

(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
2020 年 6 月 4 日 (04.06.2020)



(10) 国际公布号
WO 2020/107486 A1

(51) 国际专利分类号:
H04L 29/02 (2006.01)

深圳市南山区高新区南区粤兴一道9号香港科大深圳产学研大楼6楼, Guangdong 518057 (CN)。

(21) 国际申请号: PCT/CN2018/118784

(22) 国际申请日: 2018 年 11 月 30 日 (30.11.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(71) 申请人: 深圳市大疆创新科技有限公司 (SZ DJI TECHNOLOGY CO., LTD.) [CN/CN]; 中国广东省深圳市南山区高新区南区粤兴一道9号香港科大深圳产学研大楼6楼, Guangdong 518057 (CN)。

(72) 发明人: 郑德恩 (ZHENG, Deen); 中国广东省深圳市南山区高新区南区粤兴一道9号香港科大深圳产学研大楼6楼, Guangdong 518057 (CN)。 马超 (MA, Chao); 中国广东省深圳市南山区高新区南区粤兴一道9号香港科大深圳产学研大楼6楼, Guangdong 518057 (CN)。 周贤 (ZHOU, Xian); 中国广东省深圳市南山区高新区南区粤兴一道9号香港科大深圳产学研大楼6楼, Guangdong 518057 (CN)。 耿超 (GENG, Chao); 中国广东省

(74) 代理人: 广州三环专利商标代理有限公司 (SCIHEAD IP LAW FIRM); 中国广东省广州市越秀区先烈中路80号汇华商贸大厦1508室, Guangdong 510070 (CN)。

(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, JO, JP, KE, KG, KH, 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,

(54) Title: DATA TRANSMISSION METHOD AND DEVICE, TERMINAL, SERVER AND STORAGE MEDIUM

(54) 发明名称: 一种数据传输方法、设备、终端、服务器及存储介质

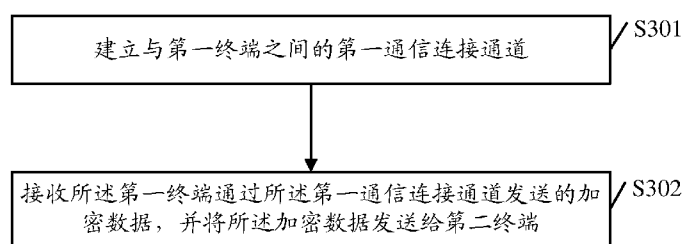


图 3

S301 Establish a first communication connection channel with a first terminal
S302 Receive encrypted data sent by the first terminal through the first communication connection channel, and send the encrypted data to a second terminal

(57) Abstract: Provided are a data transmission method and device based on a public communication network, and a terminal, a server and a storage medium. The method comprises: establishing a first communication connection channel with a first terminal; and receiving encrypted data sent by the first terminal through the first communication connection channel, and sending the encrypted data to a second terminal, wherein when the first terminal is a control device and the second terminal is a mobile platform, the encrypted data comprises data regarding control over the mobile platform by the control device; or, when the first terminal is the mobile platform and the second terminal is the control device, the encrypted data comprises working data collected by the mobile platform. In this way, the encrypted control of data transmission in the public wireless communication network is realized, such that the security of the data transmission in the public wireless communication network is improved, and long-distance communication between the first terminal and the second terminal is facilitated.

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))。

(57) 摘要：本发明实施例提供了一种基于公共通信网络的数据传输方法、设备、终端、服务器及存储介质，其中，该方法包括：建立与第一终端之间的第一通信连接通道；接收所述第一终端通过所述第一通信连接通道发送的加密数据，并将所述加密数据发送给第二终端；其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。通过这种方式，实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，有利于第一终端和第二终端之间的远距离通信。

一种数据传输方法、设备、终端、服务器及存储介质

技术领域

本发明涉及控制技术领域，尤其涉及一种基于公共通信网络的数据传输方法、设备、终端、服务器及存储介质。

背景技术

随着移动通信网络的发展，移动通信网络中数据传输的安全性问题越来越多，尤其是随着无人机技术领域的发展，通过无人机的私有安全链路进行数据传输很难实现远距离的数据传输，因此在无人机的行业应用中可以借助公用无线通信网络作为通信备份链路。

目前为止，在无人机领域中，对在移动通信网络中的数据传输的安全性问题越来越受重视，但还没有一套针对无人机系统的成熟的网络安全方案。因此，如何更好地确保移动通信网络中数据传输的安全性成为研究的重点。

发明内容

本发明实施例提供了一种基于公共通信网络的数据传输方法、设备、终端、服务器及存储介质，实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，有利于第一终端和第二终端之间的远距离通信。

第一方面，本发明实施例提供了一种基于公共通信网络的数据传输方法，应用于业务设备，所述方法包括：

建立与第一终端之间的第一通信连接通道；

接收所述第一终端通过所述第一通信连接通道发送的加密数据，并将所述加密数据发送给第二终端；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第二方面，本发明实施例提供了另一种基于公共通信网络的数据传输方

法，应用于第一终端，所述方法包括：

建立与业务设备之间的第一通信连接通道；

通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

- 5 其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

- 10 第三方面，本发明实施例提供了又一种基于公共通信网络的数据传输方法，应用于网络服务器，所述方法包括：

建立与第一终端的第二通信连接通道；

接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密；

- 15 其中，当所述第一终端为控制设备、所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

- 20 第四方面，本发明实施例提供了一种基于公共通信网络的数据传输设备，应用于业务设备，所述设备包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与第一终端之间的第一通信连接通道；

- 25 接收所述第一终端通过所述第一通信连接通道发送的加密数据，并将所述加密数据发送给第二终端；

- 30 其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第五方面，本发明实施例提供了另一种基于公共通信网络的数据传输设备，应用于第一终端，所述设备包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与业务设备之间的第一通信连接通道；

通过所述第一通信连接通道向业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第六方面，本发明实施例提供了又一种基于公共通信网络的数据传输设备，应用于网络服务器，所述设备包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与第一终端的第二通信连接通道；

接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密；

其中，当所述第一终端为控制设备、所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第七方面，本发明实施例提供了一种业务设备，包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与第一终端之间的第一通信连接通道；

接收所述第一终端通过所述第一通信连接通道发送的加密数据，并将所述加密数据发送给第二终端；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第八方面，本发明实施例提供了一种终端，包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与业务设备之间的第一通信连接通道；

通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

其中，当第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第九方面，本发明实施例提供了一种网络服务器，包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与第一终端的第二通信连接通道；

