定。

本实施方式以及本发明其他各实施方式中，终端或无人机与服务器之间可以通过 5G、4G、3G、GPRS 或 WiFi 等各种无线通信网络进行通信，在此不做限定。

- 15 另外，上述时间戳 T1 和时间戳 T2 是本实施方式和其他实施方式中的较佳实现方案，采用该方案可以使安全信息与订单吻合度更好。该两时间戳也可以采用其他时间戳替代，只要服务器生成两个不同的时间戳，分别用上述终端和无人机的公钥加密发送给两个设备以供验证即可实现提高无人机运输安全性的技术效果。

- 20 图 11 示出了另一较佳的无人机取货实施方式，该方式中，由服务器完成对用户的终端和无人机的身份认证，提升运输安全性。该实施方式中的步骤 1101 至步骤 1103 与步骤 1001 至步骤 1003 相同，这里不再赘述，在步骤 1103 后，包括以下步骤：

- 25 步骤 1104、服务器采用非对称加密方式，将时间戳 T1 通过用户账户的公钥加密，将时间戳 T2 用所指派的无人机的公钥加密，然后分别将加密后的时间戳 T1 发送给所指派的无人机，将加密后的时间戳 T2 发送给用户登录的终

端。

在替代实施方式中，也可以将时间戳 T1 和时间戳 T2 进行调换，即 T1 用无人机公钥加密，T2 用终端公钥加密，则加密后的时间戳 T1 发送给用户登录的终端，加密后的时间戳 T2 发送给无人机，后续认证过程中也进行类似调换，这里不再赘述。

步骤 1105、所指派的无人机按照物流订单中的地点信息和时间信息至取货地点取货，并将自身的位置信息反馈给服务器，同时服务器在用户通过登录的终端发起无人机位置查询时，将无人机的位置、时间信息发送给用户当时登录的终端。

步骤 1106、无人机到达取货地点后，将自身中加密后的时间戳 T1 传送给用户登录的终端，同时用户登录的终端将自身中加密后的时间戳 T2 传送给无人机。

具体地，本步骤中，在无人机到达取货地点后，无人机开始拍照或录像，用户通过登录的终端从无人机获取订单号信息，验证该到达的无人机是否是为该用户相应订单指派的无人机。

终端在验证无人机成功后，将加密后的时间戳 T2 传送给无人机，同时无人机将加密后的时间戳 T1 传送给终端。

步骤 1107、终端和无人机在收到对方发来的加密时间戳后，利用自身中的相应私钥解密接收的加密时间戳，并将解密后的时间戳反馈给对方。

本步骤中，终端和无人机之一如果解密不成功，则直接结束该次取货流程，或者将解密失败信息反馈给对方和/或上传给服务器，并结束该流程。

若终端和无人机一方解密成功，但收到另一方解密失败的消息，或通过服务器接收到对方解密失败的消息，则结束该取货流程。

步骤 1108、终端和无人机接收到解密后的时间戳后，分别将解密后的时间戳上传给服务器。

步骤 1109、服务器将接收到的解密时间戳与自身记录的时间戳进行比对，

检验终端和无人机上传的时间戳是否正确，以对两者进行身份认证，并将认证结果反馈给无人机和终端。

本步骤中，如果终端和无人机上传的时间戳均正确则认为此终端就是此物流订单的发起用户的终端，且无人机确实为指派无人机；如果时间戳 T1 正确时间戳 T2 错误（或缺失），则无人机正确但有终端伪装成发件方，且此终端已经获取到了解密时间戳 T1 的私钥；如果时间戳 T1 错误（或缺失），时间戳 T2 正确，则判别无人机为恶意骗取，且此无人机已经获取到了解密时间戳 T2 的私钥；如果时间戳 T1 和时间戳 T2 都错误或缺失，则基本可判定此无人
5 机为恶意骗取，也有小部分可能是无人机正确但有用户伪装成发件人，此时
10 应立刻发送消息至正确的用户终端，提醒订单用户无人机恶意骗取或有其他人伪装成发件人。

步骤 1110、无人机和终端接收到服务器发来的双方身份认证通过的消息后，按照步骤 1007 的描述完成取货流程。

在本发明的另一与图 11 整体流程相似的较佳实施方式中，终端和无人机
15 在收到对方发来的加密时间戳后，利用自身中的相应私钥解密接收的加密时间戳后，可以不将解密后的时间戳发给对方，而是直接将解密后的时间戳发送给服务器，直接由服务器进行认证，并分别下发认证结果给双方，具体的认证方式和结果下发方式与上一较佳实施方式中相同，这里不再赘述。

以上是针对本发明无人机取货方法实施例的描述。本发明实施例还提供了提升无人机送货安全性的方法。
20

图 12 示出了无人机送货方法的一种具体实施方式，该实施方式中，无人机采用语音问答的方式，以用户的答案和物流订单信息进行比对验证，以确定确实为收件人，具体地，该实施方式包括如下步骤：

步骤 1201、服务器指派无人机，无人机接收包括运输订单的指令后，完成货物加载后，根据指令飞往送货目标地点。
25

本实施例及下述各实施例中，运输订单中包括运输地点信息，即送货目

的地点信息。

步骤 1202、收货人出现后，无人机拍照或开始录像。

本步骤中，也可以是无人机到达送货目标地点后，即自动开始定时拍照或开始录像。

5 此外，本步骤中，无人机可以通过图像识别确定收货人出现，也可以通过收货人的对无人机的操作确定收货人出现。

步骤 1203、无人机采用语音的方式询问收货人姓名和/或地址信息。

步骤 1204、无人机检测收货人回答的信息是否正确，在检验正确后提供货物，然后执行步骤 1205。

10 本步骤中，无人机可以通过语音识别，获取收货人回答的内容，然后将回答的内容与物流订单的信息比对，如果相同则认为地点正确，自动开锁，收货人取走物品；如果比较相似则需要进一步智能验证（如通过手机号的方式，说出前几位让收货人说出后面几位等方式）直到验证通过后自动解锁，用户取走物品；如果完全不同或者验证无法通过则认为地点错误或者有人冒
15 领，无人机应返回消息待物流公司人工与收件人进行沟通后再去投递。

步骤 1205、无人机完成送货，离开时结束拍照或录像，飞往下一个投递点或返航。

图 13 示出了无人机送货方法的另一种具体实施方式，该实施方式中，无人机与收货人进行双向验证，该实施方式具体包括如下步骤：

20 步骤 1301、服务器根据用户物流订单，在需要给收货人送货时，指派进行送货的无人机，即生成运输订单下发给无人机，并记录无人机被指派时刻的时间戳 T2，并获取该用户物流订单生成时刻的时间戳 T1。

步骤 1302、服务器采用非对称加密方式，将时间戳 T2 用上述收货人用户
25 账户的公钥加密，并将时间戳 T1 用户无人机的公钥加密，然后将加密后的时间戳 T1 和 T2 分别发送给无人机和收货人用户账户登录的终端。

如上各实施例所描述，这里的 T1 和 T2 可以互换，也可以替换为其他的

时间戳。

步骤 1303、所指派的无人机加载货物并按照物流订单中的地点信息送货，并将自身的位置信息反馈给服务器，同时服务器在用户通过登录的终端发起无人机位置查询时，将无人机的位置、时间信息发送给用户当时登录的终端，
5 这里的用户可以是发货人也可以是收货人。

本实施方式中，无人机加载货物的时间可以在服务器下发加密时间戳的时间之后，也可以在其之前。

步骤 1304、无人机到达送货地点后，将自身中加密后的时间戳 T2 传送给收货人用户登录的终端，同时收货人用户登录的终端将自身中加密后的时间
10 戳 T1 传送给无人机，并分别根据接收到的加密时间戳进行身份认证。