接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密；

其中，当所述第一终端为控制设备、所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

第十方面，本发明实施例提供了一种计算机可读存储介质，该计算机可读

存储介质存储有计算机程序，该计算机程序被处理器执行时实现如上述第一方面、第二方面或第三方面所述的数据传输方法。

本发明实施例中，基于公共通信网络的数据传输设备可以建立与第一终端之间的第一通信连接通道，接收第一终端通过所述第一通信连接通道发送的加密数据，并将所述加密数据发送给第二终端，以使第二终端可以对所述加密数据进行解密，得到原始数据。通过这种实施方式，实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信。

10 附图说明

为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据这些附图获得其他的附图。

15 图 1 是本发明实施例提供的一种基于公共通信网络的数据传输方法交互的流程示意图；

图 2a 是本发明实施例提供的一种建立通信连接的示意图；

图 2b 是本发明实施例提供的另一种建立通信连接的示意图；

20 图 3 是本发明实施例提供的一种基于公共通信网络的数据传输方法的流程示意图；

图 4 是本发明实施例提供的另一种基于公共通信网络的数据传输方法的流程示意图；

图 5 是本发明实施例提供的又一种基于公共通信网络的数据传输方法的流程示意图；

25 图 6 是本发明实施例提供的一种基于公共通信网络的数据传输设备的结构示意图；

图 7 是本发明实施例提供的另一种基于公共通信网络的数据传输设备的结构示意图；

30 图 8 是本发明实施例提供的又一种基于公共通信网络的数据传输设备的结构示意图。

具体实施方式

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清楚、完整地描述，显然，所描述的实施例仅仅是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

下面结合附图，对本发明的一些实施方式作详细说明。在不冲突的情况下，下述的实施例及实施例中的特征可以相互组合。

本发明实施例中提供的基于公共通信网络的数据传输方法可以由一种数据传输系统执行，所述数据传输系统包括业务设备、第一终端、第二终端、网络服务器。在一些实施例中，所述第一终端可以通过所述业务设备与第二终端建立第一通信连接通道，在某些实施例中，所述第一通信连接通道可以是第一终端与所述业务设备通过传输控制协议（Transmission Control Protocol，TCP）建立的 TCP 通道；在某些实施例中，所述第一通信连接通道可以是第一终端与所述业务设备通过用户数据报协议（User Datagram Protocol，UDP）建立的 UDP 通道。所述第一终端可以通过所述第一通信连接通道与业务设备进行双向通信。在一些实施例中，所述第二终端与所述业务设备也可以通过 TCP 建立 TCP 通道或通过 UDP 建立 UDP 通道，以使所述第二终端可以和所述业务设备进行双向通信连接，以进行双向通信。如此，第一终端与第二终端分别与业务设备建立通信连接，进而经由业务设备实现彼此之间的第一通信连接。

所述第一终端可以通过所述网络服务器与所述第二终端建立第二通信连接通道，在某些实施例中，所述第二通信连接通道可以是第一终端通过超文本传输安全协议（Hypertext Transfer Protocol Secure，HTTPS）建立的 HTTPS 通道，以实现所述第一终端与网络服务器之间的双向通信连接，或实现所述第二终端与网络服务器之间的双向通信连接。如此，第一终端与第二终端分别与网络服务器建立通信连接，进而经由网络服务器实现彼此之间的第二通信连接。在某些实施例中，公共通信网络可以包括公共无线网络，所述业务设备可以设置在诸如 4G 或 5G 等移动通信网络中用于数据传输的服务器（或者，业务设备即在诸如 4G 或 5G 等移动通信网络中用于数据传输的业务服务器，该业务服务器可以设于公有云或私有云中）上，当然，也并限于上述 4G 或 5G

等移动通信网络，只要是公用无线通信网络即可；在某些实施例中，所述第一终端可以设置在包括显示设备（如用户界面）的控制设备（如第二终端的远程遥控设备、移动终端（如手机、平板电脑等））上，所述第二终端可以设置在移动平台（如无人机、无人船、无人汽车、机器人等）上；在某些实施例中，

5 所述第一终端可以设置在移动平台上，所述第二终端可以设置在包括显示设备的控制设备上。可以理解，对于控制设备而言，若在以下的应用场景中可以不通过显示设备进行相关操作，则控制设备也可以不包括显示设备。下面以应用于无人机的数据传输方法进行示意性说明。

本发明实施例提出的基于公共通信网络的数据传输方法可以应用于无人

10 机领域。其中，无人机领域，一般采用无人机的私有安全链路（如私有图传遥控链路，其中，无人机往往只有一种通信链路，即 WIFI 或私有图传遥控链路）进行数据传输（如图像传输或遥控数据传输）较为安全。但由于私有安全链路控制的距离较近，当控制距离较远时，私有安全链路无法进行数据传输。在无人机行业应用中，可以利用无线自组网的方式实现相对较远距离的数据传输，

15 但无线自组网的网络覆盖范围小以及在飞行中的物体、建筑物遮挡，会导致无线自组网失效。而由于无人机飞行的特殊性，需要时刻保持飞机可控，因此在行业应用中可以借助于公共无线通信网络作为通信备份链路。一般来说，4G/5G 等移动通信网络运行在公网，无人机与遥控端之间的数据容易被第三方劫持，导致飞行任务容易遭到黑客攻击。因此，如何在公共无线通信网络中保

20 护飞行安全是无人机在诸如 4G/5G 等移动通信网络的图传控制中非常重要的一点。本发明实施例中，通过公用无线通信网络对待传输的数据进行加密后，进行远距离的数据传输，可以确保数据传输的安全性。

在本发明实施例中，以公用无线通信网络为移动通信网络为例进行说明。其中，所述移动通信网络可以包括第四代移动通信网络（the 4th Generation

25 mobile communication technology, 4G）或第五代移动通信网络（Fifth-Generation, 5G）。

在一个实施例中，在结合 4G 或 5G 等移动通信网络和无人机的私有安全链路进行数据传输时，无人机（如第一终端）可以和控制设备（如第二终端）进行近距离对频。在无人机和所述控制设备进行近距离对频之后，所述无人机

30 可以和控制设备同步预设类型的数据组（如三元组）。在某些实施例中，所述

预设类型的数据组是所述无人机和所述控制设备在对频之后,根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的;在某些实施例中,所述同步随机数包括所述无人机生成的随机数和/或控制设备生成的随机数。

在一个实施例中,所述无人机可以向网络服务器发送登录认证信息,所述
5 登录认证信息携带了业务认证信息的获取请求。所述网络服务器可以对所述登录认证信息进行验证,并在验证成功之后将业务认证信息发送给所述无人机。无人机可以向业务设备发送业务认证信息,以使所述业务设备与所述无人机之间建立 TCP 通道或 UDP 通道。无人机可以根据生成的随机数计算得到数据密钥,并根据根密钥和预设类型的数据组经过加密运算得到业务密钥。无人机可以
10 根据业务密钥对数据密钥进行加密得到加密密钥,并将加密密钥通过网络服务器同步发送给控制设备。无人机可以根据数据密钥对待传输的原始数据进行加密得到加密数据,并通过 TCP 通道或 UDP 通道将加密数据发送给业务设备,以使业务设备可以将加密数据转发给控制设备。如此,可以实现控制设备与无人机之间的数据的安全传输。而在遥控设备根据同步的加密密钥对所述加密数
15 据进行解密,得到加密数据对应的原始数据时,由于,所述加密密钥是业务密钥对数据密钥进行加密得到的,且所述业务密钥根据根密钥和预设类型的数据组计算得到的,所述预设类型的数据组则是进一步通过私有安全链路同步至第一终端和第二终端的(所述根密钥是固定的),如此,通过私有安全链路同步预设类型的数据组可以确保业务密钥的安全性,对所述数据密钥进行二次加
20 密,进一步提高了数据的安全性。因此,通过这种结合无人机与遥控设备的私有安全链路以及公用无线通信网络的方式,不仅实现了对公共无线通信网络中的数据传输进行加密控制,提高了公共无线通信网络中数据传输的安全性,也有利于无人机和遥控设备之间的远距离通信,尤其有利于无人机的应用。

25 下面结合附图对本发明实施例提供的基于公共通信网络的数据传输方法的实施例进行示意性说明。

请参见图 1,图 1 是本发明实施例提供的一种基于公共通信网络的数据传输方法交互的流程示意图,所述交互方法可以应用于数据传输系统,其中,所述数据传输系统的具体解释如前所述。具体地,本发明实施例的所述方法包括
30 如下步骤。

S101: 第一终端向网络服务器发送登录认证信息, 所述登录认证信息携带了业务认证信息的获取请求。

本发明实施例中, 第一终端可以向网络服务器发送登录认证信息, 所述登录认证信息携带了业务认证信息的获取请求。在一个实施例中, 所述第一终端
5 可以通过私有安全链路向网络服务器发送登录认证信息, 以防止所述登录认证信息被其他设备劫持。在某些实施例中, 所述第一终端可以为控制设备或移动平台。

在某些实施例中, 所述业务认证信息可以为业务令牌如业务 token, 所述登录认证信息可以为登录认证令牌如登录 token。在某些实施例中, 所述登录
10 认证信息可以通过第三终端从用户中心服务器中获取, 并发送给第一终端和第二终端中的一个, 并由第一终端和第二终端中的一个利用私有安全链路同步给另一个; 在某些实施例中, 所述第三终端可以是控制设备, 或者, 所述第三终端可以是与控制设备建立通信连接的设备。在某些实施例中, 所述登录认证信息是通过第三终端将身份认证信息发送给用户中心服务器, 以使所述用户中心
15 服务器可以对所述身份认证信息进行验证, 如果验证成功, 则所述用户服务器中心向第三终端发送所述登录认证信息。在某些实施例中, 所述身份认证信息可以包括账户信息和密码, 所述账户信息和密码是通过第三终端的用户界面获取到的, 在某些实施例中, 所述第三终端为与所述用户中心服务器建立通信连接的设备。

20 其中, 可以理解, 用户中心服务器中可以存储有关于移动平台以及移动平台对应的控制设备的相关信息, 从而可以实现对第三终端发送的账户信息和密码进行认证。用户中心服务器可以独立于网络服务器, 也可以是网络服务器包括用户中心服务器, 即网络服务器可以实现用户中心服务器的功能, 也能实现给第一终端、第二终端发送业务认证信息的功能。

25 例如, 假设所述第一终端是无人机, 第二终端是控制设备, 所述用户界面设置在所述控制设备上, 则用户可以通过所述控制设备的用户界面输入账户信息和密码, 以使所述控制设备将所述账户信息和密码发送给用户中心服务器进行验证, 如果用户中心服务器验证成功, 则可以向控制设备发送登录认证信息, 所述控制设备可以将所述登录认证信息同步发送给作为第一终端的无人机, 以
30 使无人机可以将登录认证信息发送给网络服务器, 以获取业务认证信息。

S102: 网络服务器对所述登录认证信息进行验证,并在验证成功之后发送业务认证信息给所述第一终端。

本发明实施例中,网络服务器在接收到第一终端发送的登录认证信息之后,可以对所述登录认证信息进行验证,如果验证成功,则可以建立与所述第一终端的第二通信连接通道,并通过第二通信连接通道将业务认证信息发送给所述第一终端。

在一个实施例中,所述网络服务器在接收到第一终端发送的登录认证信息之后,可以对所述登录认证信息进行验证,如果验证成功,则可以允许所述第一终端登录所述网络服务器,所述网络服务器可以将所述第一终端请求获取的业务认证信息发送给所述第一终端。

S103: 第一终端向业务设备发送所述业务认证信息。

本发明实施例中,第一终端可以向业务设备发送所述业务认证信息。

S104: 业务设备建立与第一终端之间的第一通信连接通道。

本发明实施例中,业务设备可以根据所述业务认证信息建立与第一终端之间的第一通信连接通道。在某些实施例中,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

具体可以图 2a 为例进行说明,图 2a 是本发明实施例提供的一种建立通信连接的示意图。如图 2a 所示,第一终端 21 可以通过验证网络服务器 22 的设备证书来建立第二通信连接通道如 HTTPS 通道,并通过所述第二通信连接通道向所述网络服务器发送给登录认证信息。在某些实施例中,所述登录认证信息中携带了业务认证信息的获取请求。所述网络服务器 22 在接收到所述登录认证信息之后,可以对所述登录认证信息进行验证,如果验证成功,则可以响应所述业务认证信息的获取请求,将业务认证信息发送给第一终端 21。第一终端 21 可以将所述业务认证信息发送给业务设备 23,所述业务设备 23 可以根据所述业务认证信息建立与第一终端 21 之间的第一通信连接通道如 TCP 通道或 UDP 通道。在某些实施例中,所述第一终端可以为无人机或者控制设备。

同理,又以图 2b 为例进行说明,图 2b 是本发明实施例提供的另一种建立通信连接的示意图。如图 2b 所示,第二终端 24 可以通过验证网络服务器 22 的设备证书来建立第二通信连接通道如 HTTPS 通道,并通过所述第二通信连接通道向所述网络服务器发送给登录认证信息。在某些实施例中,所述登录认