具体地，本步骤中，在无人机到达送货地点后，还可以拍照或录像，并在传送加密后的时间戳之前，收货人用户通过登录的终端从无人机获取订单号信息，验证该到达的无人机是否是为该用户相应订单指派的无人机，或者也可以如上一实施方式中所描述，无人机对收货人是否正确进行验证，然后
15 再执行本步骤中的密钥交互操作。

终端和无人机在收到对方发来的加密时间戳后，利用自身的私钥解密接收的加密时间戳，并将其与解密后的来自服务器的相应时间戳进行比对，如果一致，则对方通过身份验证。

较佳地，本步骤中，终端和无人机的之间的通信可以通过各种无线通信
20 方式完成。在本实施方式中，较佳地，可以采用蓝牙、非接触式射频识别(NFC)方式，或者通过扫描识别编码（如二维码或条形码）等直接交互方式，其相对于通过无线网络进行通信可以进一步提升安全性。

步骤 1305、双方身份验证通过后，则无人机自动解锁，由收货人用户将物品取出，确认完成取货后，锁闭货仓，无人机送货完成；若双方身份验证
25 未通过，结束取货流程。

本步骤中，取货完成后无人机可以飞往物流集散点、下一个送货点，或

取货点。

本实施例中，若终端验证 T2 不通过，将不通过的信息反馈给服务器，并等待正确的无人机到达；若无人机验证 T1 不通过或未接收到来自终端的加密 T1 信息，则无人机将验证失败信息反馈给服务器，并根据服务器反馈的指令
5 飞回物流集散点、飞往下一个取货点，或者原地等待。

图 14 示出了无人机送货方法的再一种具体实施方式，该实施方式中，无人机对收货人进行单向验证，该实施方式具体包括如下步骤：

步骤 1401、服务器根据用户物流订单，在需要给收货人送货时，指派进行送货的无人机，即生成运输订单下发给无人机，并记录无人机被指派时刻
10 的时间戳 T2。

步骤 1402、服务器采用非对称加密方式，将时间戳 T2 用上述收货人用户账户的公钥加密，然后加密后的时间戳 T2 发送给所指派的无人机。

本步骤中，服务器还可以将时间戳 T2 用无人机自身的公钥加密后发给所指派的无人机。

步骤 1403、所指派的无人机加载货物，按照物流订单中的地点信息送货，并将自身的位置信息反馈给服务器，同时服务器在用户通过登录的终端发起无人机位置查询时，将无人机的位置、时间信息发送给用户当时登录的终端，这里的用户可以是发货人也可以是收货人。
15

本实施方式中，无人机加载货物的时间可以在服务器下发加密时间戳的时间之后，也可以在其之前。
20

步骤 1404、无人机到达送货地点后，将自身中用户账户公钥加密后的时间戳 T2 传送给收货人用户登录的终端。

具体地，本步骤中，在无人机到达取货地点后，无人机开始拍照或录像，用户通过终端从无人机获取订单号信息，验证该到达的无人机是否是为该用户相应订单指派的无人机，此后再执行传送加密时间戳的步骤。
25

步骤 1405、无人机接收终端反馈的解密后的 T2 信息，根据解密后的 T2

信息对终端进行认证。

本步骤中，如果在步骤 1402 中，服务器向无人机下发了用无人机公钥加密的 T2，则无人机对该加密信息解密后，将解密后的 T2 与来自终端的 T2 进行对比，如果一致，则对终端验证身份通过，如果不一致，则验证不通过。

5 如果在步骤 1402 中，服务器没有向无人机下发用无人机公钥加密的 T2，则无人机在接收到终端反馈的解密后的 T2 信息后，将该 T2 信息和运输订单相关信息，如订单号，发送给服务器，由服务器对解密后的 T2 是否正确进行验证，并将验证结果反馈给无人机，无人机根据验证结果确定是否对终端验证身份通过。

10 并将解密后的 T2 信息与自身中的 T2，或用自身私钥解密后得到的 T2 进行对比，确定终端反馈的 T2 是否正确，以对终端进行身份认证。

步骤 1406、无人机对终端身份验证通过后，无人机自动解锁，由收货人用户将物品取出，确认完成取货后，锁闭货仓，无人机送货完成；若身份验证未通过，结束取货流程。

15 本步骤中，取货完成后无人机可以飞往物流集散点、下一个送货点，或取货点。

在图 14 所示实施例的替代方式中，无人机对收货人进行单向验证过程，也可以是：服务器将用无人机公钥加密的 T2 同时发送给无人机和用户登录的终端，无人机在到达送货地点后，从用户登录的终端获取无人机公钥加密的 T2 后，将该 T2 和此前服务器发给自身的加密 T2 同时利用自身私钥解密，解密后对比，若一致则对终端认证通过，不一致认证通过。

20 本发明无人机的一个示例性实施方式的结构如图 15 所示。本实施方式中，当无人机用于取货时，通过无人机与用户登录的终端相互认证，提高无人机取货的安全性。

25 本实施例中，无人机包括：通信单元 151、处理单元 152 和存储单元 153，其中通信单元 151 和存储单元 153 均通过总线与处理单元 152 通讯。当然，

随着技术进步，若出现其他的计算机内部通信方式，通信单元 151 和存储单元 153 等也可以通过其他的计算机内部通信方式与处理单元 152 通讯。

所述通信单元 151 用于接收来自服务器的运输任务及运输地点、订单信息和用于安全认证的第一加密信息，将其发送给处理单元 152；和，根据处理
5 单元 152 的指令，将第一加密信息发送给所述订单信息对应的终端，并接收来自所述终端的第二加密信息，将其发送给处理单元 152；以及，接收终端验证无人机通过的通知，并将其发送给处理单元 152；

所述处理单元 152 用于接收所述运输任务及运输地点、订单信息、第一加密信息，并存储至存储单元 153；并在确认无人机到达运输地点后，读取存
10 储单元 153 中的第一加密信息，指示通信单元 151 发送给所述终端；以及根据接收的所述第二加密信息确定终端合法，并接收到终端验证无人机通过的通知后，控制所述无人机执行所述运输任务；

所述存储单元 153 用于根据处理单元 152 的指令存储或提供信息。

上述第二加密信息也可以先存储于存储单元 153 中，在处理单元 152 使
15 用时，再从存储单元 153 读取。

所述第二加密信息为用所述无人机的公钥加密的信息；

所述通信单元 151 用于根据所述第二加密信息确定所述终端合法包括：

所述处理单元 152 用于从存储单元 153 中读取所述无人机的私钥，对所述
20 第二加密信息解密后，确定所述解密后的信息与存储单元 153 中存储的对应信息匹配。

所述通信单元 151 进一步可以用于从接收来自所述服务器的第二加密信息；

所述通信单元 151 进一步用于将所述来自服务器的第二加密信息存储至
存储单元 153；

25 所述通信单元 151 用于根据所述第二加密信息确定所述终端合法包括：

所述处理单元 152 用于从存储单元 153 中读取所述无人机的私钥和来自

服务器的第二加密信息，对来自所述终端的第二加密信息和来自所述服务器的第二加密信息分别解密后，确定解密后的信息相匹配。

较佳地，所述加密信息为加密的时间戳。其中，所述第一加密信息中的时间戳根据服务器向无人机下发运输任务的时刻生成，所述第二加密信息中的时间戳根据服务器生成所述订单的时刻生成；或者，所述第一加密信息中的时间戳根据服务器生成所述订单的时刻生成，所述第二加密信息中的时间戳根据服务器向无人机下发运输任务的时刻生成。