证信息中携带了业务认证信息的获取请求。所述网络服务器 22 在接收到所述登录认证信息之后，可以对所述登录认证信息进行验证，如果验证成功，则可以响应所述业务认证信息的获取请求，将业务认证信息发送给第二终端 24。第二终端 24 可以将所述业务认证信息发送给业务设备 23，所述业务设备 23 可以根据所述业务认证信息建立与第二终端 24 之间的第一通信连接通道如 TCP 通道或 UDP 通道。在某些实施例中，所述第二终端可以为无人机或者控制设备。

如此，第一终端 21、第二终端 24 均可以与网络服务器 22 建立第二通信连接通道，且均可以通过网络服务器 22 与业务设备 23 建立第一通信连接通道。

S105: 第一终端根据生成的随机数计算得到数据密钥。

本发明实施例中，第一终端可以根据生成的随机数计算得到数据密钥。

S106: 第一终端根据根密钥和预设类型的数据组经过加密运算得到业务密钥。

本发明实施例中，第一终端可以根据根密钥和预设类型的数据组经过加密运算得到业务密钥。

在某些实施例中，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。例如，假设所述第一终端为无人机，所述第二终端为控制设备，则所述无人机和控制设备在出厂之前，需要烧录经过证书中心签发过的私钥即根密钥。

在某些实施例中，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；在某些实施例中，所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。本发明实施例通过私有安全链路在第一终端和第二终端之间对同步随机数和/或验证码进行同步处理的方式，使得第一终端和第二终端拥有相同的预设类型的数据组，且第三方无法获取该预设类型的数据组，确保所述预设类型数据组的安全性。

S107: 第一终端根据业务密码对所述数据密钥进行加密得到加密密钥。

本发明实施例中，第一终端可以根据业务密码对所述数据密钥进行加密得到加密密钥。

在某些实施例中，所述业务密钥是根据根密钥和预设类型的数据组计算得

到,所述根密钥是预设不变的,所述预设类型的数据组是第一终端和所述第二终端在对频之后,根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的,所述数据密钥是第一终端根据生成的随机数计算得到的,其中,所述随机数和同步随机数在第一终端重启时才会发生变化,因此,所述加密密钥在第一终端重启之前是不变的,所述加密密钥只需要生成一次即可。

在某些实施例中,第一终端可以采用对称加密算法、非对称加密算法或 Hash 算法对所述数据密钥进行加密,本发明实施例对所述数据密钥进行加密的算法不做具体限定。

S108: 第一终端将所述加密密钥发送给网络服务器。

本发明实施例中,第一终端可以将所述加密密钥发送给网络服务器。在一些实施例中,所述第一终端可以通过第二通信连接通道向所述网络服务器发送加密密钥,以便第二终端可以从所述网络服务器中获取所述加密密钥。在某些实施例中,所述第二通信连接通道包括 HTTPS 通道。

在一个实施例中,所述第一终端还可以通过第一通信连接通道向业务设备发送加密密钥,以便所述业务设备可以通过第一通信连接通道将所述加密密钥发送给所述第二终端。

可以理解,在上述两种加密密钥的传输方式中,可以优选将加密密钥发送至网络服务器,如此,可以将加密密钥以及下述说明的加密数据从两个不同的传输路径传输至第二终端,有利于防止加密密钥和加密数据被第三方同时截取而造成的加密数据的泄露,进一步提高了第一终端和第二终端之间的数据传输的安全性。

在某些实施例中,所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的;在某些实施例中,所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。在某些实施例中,所述设备证书包括网络服务器证书和/或终端设备证书,所述网络服务器证书设置于网络服务器上,所述终端设备证书设置于所述第一终端上。例如,假设所述第一终端为无人机,所述第二终端为控制设备,则所述无人机和控制设备在出厂之前,需要烧录经过证书中心签发过的设备证书。

可以理解,数据密钥也可以不利用业务密钥进行加密,相应的,数据密钥或对数据密钥加密后的加密密钥可以不经由网络服务器或业务设备在第一终

端或第二终端进行转发,而是可以在第一终端与第二终端在近距离对频时经由私有安全链路传输。

S109: 第二终端从网络服务器中获取所述加密密钥。

5 本发明实施例中,第二终端可以从网络服务器中获取所述加密密钥。具体的,只要第一终端具有诸如 4G、5G 等移动通信网络的信号,则可以主动去网络服务器请求获取加密密钥,直至获取到加密密钥为止。

S110: 第一终端根据数据密钥对待传输的原始数据进行加密得到加密数据。

10 本发明实施例中,第一终端可以根据数据密钥对待传输的原始数据进行加密得到加密数据。在某些实施例中,第一终端可以采用对称加密算法、非对称加密算法或 Hash 算法对待传输的原始数据进行加密,本发明实施例对原始数据进行加密的算法不做具体限定。

15 在某些实施例中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述加密数据包括所述控制设备对所述移动平台的控制数据;或,当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时,所述加密数据包括所述移动平台采集的工作数据。在某些实施例中,控制数据可以为诸如摇杆数据、变焦数据、飞行参数的设定数据等能控制无人机执行相应操作的数据,所述工作数据可以包括图像数据、视频数据、电量数据、位置数据,也可以包括所述移动平台采集到的其他数据,本发明实施例不做具体限定。

20 例如,假设所述第一终端为无人机的控制设备,所述第二终端为无人机,则所述待传输的原始数据为所述控制设备对所述无人机的控制数据如摇杆数据。又例如,假设所述第一终端为无人机,所述第二终端为无人机的控制设备,则所述待传输的原始数据为无人机采集的工作数据如图像数据。

S111: 第一终端将所述加密数据发送给业务设备。

25 本发明实施例中,第一终端可以通过第一通信连接通道将所述加密数据发送给业务设备。例如,假设所述第一终端为无人机,所述加密数据为加密图像数据,则所述无人机可以通过 TCP 通道或 UDP 通道将所述加密图像数据发送给业务设备。

S112: 业务设备将所述加密数据发送给第二终端。

30 本发明实施例中,业务设备可以通过第一通信连接通道将所述加密数据发

送给第二终端。例如，所述无人机可以将获取到的加密图像数据通过 TCP 通道或 UDP 通道发送给控制设备。

S113: 第二终端根据所述加密密钥对所述加密数据进行解密，得到原始数据。

5 本发明实施例中，第二终端可以根据所述加密密钥对所述加密数据进行解密，得到原始数据。在一个实施例中，所述第二终端可以根据所述加密密钥对所述加密数据进行解密，得到数据密钥，并根据所述数据密钥对所述加密数据进行解密得到所述第一终端传输给所述第二终端的原始数据。

10 例如，假设第一终端为无人机，第二终端为控制设备，如果所述原始数据为图像数据，则所述控制设备可以根据加密密钥对加密图像数据进行解密，得到数据密钥，并根据所述数据密钥对所述加密图像数据进行解密，得到所述无人机传输给所述控制的图像数据。

可以理解，在图 1 所示实施例中的部分步骤之间可以其它时序，例如，步骤 S108 与步骤 S111 可以同步执行，也可以是步骤 S111 在步骤 S108 之前执行，15 具体可以根据需要进行设定，图 1 并不对步骤之间的时序造成限定。

本发明实施例中，第一终端可以向网络服务器发送登录认证信息，以使网络服务器对所述登录认证信息中携带的身份认证信息进行验证，并在验证成功之后，向所述第一终端发送业务认证信息。所述第一终端可以将所述业务认证信息发送给业务设备，以使业务设备建立与第一终端之间的第一通信连接通20 道。第一终端可以对待传输的原始数据进行加密得到加密数据，并通过所述第一通信连接通道将加密数据发送给业务设备，以使业务设备将所述加密数据发送给第二终端。如此，可以实现第一终端与第二终端的数据的安全传输。而在第二终端根据同步的加密密钥对所述加密数据进行解密，得到原始数据时，由于，所述加密密钥是业务密钥对数据密钥进行加密得到的，且所述业务密钥根据根密钥和预设类型的数据组计算得到的，所述预设类型的数据组则是进一步25 通过私有安全链路同步至第一终端和第二终端的（所述根密钥是固定的），如此，通过私有安全链路同步预设类型的数据组可以确保业务密钥的安全性，对所述数据密钥进行二次加密，进一步提高了数据的安全性。因此，通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式，不仅实30 现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网

络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其有利于无人机的应用。

请参见图 3，图 3 是本发明实施例提供的一种基于公共通信网络的数据传输方法的流程图，所述方法可以由基于公共通信网络的数据传输设备执行，其中，所述数据传输设备可以设置在业务设备上。本发明实施例对应用于业务设备的数据传输方法的详细实施过程的示意性说明如下。

S301: 建立与第一终端之间的第一通信连接通道。

本发明实施例中，所述数据传输设备可以建立与第一终端之间的第一通信连接通道。在某些实施例中，所述第一通信连接通道可以为 TCP 通道或 UDP 通道。

在一个实施例中，所述数据传输设备在建立与第一终端之间的第一通信连接通道时，可以接收第一终端发送的业务认证信息，并根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。在某些实施例中，所述业务认证信息是所述第一终端通过第二通信连接通道和登录认证信息从网络服务器中获取到的。在某些实施例中，所述第二通信连接通道可以包括 HTTPS 通道，所述 HTTPS 在 HTTP 协议的基础上加入了 TLS 协议，其目的是保证数据在诸如 4G 或 5G 等移动通信网络上传输的安全性。在某些实施例中，所述登录认证信息可以为登录令牌即登录 token，在某些实施例中，所述业务认证信息可以业务令牌即业务 token。

在某些实施例中，所述第二通信连接通道可以是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；在某些实施例中，所述第二通信连接通道可以是所述第一终端通过校验所述网络服务器的设备证书建立的。在某些实施例中，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，所述终端设备证书设置于所述第一终端上。

在某些实施例中，所述登录认证信息携带了所述业务认证信息的获取请求；其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送业务认证信息给所述第一终端。

例如，假设所述第一终端为无人机，所述第二终端为控制设备，则所述无

人机可以通过对网络服务器的设备证书进行校验,以及所述网络服务器对所述无人机的设备证书进行校验,以建立所述无人机与网络服务器之间的 HTTPS 通道。所述无人机可以通过所述 HTTPS 通道将登录认证信息发送给网络服务器,网络服务器根据所述登录认证信息对所述登录认证信息进行验证,并在验证成功之后向无人机发送业务认证信息。所述无人机可以将业务认证信息发送给业务设备,以使业务设备可以根据所述业务认证信息建立与无人机之间的 TCP 通道或 UDP 通道,以便无人机可以通过所述 TCP 通道或 UDP 通道向业务设备传输数据。

在一个实施例中,所述第一终端可以为无人机,所述第二终端可以为控制设备;或所述第一终端可以为控制设备,所述第二终端可以为无人机。所述控制设备上包括用户界面,所述用户界面上包括应用程序 APP,用户可以通过所述用户界面在所 AAP 上输入账户信息和密码,所述控制设备可以将所述 APP 上获取到所述账户信息和密码发送给用户中心服务器,以使用户中心服务器对所述账户信息和密码进行验证,如果验证成功,则所述用户中心服务器向所述控制设备返回登录认证信息,所述控制设备可以通过私有安全链路将所述登录认证信息同步发送给无人机。同时,控制设备可以通过 HTTPS 通道将所述登录认证信息发送给网络服务器,以使所述登录认证信息进行验证。如果所述网络服务器对所述登录认证信息验证成功,则所述网络服务器可以向所述控制设备发送业务认证信息,所述控制设备可以将所述业务认证信息同步至无人机中。

可以理解,上述应用程序 APP 也可以设置在控制设备以外的设备上,如与控制设备通信连接的移动终端(如手机、平板电脑等),用户可以通过所述用户界面在所 AAP 上输入账户信息和密码,所述移动终端可以将所述 APP 上获取到所述账户信息和密码发送给用户中心服务器,以使用户中心服务器对所述账户信息和密码进行验证,如果验证成功,则所述用户中心服务器向所述移动终端返回登录认证信息,所述移动终端可以将登录认证信息发送给控制设备,再由控制设备通过私有安全链路同步发送给无人机。

S302: 接收所述第一终端通过所述第一通信连接通道发送的加密数据,并将所述加密数据发送给第二终端。

本发明实施例中,所述数据传输设备可以接收所述第一终端通过所述第一

通信连接通道发送的加密数据，并将所述加密数据发送给第二终端。

在某些实施例中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

在一个实施例中，所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的；在某些实施例中，所述数据密钥是所述第一终端根据生成的随机数计算得到的。其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

在一个实施例中，所述数据传输设备还可以接收所述第一终端通过所述第一通信连接通道发送的加密密钥，并将所述加密密钥发送给所述第二终端，以使得所述第二终端根据所述加密密钥对所述加密数据进行解密。

在某些实施例中，所述加密密钥是所述第一终端对所述数据密钥进行加密得到的，具体地，所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。在某些实施例中，所述业务密码是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。在某些实施例中，所述根密钥是所述第一终端和所述第二终端中预先设置的，其中，所述第一终端的根密钥与所述第二终端的根密钥相同。在某些实施例中，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；其中，所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