较佳地，所述第一加密信息为用所述终端用户账户的公钥加密的信息；则所述通信单元 151 用于接收终端验证无人机通过的通知可以包括：

所述通信单元 151 用于接收所述终端对所述第一加密信息利用终端中所述用户账户私钥解密并验证成功后，发送的验证通过消息。

较佳地，如图 16 所示，本实施方式中，通信单元 151 包括第一通信单元 1511 和第二通信单元 1512。其中，第一通信单元 1511 用于无人机的处理单元 152 通过无线通信网络与服务器或其他设备进行无线通信。较佳地，该第一通信单元 1511 具体可以是 5G、4G、3G、GPRS 或 WiFi 通信单元，或者是集成了以上任意两种或两种以上通信功能。

第二通信单元 1512 用于无人机的处理单元 152 通过其与用户的终端进行无线通信。较佳地，该第二通信单元 1512 可以是蓝牙通信单元、射频识别单元等可以直接与终端进行无线通信，无需通过通信网络的通信单元。

在本发明的另一个无人机的较佳实施方式中，当无人机用于取货时，通过无人机与用户登录的终端通过服务器进行对方身份认证，提高无人机取货的安全性。

本实施方式中，与上一实施方式的区别之处主要在于，处理单元对终端的合法验证部分和无人机如何接收终端对其验证通过的信息，其余部分与上一无人机实施方式相同，相同的部分这里不再追溯。

本实施方式中，处理单元可以基于第二加密信息确定终端合法，也可以

通过第一加密信息确定终端合法。

处理单元用于根据第二加密信息确定所述终端合法的方式包括：所述处理单元用于从存储单元中读取所述无人机的私钥，对所述第二加密信息解密后，指示通信单元将所述解密后的信息发送给服务器，并通过通信单元接收
5 到所述服务器反馈的认证成功消息。

所述处理单元用于根据所述第一加密信息确定所述终端合法包括：所述处理单元用于通过通信单元接收所述终端反馈的解密后的第一加密信息，并将解密后的信息通过通信单元发送给服务器，在通过通信单元接收到服务器反馈确认所述解密后的信息验证成功后，确定所述终端合法。

10 图 17 示出了本发明无人机的再一种实施方式的结构示意图，所述无人机包括：存储器 171，收发器 173 和一个或多个处理器 172；以及一个或多个软件模块，所述一个或多个软件模块被存储在所述存储器 171 中，并被配置成由所述一个或多个处理器执行，所述一个或多个软件模块包括用于执行上述无人机取货和/或送货实施方式中无人机所执行的各个步骤的指令。

15 本领域技术人员公知的，图 15 所示的实施方式和图 17 所示的实施方式可以是相同的，这里仅是从不同的技术角度进行描述。

本发明实施例还提供了一种与无人机结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述无人机取货和/或送货实施方式中
20 无人机所执行的各个步骤的指令。

图 18 示出了本发明终端实施方式的结构示意图，该终端包括：显示器 181，存储器 182，收发器 183，一个或多个处理器 184；以及一个或多个软件模块，所述一个或多个软件模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个软件模块包括用于执行上述无人机取货和/或
25 或送货实施方式中终端所执行的各个步骤的指令。本实施方式中，一个或多个软件模块可以是客户端应用软件。

图 19 示出了本发明服务器实施方式的结构示意图，该服务器包括：该服务器包括：存储器 191，收发器 192，一个或多个处理器 193；以及一个或多个模块，所述一个或多个模块被存储在所述存储器 191 中，并被配置成由所述一个或多个处理器 193 执行，所述一个或多个模块包括用于执行上述无人

5 机取货和/或送货实施方式中服务器所执行的各个步骤的指令。

本发明实施例还提供了一种与电子设备结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述无人机取货和/或送货实施方式中终端所执行的各个步骤的指令。该计算机程序产品可以是客户端应用软件。

10 本发明实施例还提供了一种与服务器结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行上述无人机取货和/或送货实施方式中服务器所执行的各个步骤的指令。

本发明通过上述各实施方式，在无人机与终端双方均对对方身份认证通

15 过后，无人机才继续执行运输任务，或者用户可以通过终端上呈现的双方验证通过的信息确定是否发货或取货，提升了无人机运输的安全性。本发明很大程度上避免了无人机取货时的错误提取、被其他无人机骗取、取货地点错误等，也避免了无人机送货时的冒领或地点错误等问题，取货/送货安全性得到了很大的提升，为未来无人机自动化物流体系的建立有很大帮助。

20 本领域内的技术人员应明白，本发明的实施例可提供为方法、系统、或计算机程序产品。因此，本发明可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且，本发明可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质（包括但不限于磁盘存储器、CD-ROM、光学存储器等）上实施的计算机程序产品的形式。

25 本发明是参照根据本发明实施例的方法、设备（系统）、和计算机程序产品的流程图和 / 或方框图来描述的。应理解可由计算机程序指令实现流程图

和 / 或方框图中的每一流程和 / 或方框、以及流程图和 / 或方框图中的流程和 / 或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的装置。

这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能。

这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和 / 或方框图一个方框或多个方框中指定的功能的步骤。

尽管已描述了本发明的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本发明范围的所有变更和修改。

权利要求书

1、一种提升无人机运输安全的方法，其特征在于，所述方法包括：

无人机获取运输订单信息和用于安全认证的第一加密信息，所述运输订单信息中包括运输地点信息；

5 无人机根据所述运输地点信息到达运输地点后，将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并接收所述终端发来的反馈信息，根据所述反馈信息确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启；或，

10 无人机根据所述运输地点信息到达运输地点后，接收所述运输订单信息对应用户账户登录的终端发来的第二加密信息，无人机对所述第一加密信息和第二加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启；或，

15 所述无人机进一步接收用于安全认证的第三加密信息，无人机根据所述运输地点信息到达运输地点后，将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并接收所述终端发来的针对所述第一加密信息的反馈信息，以及，接收所述终端发来的第二加密信息，无人机对所述第三加密信息和第二加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，在确定成功后，控制所述运输订单信息对应的货仓开启。

20 2、根据权利要求1所述的方法，其特征在于，所述针对所述第一加密信息的反馈信息包括：对所述第一加密信息验证是否通过的信息；

或者，针对所述第一加密信息的反馈信息包括：所述第一加密信息解密后的信息；则接收所述反馈信息后进一步包括：将所述第一加密信息解密后的信息发送给服务器，并接收服务器反馈的针对所述加密后的信息验证是否
25 通过的信息；则所述根据反馈信息确定安全认证是否成功包括：根据所述服

务器反馈的验证是否通过的信息确定安全认证是否成功。

3、根据权利要求1所述的方法，其特征在于，所述发送给终端的第一加密信息包括：用所述运输订单对应用户账户的公钥加密的信息；

所述第二加密信息包括：用所述无人机的公钥加密的信息；

5 所述无人机解密的第一加密信息或第三加密信息包括：用所述无人机的公钥加密的信息。

4、根据权利要求1至3中任一所述的方法，其特征在于，所述运输订单为取货订单，或送货订单；

所述第一加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第二加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第三加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

15 5、一种提升无人机运输安全的方法，其特征在于，所述方法包括：

终端根据用户的账户信息从服务器获取运输订单信息和用于安全认证的第四加密信息；

所述终端在与所述运输订单信息对应的无人机进行通讯时，将所述第四加密信息发送给所述无人机，并接收所述无人机发来的反馈信息，根据所述反馈信息确定安全认证是否成功，并显示安全认证是否成功的信息；或，

所述终端在与所述运输订单信息对应的无人机进行通讯时，接收所述无人机发来的第五加密信息，所述终端对所述第四加密信息和第五加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，并显示安全认证是否成功的信息；或，

25 所述终端进一步从服务器获取用于安全认证的第六加密信息，所述终端在与所述运输订单信息对应的无人机进行通讯时，将所述第四加密信息发送

给所述无人机，并接收所述无人机发来的反馈信息，以及，接收所述无人机发来的第五加密信息，所述终端对所述第五加密信息和第六加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，并显示安全认证是否成功的信息。

5 6、根据权利要求5所述的方法，其特征在于，所述针对所述第四加密信息的反馈信息包括：对所述第四加密信息验证是否通过的信息；

 或者，针对所述第四加密信息的反馈信息包括：所述第四加密信息解密后的信息；则接收所述反馈信息后进一步包括：将所述第四加密信息解密后的信息发送给服务器，并接收服务器反馈的针对所述加密后的信息验证是否
10 通过的信息；则所述根据反馈信息确定安全认证是否成功包括：根据所述服务器反馈的验证是否通过的信息确定安全认证是否成功。

 7、根据权利要求5所述的方法，其特征在于，所述发送给无人机的第四加密信息包括：用所述无人机的公钥加密的信息；

 所述第五加密信息包括：用所述用户账户的公钥加密的信息；

15 所述终端解密的第四加密信息和第六加密信息包括：用所述用户账户的公钥加密的信息。

 8、根据权利要求5至7中任一所述的方法，其特征在于，所述运输订单为取货订单，或送货订单；

 所述第四加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；
20 戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

 所述第五加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

 所述第六加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

25 9、一种无人机，其特征在于，所述无人机包括：通信单元、处理单元和存储单元，其中通信单元和存储单元均通过总线与处理单元通讯；

所述通信单元用于处理单元通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元用于根据处理单元的指令存储信息；

所述处理单元用于通过所述通信单元接收运输订单信息和用于安全认证的第一加密信息，所述运输订单信息中包括运输地点信息，并存储至存储单元；以及，

在确认所述无人机到达运输地点后，读取存储单元中的第一加密信息，通过通信单元发送给所述运输订单信息对应用户账户登录的终端，并通过所述通信单元接收所述终端发来的反馈信息，根据所述反馈信息确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令；

或者，在确认所述无人机到达运输地点后，通过通信单元接收所述运输订单信息对应用户账户登录的终端发来的第二加密信息，读取所述存储的第一加密信息，并将所述第一加密信息和第二加密信息分别解密和进行对比，根据对比结果确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令；或，

或者，所述通信单元进一步用于通过通信单元接收用于安全认证的第三加密信息，在确认所述无人机到达运输地点后，从存储单元中读取所述第一加密信息，通过通信单元将所述第一加密信息发送给所述运输订单信息对应用户账户登录的终端，并通过通信单元接收所述终端发来的针对所述第一加密信息的反馈信息，以及，通过通信单元接收所述终端发来的第二加密信息，将所述第三加密信息和第二加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，在确定成功后，发出控制所述运输订单信息对应的货仓开启的指令。

10、根据权利要求 9 所述的无人机，其特征在于，所述针对所述第一加密信息的反馈信息包括：对所述第一加密信息验证是否通过的信息；

或者，针对所述第一加密信息的反馈信息包括：所述第一加密信息解密后的信息；则所述处理单元通过所述通信单元进一步用于：通过通信单元将所述第一加密信息解密后的信息发送给服务器，并通过通信单元接收服务器反馈的针对所述加密后的信息验证是否通过的信息；则所述通信单元用于根据反馈信息确定安全认证是否成功包括：所述通信单元用于根据所述服务器反馈的验证是否通过的信息确定安全认证是否成功。

11、根据权利要求 9 所述的无人机，其特征在于，所述发送给终端的第一加密信息包括：用所述运输订单对应用户账户的公钥加密的信息；

所述第二加密信息包括：用所述无人机的公钥加密的信息；

所述处理单元解密的第一加密信息或第三加密信息包括：用所述无人机的公钥加密的信息。

12、根据权利要求 9 至 11 中任一所述的无人机，其特征在于，所述运输订单为取货订单，或送货订单；

所述第一加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第二加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第三加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

13、一种终端，其特征在于，所述终端包括：通信单元、处理单元、存储单元和显示单元，其中通信单元、存储单元和显示单元均通过总线与处理单元通讯；

所述通信单元用于处理单元通过其接收来自外部设备的信息，或向外部设备发送信息；

所述存储单元用于根据处理单元的指令存储信息；

所述显示单元用于根据处理单元的指令显示信息；

所述处理单元用于通过通信单元从服务器获取运输订单信息和用于安全认证的第四加密信息，并存储至存储单元；以及，

在通过通信单元与所述运输订单信息对应的无人机进行通讯时，读取存储单元中的所述第四加密信息，通过通信单元将所述第四加密信息发送给所述无人机，并通过通信单元接收所述无人机发来的反馈信息，根据所述反馈信息确定安全认证是否成功，指示显示单元显示安全认证是否成功的信息；或，

在通过通信单元与所述运输订单信息对应的无人机进行通讯时，通过通信单元接收所述无人机发来的第五加密信息，读取存储单元中存储的第四加密信息，将所述第四加密信息和第五加密信息分别解密并进行对比，根据对比结果确定安全认证是否成功，并指示显示单元显示安全认证是否成功的信息；或，

所述处理单元进一步用于通过通信单元从服务器获取用于安全认证的第六加密信息，以及在通过通信单元与所述运输订单信息对应的无人机进行通讯时，读取存储单元中存储的第四加密信息，通过通信单元将所述第四加密信息发送给所述无人机，并通过通信单元接收所述无人机发来的反馈信息，以及，通过通信单元接收所述无人机发来的第五加密信息，对所述第五加密信息和第六加密信息分别解密并进行对比，根据对比结果和所述反馈信息确定安全认证是否成功，并指示显示单元显示安全认证是否成功的信息。

14、根据权利要求 13 所述的终端，其特征在于，所述针对所述第四加密信息的反馈信息包括：对所述第四加密信息验证是否通过的信息；

或者，针对所述第四加密信息的反馈信息包括：所述第四加密信息解密后的信息；则所述通信单元进一步用于：将所述第四加密信息解密后的信息通过所述通信单元发送给服务器，并通过通信单元接收服务器反馈的针对所述加密后的信息验证是否通过的信息；则所述通信单元用于根据反馈信息确定安全认证是否成功包括：所述通信单元用于根据所述服务器反馈的验证是

否通过的信息确定安全认证是否成功。

15、根据权利要求 13 所述的终端，其特征在于，所述发送给无人机的第四加密信息包括：用所述无人机的公钥加密的信息；

所述第五加密信息包括：用所述用户账户的公钥加密的信息；

5 所述终端解密的第四加密信息或第六加密信息包括：用所述用户账户的公钥加密的信息。

16、根据权利要求 13 至 15 中任一所述的方法，其特征在于，所述运输订单为取货订单，或送货订单；

所述第四加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第五加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第六加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

15 17、一种无人机，其特征在于，所述无人机包括：存储器，和一个或多个处理器；以及一个或多个模块，所述一个或多个模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行权利要求 1-4 中任一所述方法中各个步骤的指令。

18、一种与无人机结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行权利要求 1-4 中任一所述方法中各个步骤的指令。

19、一种终端，其特征在于，所述终端包括：显示器，存储器，收发器，一个或多个处理器；以及一个或多个模块，所述一个或多个模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行权利要求 5-8 中任一所述方法中各个步骤的指令。