例如，假设所述第一终端为无人机，所述第二终端为控制设备，所述待传输的原始数据为所述无人机采集的图像数据，则第一终端可以根据生成的随机数计算得到数据密钥，并根据所述数据密钥对所述无人机采集到的图像数据进行加密，得到加密数据。所述无人机可以根据业务密码对所述数据密钥进行加密得到加密密钥，并将所述加密密钥通过网络服务器发送给控制设备。所述无人机可以通过 TCP 通道或 UDP 通道将所述加密数据发送给业务设备，以使所述业务设备将所述加密数据发送给控制设备，以便所述控制设备可以根据加密

密钥对所述加密数据进行解密,得到数据密钥,并根据所述数据密钥对所述加密数据进行解密得到图像数据。

本发明实施例中,数据传输设备可以建立与第一终端之间的第一通信连接通道,并接收所述第一终端通过所述第一通信连接通道发送的加密数据,以及
5 将所述加密数据发送给第二终端。如此,可以实现第一终端与第二终端之间的数据的安全传输。而在第二终端根据同步的加密密钥对所述加密数据进行解密,得到原始数据时,由于,所述加密密钥是业务密钥对数据密钥进行加密得到的,且所述业务密钥根据根密钥和预设类型的数据组计算得到的,所述预设类型的数据组则是进一步通过私有安全链路同步至第一终端和第二终端的(所述根密钥是固定的),如此,通过私有安全链路同步预设类型的数据组可以确
10 保业务密钥的安全性,对所述数据密钥进行二次加密,进一步提高了数据的安全性。因此,通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式,不仅实现了对公共无线通信网络中的数据传输进行加密控制,提高了公共无线通信网络中数据传输的安全性,也有利于第一终端和第二
15 终端之间的远距离通信,尤其有利于无人机的应用。

请参见图 4,图 4 是本发明实施例提供的另一种基于公共通信网络的数据传输方法的流程示意图,所述方法可以由基于公共通信网络的数据传输设备执行,其中,所述数据传输设备可以设置在第一终端上。本发明实施例对应用于
20 第一终端的数据传输方法的详细实施过程的示意性说明如下。

S401: 建立与业务设备之间的第一通信连接通道。

本发明实施例中,所述数据传输设备可以建立与业务设备之间的第一通信连接通道。其中,所述第一通信连接通道的解释如前所述,此处不再赘述。

在一个实施例中,所述数据传输设备在建立与业务设备之间的第一通信连接通道时,可以向业务设备发送业务认证信息,并根据所述业务认证信息建立与
25 所述第一终端之间的第一通信连接通道。在某些实施例中,所述业务认证信息是通过第二通信连接通道和登录认证信息从网络服务器中获取到的。在某些实施例中,所述第一通信连接通道的解释如前所述,所述第二通信连接通道的解释如前所述,所述设备证书的解释如前所述,此处不再赘述。

30 在某些实施例中,所述登录认证信息携带了所述业务认证信息的获取请

求；其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送业务认证信息给所述第一终端。具体实施例如前所述，此处不再赘述。

S402: 通过所述第一通信连接通道向所述业务设备发送加密数据，以使得
5 所述业务设备将所述加密数据发送至第二终端。

本发明实施例中，所述数据传输设备可以通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端。在某些实施例中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当
10 所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。其中，所述加密数据的解释如前所述，所述数据密钥的解释如前所述，此处均不再复述。

在一个实施例中，所述数据传输设备可以通过所述第二通信连接通道向所述网络服务器发送加密密钥，以使得所述第二终端根据从所述网络服务器获取
15 的所述加密密钥对所述加密数据进行解密；或者，通过所述第一通信连接通道向所述业务设备发送加密密钥，以使得所述第二终端根据从所述业务设备获取的所述加密密钥对所述加密数据进行解密；其中，所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。在某些实施例中，所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。其
20 中，所述根密钥的解释如前所述，所述预设类型的数据组的解释如前所述，此处均不再复述。

例如，假设所述第一终端为控制设备，所述第二终端为无人机，所述待传输的原始数据为对所述无人机的控制数据，则控制设备可以根据生成的随机数计算得到数据密钥，并根据所述数据密钥对所述控制数据进行加密，得到加密
25 数据。所述控制设备可以根据业务密码对所述数据密钥进行加密得到加密密钥，并将所述加密密钥通过网络服务器发送给无人机。所述控制设备可以通过TCP通道或UDP通道将所述加密数据发送给业务设备，以使所述业务设备将所述加密数据发送给无人机，以便所述无人机可以根据加密密钥对所述加密数据进行解密，得到数据密钥，并根据所述数据密钥对所述加密数据进行解密得
30 到所述控制数据，从而使所述无人机可以根据所述控制数据对无人机进行控

制。

本发明实施例中，数据传输设备可以建立与业务设备之间的第一通信连接通道，并通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端。如此，可以实现第一终端与第二终端之间的数据的安全传输。而在第二终端根据同步的加密密钥对所述加密数据进行解密，得到原始数据时，由于，所述加密密钥是业务密钥对数据密钥进行加密得到的，且所述业务密钥根据根密钥和预设类型的数据组计算得到的，所述预设类型的数据组则是进一步通过私有安全链路同步至第一终端和第二终端的（所述根密钥是固定的），如此，通过私有安全链路同步预设类型的数据组可以确保业务密钥的安全性，对所述数据密钥进行二次加密，进一步提高了数据的安全性。因此，通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式，不仅实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其有利于无人机的应用。

15

请参见图 5，图 5 是本发明实施例提供的又一种基于公共通信网络的数据传输方法的流程示意图，所述方法可以由基于公共通信网络的数据传输设备执行，其中，所述数据传输设备可以设置在网络服务器上。本发明实施例对应用于网络服务器的数据传输方法的详细实施过程的示意性说明如下。

20 S501：建立与第一终端的第二通信连接通道。

本发明实施例中，数据传输设备可以建立与第一终端的第二通信连接通道。在某些实施例中，所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。其中，所述设备证书的解
25 释如前所述，此处不再赘述。在某些实施例中，所述第二通信通道包括 HTTPS 通道。

S502：接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密。

30 本发明实施例中，数据传输设备可以接收所述第一终端通过所述第二通信

连接通道发送的加密密钥,以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密。

在某些实施例中,当所述第一终端为控制设备、所述第二终端为移动平台时,所述加密数据包括所述控制设备对所述移动平台的控制数据;或,当所述
5 第一终端为所述移动平台、且所述第二终端为所述控制设备时,所述加密数据包括所述移动平台采集的工作数据。