20、一种与电子设备结合使用的计算机程序产品，所述计算机程序产品

包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行权利要求 5-8 中任一所述方法中各个步骤的指令。

21、一种提升无人机运输安全的方法，其特征在于，该方法包括：

为无人机生成运输订单信息，所述运输订单信息中包括运输地点信息；

5 生成用于安全认证的第一加密信息，或生成用于安全加密的第二加密信息和第三加密信息；

将所述生成的运输订单发送给所述无人机，并将所述生成的加密信息发送给所述无人机，或发送给所述运输订单对应的用户账户登录的终端。

22、根据权利要求 21 所述的方法，其特征在于，所述发送加密信息的步骤后，进一步包括：

接收所述无人机或所述终端发送的解密信息，并对解密信息进行安全认证，然后向所述无人机或所述终端反馈安全认证结果。

23、根据权利要求 21 所述的方法，其特征在于，所述发送给无人机的第一加密信息为：用所述用户账户的公钥加密的信息；

15 所述发送给用户账户登录的终端的第一加密信息包括：用所述无人机的公钥加密的信息；

所述第二加密信息和第三加密信息分别包括用所述无人机的公钥加密的信息和用所述用户账户的公钥加密的信息。

24、根据权利要求 21 至 23 中任一所述的方法，其特征在于，所述运输
20 订单为取货订单，或送货订单；

所述第一加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或所述服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第二加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

25 所述第三加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

25、一种服务器，其特征在于，所述服务器包括：通信单元、处理单元和存储单元，其中通信单元和存储单元均通过总线与处理单元通讯；

所述通信单元用于处理单元通过其接收来自外部设备的信息，或向外部设备发送信息；

5 所述存储单元用于根据处理单元的指令存储信息；

所述处理单元用于为无人机生成包括运输地点信息的运输订单，并生成用于安全认证的第一加密信息，或生成用于安全认证的第二和第三加密信息，并通过通信单元将所述生成的运输订单发送给所述无人机，以及通过通信单元将所述生成的加密信息发送给无人机或所述运输订单对应的用户账户登录的终端。

10

26、根据权利要求 25 所述的服务器，其特征在于，所述处理单元进一步用于通过通信单元接收所述无人机或所述终端发送的解密信息，并对解密信息进行安全认证，然后通过所述通信单元向所述无人机或所述终端反馈安全认证结果。

15 27、根据权利要求 25 所述的服务器，其特征在于，所述发送给无人机的第一加密信息为：用所述用户账户的公钥加密的信息；

所述发送给用户账户登录的终端的第一加密信息包括：用所述无人机的公钥加密的信息；

所述第二加密信息和第三加密信息分别包括用所述无人机的公钥加密的信息和用所述用户账户的公钥加密的信息。

20

28、根据权利要求 25 至 27 中任一所述的服务器，其特征在于，所述运输订单为取货订单，或送货订单；

所述第一加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或所述服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

25 所述第二加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳；

所述第三加密信息中被加密的信息包括：所述运输订单生成时刻的时间戳，或服务器确认所述运输订单对应的用户物流订单时刻的时间戳。

29、一种服务器，其特征在于，所述服务器包括：存储器，收发器，一个或多个处理器；以及一个或多个模块，所述一个或多个模块被存储在所述存储器中，并被配置成由所述一个或多个处理器执行，所述一个或多个模块包括用于执行权利要求 21-24 中任一所述方法中各个步骤的指令。

30、一种与服务器结合使用的计算机程序产品，所述计算机程序产品包括计算机可读的存储介质和内嵌于其中的计算机程序机制，所述计算机程序机制包括用于执行权利要求 21-24 中任一所述方法中各个步骤的指令。

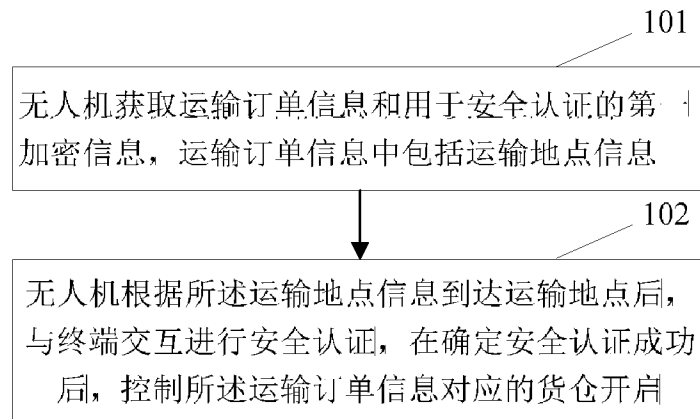


图 1

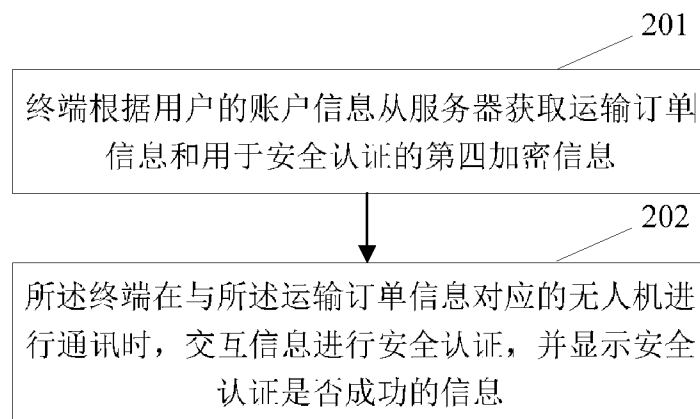


图 2

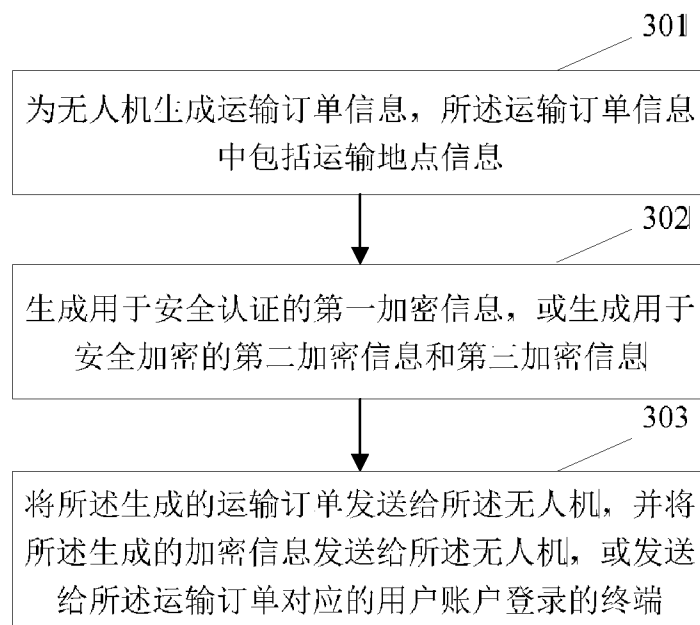


图 3

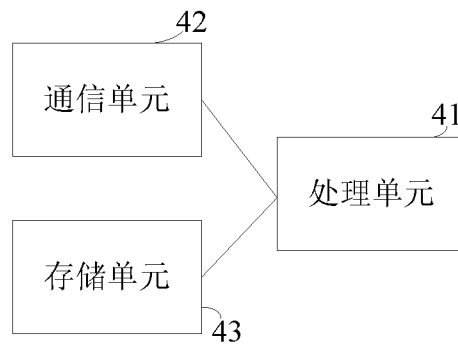


图 4

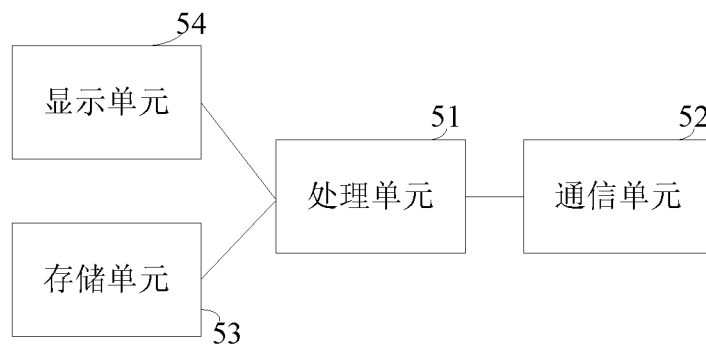


图 5

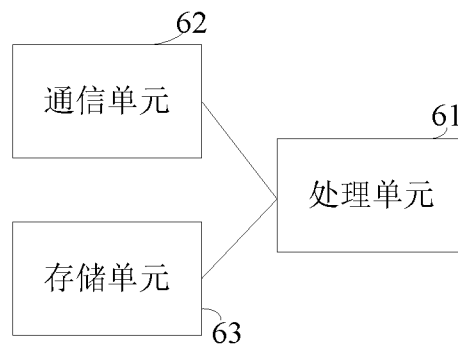


图 6