在一个实施例中,所述加密密钥是所述第一终端对数据密钥加密得到的,所述加密数据是所述第一终端根据所述数据密钥对待传输的原始数据进行加密得到的;其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,
10 所述原始数据为所述控制设备对所述移动平台的控制数据;或,当所述第一终端为移动平台、且所述第二终端为控制设备时,所述原始数据为所述移动平台采集的工作数据。在某些实施例中,所述加密密钥是所述第一终端根据业务密码对数据密钥进行加密得到的。在某些实施例中,所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。在某些实施例中,所
15 述数据密钥是第一终端根据生成的随机数计算得到的。其中,所述根密钥的解释和所述预设类型的数据组的解释如前所述,此处不再赘述。

在一个实施例中,所述数据传输设备在建立与第一终端的第二通信连接通道之后,还可以接收所述第一终端通过所述第二通信连接通道发送的登录认证信息,将所述登录认证信息对应的业务认证信息给所述第一终端,以使得所述
20 第一终端根据所述业务认证信息建立与业务设备之间的第一通信连接通道。在某些实施例中,所述加密数据为所述第一终端通过所述第一通信连接通道发送至所述业务设备,并由所述业务设备发送至所述第二终端。在某些实施例中,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

在某些实施例中,所述登录认证信息携带了所述业务认证信息的获取请求;其中,所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证,并在验证成功之后发送业务认证信息给所述第一终端。具体实施例如前所述,此处不再赘述。

本发明实施例中,数据传输设备可以建立与第一终端的第二通信连接通
30 道,并接收所述第一终端通过所述第二通信连接通道发送的加密密钥。如此,

可以实现第一终端与第二终端之间的数据的安全传输。而在第二终端根据同步的加密密钥对所述加密数据进行解密,得到原始数据时,由于,所述加密密钥是业务密钥对数据密钥进行加密得到的,且所述业务密钥根据根密钥和预设类型的数据组计算得到的,所述预设类型的数据组则是进一步通过私有安全链路同步至第一终端和第二终端的(所述根密钥是固定的),如此,通过私有安全链路同步预设类型的数据组可以确保业务密钥的安全性,对所述数据密钥进行二次加密,进一步提高了数据的安全性。因此,通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式,不仅实现了对公共无线通信网络中的数据传输进行加密控制,提高了公共无线通信网络中数据传输的安全性,也有利于第一终端和第二终端之间的远距离通信,尤其有利于无人机的应用。

请参见图 6,图 6 是本发明实施例提供的一种基于公共通信网络的数据传输设备的结构示意图。具体的,所述数据传输设备包括:存储器 601、处理器 602 以及数据接口 603。

所述存储器 601 可以包括易失性存储器 (volatile memory); 存储器 601 也可以包括非易失性存储器 (non-volatile memory); 存储器 601 还可以包括上述种类的存储器的组合。所述处理器 602 可以是中央处理器 (central processing unit, CPU)。所述处理器 602 还可以进一步包括硬件数据传输设备。上述硬件数据传输设备可以是专用集成电路 (application-specific integrated circuit, ASIC), 可编程逻辑器件 (programmable logic device, PLD) 或其组合。具体例如可以是复杂可编程逻辑器件 (complex programmable logic device, CPLD), 现场可编程逻辑门阵列 (field-programmable gate array, FPGA) 或其任意组合。

进一步地,所述存储器 601 用于存储程序指令,当程序指令被执行时所述处理器 602 可以调用存储器 601 中存储的程序指令,用于执行如下步骤:

建立与第一终端之间的第一通信连接通道;

接收所述第一终端通过所述第一通信连接通道发送的加密数据,并将所述加密数据发送给第二终端;

其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述加密数据包括所述控制设备对所述移动平台的控制数据;或,当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时,所述加密数据包括所述

移动平台采集的工作数据。

进一步地，所述处理器 602 建立与第一终端之间的第一通信连接通道时，具体用于：

接收第一终端发送的业务认证信息，所述业务认证信息是所述第一终端通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

进一步地，所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

进一步地，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，所述终端设备证书设置于所述第一终端上。

进一步地，所述第二通信连接通道包括超文本传输安全协议 HTTPS 通道。

进一步地，所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送业务认证信息给所述第一终端。

进一步地，所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括所述用户中心服务器。

进一步地，所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

进一步地，所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为

移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

进一步地，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

进一步地，所述处理器 602 还用于：

- 5 接收所述第一终端通过所述第一通信连接通道发送的加密密钥，并将所述加密密钥发送给所述第二终端，以使得所述第二终端根据所述加密密钥对所述加密数据进行解密；

所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

- 10 进一步地，所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

进一步地，所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

进一步地，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

- 15 进一步地，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

- 20 本发明实施例中，所述数据传输设备可以建立与第一终端之间的第一通信连接通道，并接收所述第一终端通过所述第一通信连接通道发送的加密数据，以及将所述加密数据发送给第二终端。如此，可以实现第一终端与第二终端之间的数据的安全传输。而在第二终端根据同步的加密密钥对所述加密数据进行解密，得到原始数据时，由于，所述加密密钥是业务密钥对数据密钥进行加密
- 25 得到的，且所述业务密钥根据根密钥和预设类型的数据组计算得到的，所述预设类型的数据组则是进一步通过私有安全链路同步至第一终端和第二终端的（所述根密钥是固定的），如此，通过私有安全链路同步预设类型的数据组可以确保业务密钥的安全性，对所述数据密钥进行二次加密，进一步提高了数据的安全性。因此，通过这种结合第一终端与第二终端的私有安全链路以及公用
- 30 无线通信网络的方式，不仅实现了对公共无线通信网络中的数据传输进行加密

控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其有利于无人机的应用。

请参见图 7，图 7 是本发明实施例提供的另一种基于公共通信网络的数据传输设备的结构示意图。具体的，所述数据传输设备包括：存储器 701、处理器 702 以及数据接口 703。

所述存储器 701 可以包括易失性存储器 (volatile memory)；存储器 701 也可以包括非易失性存储器 (non-volatile memory)；存储器 701 还可以包括上述种类的存储器的组合。所述处理器 702 可以是中央处理器 (central processing unit, CPU)。所述处理器 702 还可以进一步包括硬件数据传输设备。上述硬件数据传输设备可以是专用集成电路 (application-specific integrated circuit, ASIC)，可编程逻辑器件 (programmable logic device, PLD) 或其组合。具体例如可以是复杂可编程逻辑器件 (complex programmable logic device, CPLD)，现场可编程逻辑门阵列 (field-programmable gate array, FPGA) 或其任意组合。