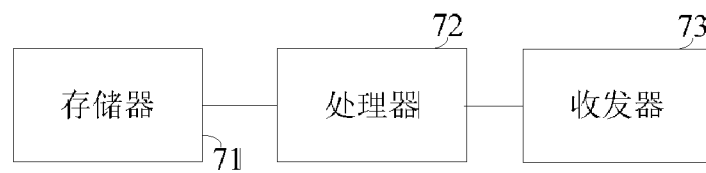


图 7

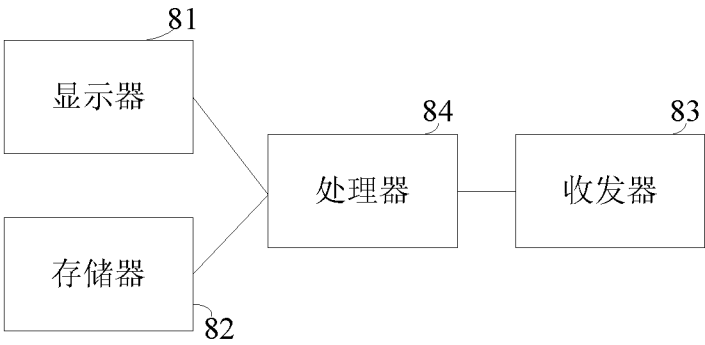


图 8

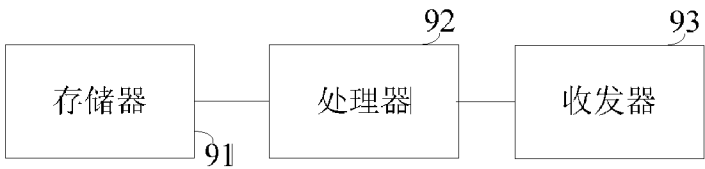


图 9

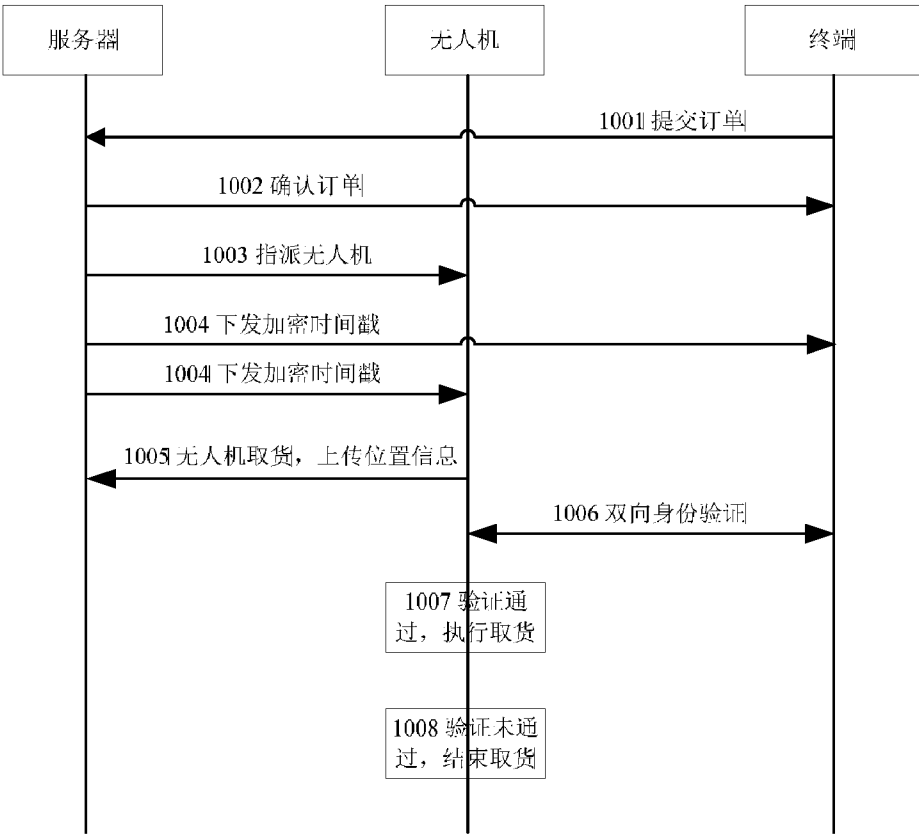


图 10

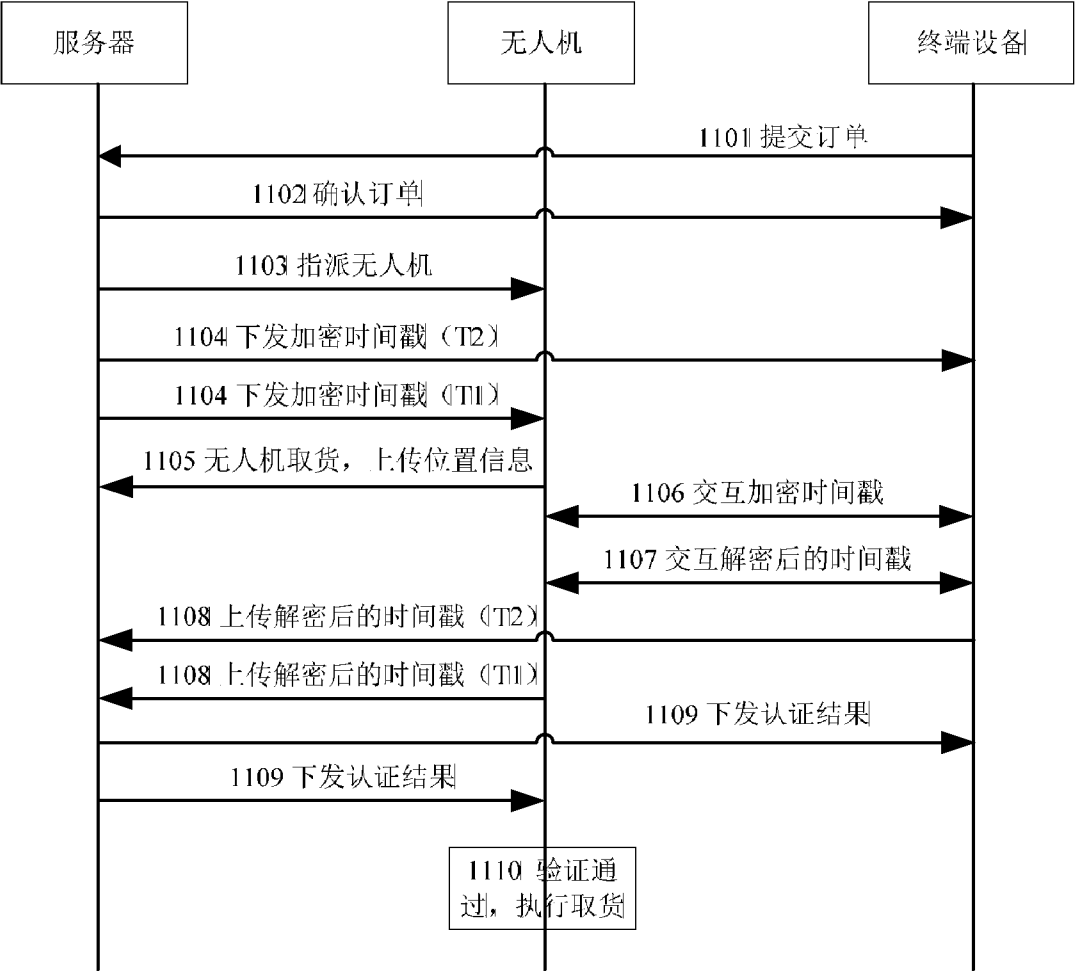
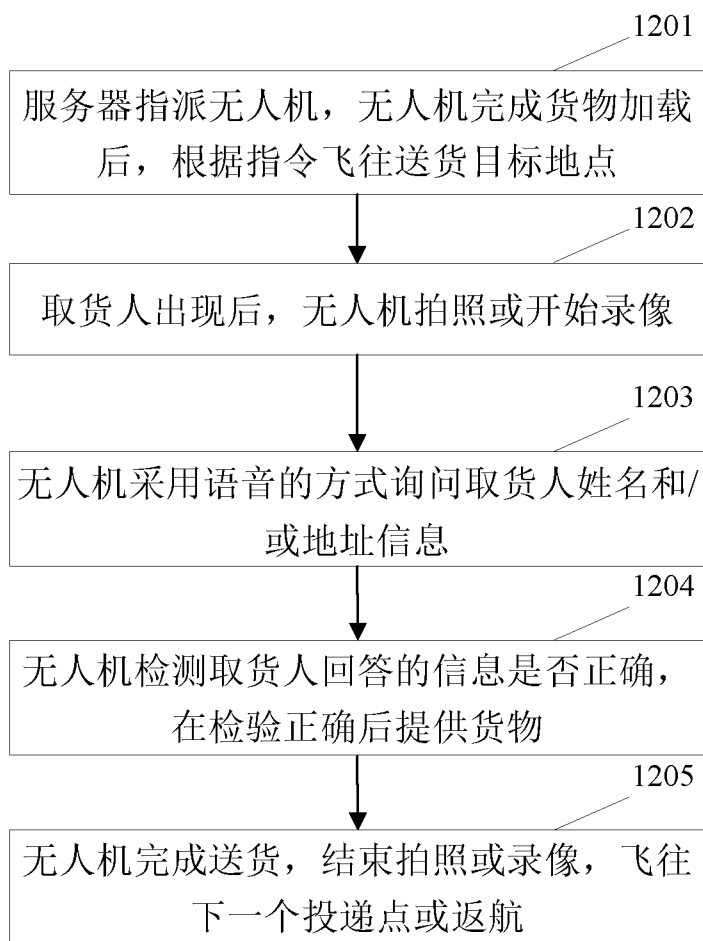
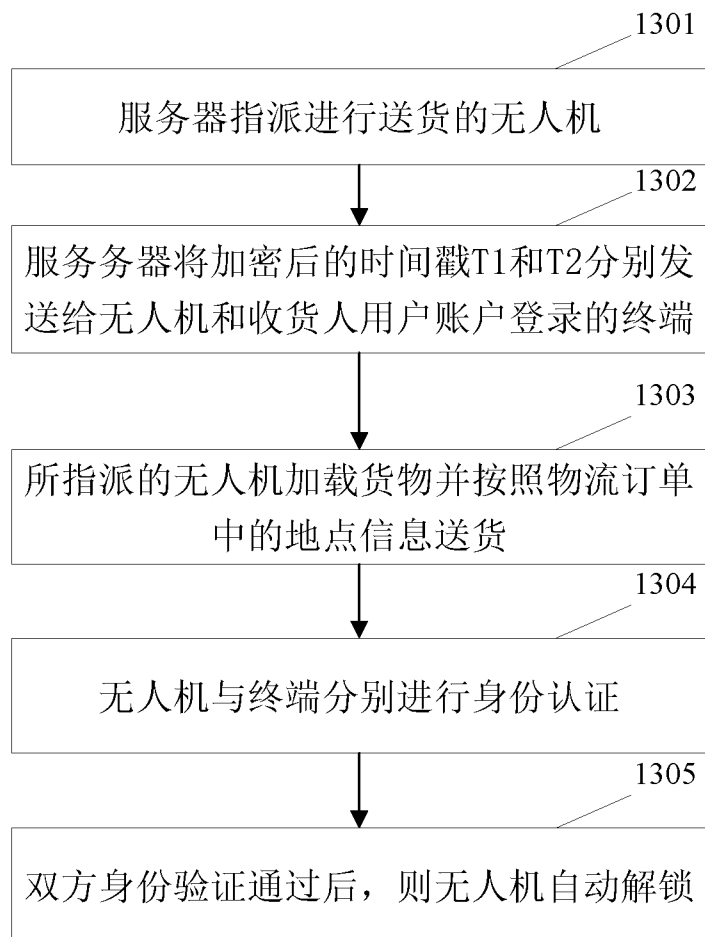


图 11

**图 12**

**图 13**

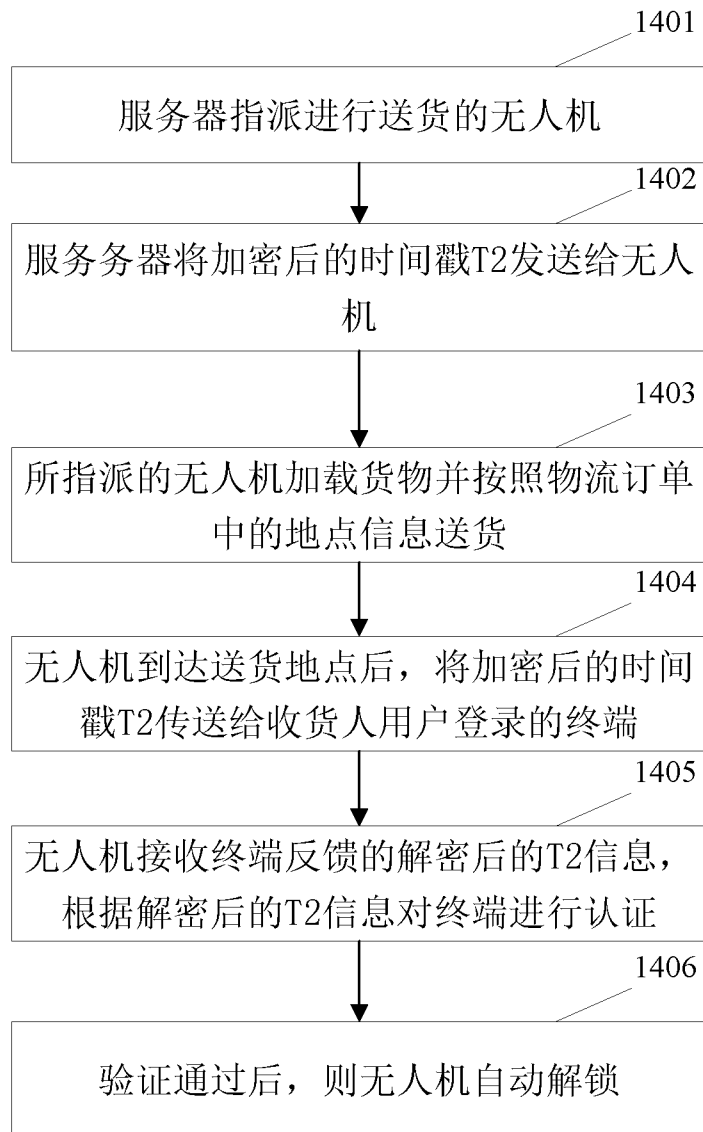


图 14

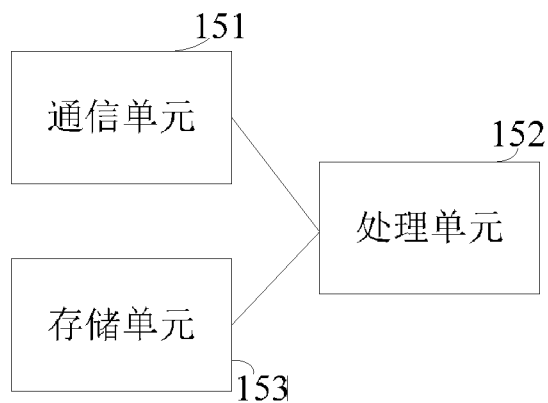


图 15

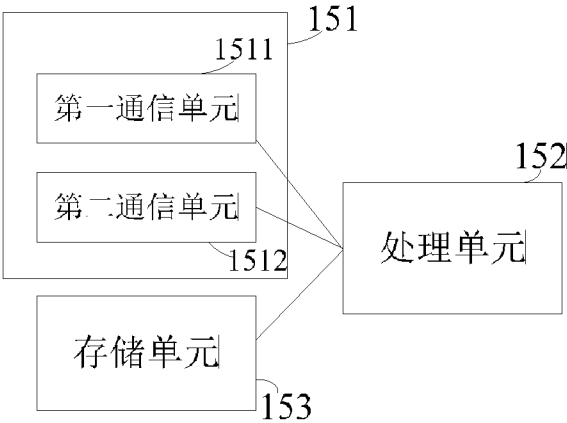


图 16

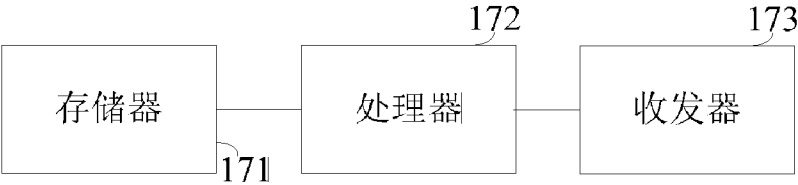


图 17

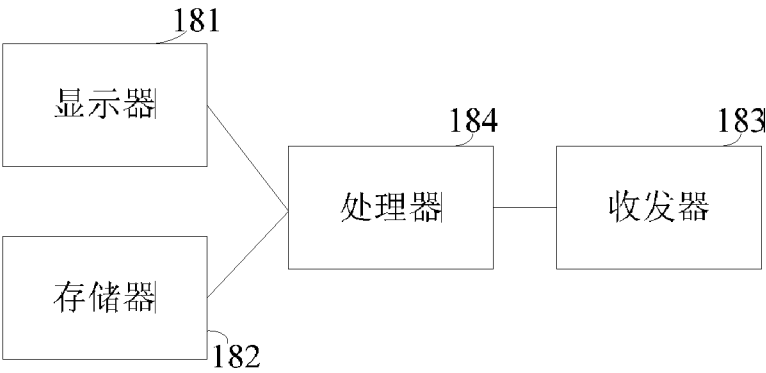


图 18

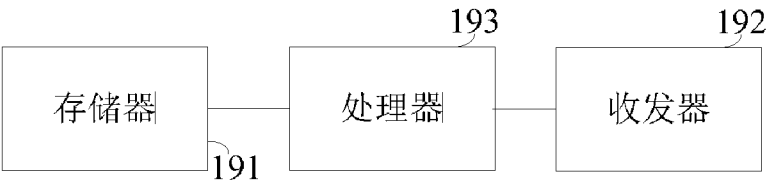


图 19

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/106749

A. CLASSIFICATION OF SUBJECT MATTER

B64C 39/02 (2006.01) i; G05D 1/00 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

B64C; G05D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNKI, CNABS, SIPOABS, DWPI: 无人机, 运输, 加密, 密码, 快递, 邮政, 邮寄, 运送, 订单, unmanned, vehicle, transport, code, password, post, delivery, mail, express+, order

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016068265 A1 (IBM), 10 March 2016 (10.03.2016), description, paragraphs [0017]-[0060], and figures 1-6	1-30
X	WO 2016140988 A1 (AMAZON TECH INC.), 09 September 2016 (09.09.2016), description, paragraphs [0026]-[0052], and figures 1-5	1-30
A	CN 204776032 U (ZHU, Wei), 18 November 2015 (18.11.2015), entire document	1-30
A	WO 2016134193 A1 (AMAZON TECH INC.), 25 August 2016 (25.08.2016), entire document	1-30
A	TW 201545111 A (LI, Xiaozhong), 01 December 2015 (01.12.2015), entire document	1-30
A	US 2016257423 A1 (MARTIN, J.), 08 September 2016 (08.09.2016), entire document	1-30

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:	“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
“A” document defining the general state of the art which is not considered to be of particular relevance	“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
“E” earlier application or patent but published on or after the international filing date	“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	“&” document member of the same patent family
“O” document referring to an oral disclosure, use, exhibition or other means	
“P” document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 02 August 2017	Date of mailing of the international search report 23 August 2017
Name and mailing address of the ISA State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No. (86-10) 62019451	Authorized officer GAO, Xianwen Telephone No. (86-10) 62085281

International application No.
PCT/CN2016/106749

Form PCT/ISA/210 (patent family annex) (July 2009)

国际检索报告

国际申请号

PCT/CN2016/106749

A. 主题的分类 B64C 39/02 (2006.01)i; G05D 1/00 (2006.01)i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类		
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) B64C; G05D 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNKI, CNABS, SIPOABS, DWPI: 无人机, 运输, 加密, 密码, 快递, 邮政, 邮寄, 运送, 订单, unmanned, vehicle, transport, code, password, post, delivery, mail, express+, order		
C. 相关文件		
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
X	US 2016068265 A1 (IBM) 2016年 3月 10日 (2016 - 03 - 10) 说明书第[0017]-[0060]段、附图1-6	1-30
X	WO 2016140988 A1 (AMAZON TECH INC) 2016年 9月 9日 (2016 - 09 - 09) 说明书第[0026]-[0052]段、附图1-5	1-30
A	CN 204776032 U (朱威) 2015年 11月 18日 (2015 - 11 - 18) 全文	1-30
A	WO 2016134193 A1 (AMAZON TECH INC) 2016年 8月 25日 (2016 - 08 - 25) 全文	1-30
A	TW 201545111 A (李孝中) 2015年 12月 1日 (2015 - 12 - 01) 全文	1-30
A	US 2016257423 A1 (MARTIN JOSEPH) 2016年 9月 8日 (2016 - 09 - 08) 全文	1-30
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。		
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件		
国际检索实际完成的日期		国际检索报告邮寄日期
2017年 8月 2日		2017年 8月 23日
ISA/CN的名称和邮寄地址		受权官员
中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451		高现文 电话号码 (86-10)62085281

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2016/106749

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
US	2016068265	A1	2016年 3月 10日	无	
WO	2016140988	A1	2016年 9月 9日	US 2016257401	A1 2016年 9月 8日
CN	204776032	U	2015年 11月 18日	无	
WO	2016134193	A1	2016年 8月 25日	US 2016378108	A1 2016年 12月 29日
TW	201545111	A	2015年 12月 1日	无	
US	2016257423	A1	2016年 9月 8日	无	