进一步地，所述存储器 701 用于存储程序指令，当程序指令被执行时所述处理器 702 可以调用存储器 701 中存储的程序指令，用于执行如下步骤：

建立与业务设备之间的第一通信连接通道；

通过所述第一通信连接通道向业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

进一步地，所述处理器 702 建立与业务设备之间的第一通信连接通道时，具体用于：

向业务设备发送业务认证信息，所述业务认证信息是通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

进一步地，所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

进一步地，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，所述终端设备证书设置于所述第一终端上。

进一步地，所述第二通信连接通道包括 HTTPS 通道。

进一步地，所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送业务认证信息给所述第一终端。

10 进一步地，所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括所述用户中心服务器。

15 进一步地，所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

进一步地，所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

25 进一步地，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

进一步地，所述处理器 702 还用于：

通过所述第二通信连接通道向所述网络服务器发送加密密钥，以使得所述第二终端根据从所述网络服务器获取的所述加密密钥对所述加密数据进行解密；或者，

30 通过所述第一通信连接通道向所述业务设备发送加密密钥，以使得所述第

二终端根据从所述业务设备获取的所述加密密钥对所述加密数据进行解密；

其中，所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

进一步地，所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

5 进一步地，所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

进一步地，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

10 进一步地，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

15 本发明实施例中，数据传输设备可以建立与业务设备之间的第一通信连接通道，并通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端。如此，可以实现第一终端与第二终端的数据的安全传输。而在第二终端根据同步的加密密钥对所述加密数据进行解密，得到原始数据时，由于，所述加密密钥是业务密钥对数据密钥进行加密得到的，且所述业务密钥根据根密钥和预设类型的数据组计算得到的，所述
20 预设类型的数据组则是进一步通过私有安全链路同步至第一终端和第二终端的（所述根密钥是固定的），如此，通过私有安全链路同步预设类型的数据组可以确保业务密钥的安全性，对所述数据密钥进行二次加密，进一步提高了数据的安全性。因此，通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式，不仅实现了对公共无线通信网络中的数据传输进行加
25 密控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其有利于无人机的应用。

请参见图 8，图 8 是本发明实施例提供的又一种基于公共通信网络的数据传输设备的结构示意图。具体的，所述数据传输设备包括：存储器 801、处理
30 器 802 以及数据接口 803。

所述存储器 801 可以包括易失性存储器 (volatile memory); 存储器 801 也可以包括非易失性存储器 (non-volatile memory); 存储器 801 还可以包括上述种类的存储器的组合。所述处理器 802 可以是中央处理器 (central processing unit, CPU)。所述处理器 802 还可以进一步包括硬件数据传输设备。上述硬件

5 数据传输设备可以是专用集成电路 (application-specific integrated circuit, ASIC), 可编程逻辑器件 (programmable logic device, PLD) 或其组合。具体例如可以是复杂可编程逻辑器件 (complex programmable logic device, CPLD), 现场可编程逻辑门阵列 (field-programmable gate array, FPGA) 或其任意组合。

进一步地, 所述存储器 801 用于存储程序指令, 当程序指令被执行时所述

10 处理器 802 可以调用存储器 801 中存储的程序指令, 用于执行如下步骤:

建立与第一终端的第二通信连接通道;

接收所述第一终端通过所述第二通信连接通道发送的加密密钥, 以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密;

15 其中, 当所述第一终端为控制设备、所述第二终端为移动平台时, 所述加密数据包括所述控制设备对所述移动平台的控制数据; 或, 当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时, 所述加密数据包括所述移动平台采集的工作数据。

进一步地, 所述第二通信连接通道是所述第一终端和所述网络服务器之间

20 通过校验双方的设备证书建立的; 或,

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

进一步地, 所述设备证书包括网络服务器证书和/或终端设备证书, 所述网络服务器证书设置于所述网络服务器上, 所述终端设备证书设置于所述第一

25 终端上。

进一步地, 所述第二通信连接通道包括 HTTPS 通道。

进一步地, 所述加密密钥是所述第一终端对数据密钥加密得到的, 所述加密数据是所述第一终端根据所述数据密钥对待传输的原始数据进行加密得到的;

30 其中, 当所述第一终端为控制设备、且所述第二终端为移动平台时, 所述

原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

进一步地，所述加密密钥是所述第一终端根据业务密码对数据密钥进行加密得到的。

进一步地，所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

进一步地，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

进一步地，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

进一步地，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

进一步地，所述处理器 802 建立与第一终端的第二通信连接通道之后，还用于：

接收所述第一终端通过所述第二通信连接通道发送的登录认证信息；

将所述登录认证信息对应的业务认证信息给所述第一终端，以使得所述第一终端根据所述业务认证信息建立与业务设备之间的第一通信连接通道；

所述加密数据为所述第一终端通过所述第一通信连接通道发送至所述业务设备，并由所述业务设备发送至所述第二终端。

进一步地，所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送业务认证信息给所述第一终端。

进一步地，所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连

接,所述用户中心服务器独立于所述网络服务器,或者,所述网络服务器包括所述用户中心服务器。

进一步地,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

- 5 本发明实施例中,数据传输设备可以建立与第一终端的第二通信连接通道,并接收所述第一终端通过所述第二通信连接通道发送的加密密钥,以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密,得到原始数据。通过这种实施方式,实现了对网络中的数据传输进行加密控制,提高网络中数据传输的安全性。

10

本发明实施例中提供了一种业务设备,包括:处理器和存储器;所述存储器,用于存储程序指令;所述处理器,执行所述存储器存储的程序指令,当程序指令被执行时,所述处理器用于执行如下步骤:

建立与第一终端之间的第一通信连接通道;

- 15 接收所述第一终端通过所述第一通信连接通道发送的加密数据,并将所述加密数据发送给第二终端;

其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述加密数据包括所述控制设备对所述移动平台的控制数据;或,当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时,所述加密数据包括所述移动平台采集的工作数据。

20

进一步地,所述处理器建立与第一终端之间的第一通信连接通道时,具体用于:

接收第一终端发送的业务认证信息,所述业务认证信息是所述第一终端通过第二通信连接通道和登录认证信息从网络服务器中获取到的;

- 25 根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

进一步地,所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的;或,

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

- 30 进一步地,所述设备证书包括网络服务器证书和/或终端设备证书,所述

网络服务器证书设置于网络服务器上,所述终端设备证书设置于所述第一终端上。

进一步地,所述第二通信连接通道包括超文本传输安全协议 HTTPS 通道。

进一步地,所述登录认证信息携带了所述业务认证信息的获取请求;

5 其中,所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证,并在验证成功之后发送业务认证信息给所述第一终端。

进一步地,所述登录认证信息是第三终端通过用户中心服务器获取,并由所述第三终端发送给所述控制设备,以及由所述控制设备通过私有安全链路同步发送给所述移动平台的;

10 其中,所述第三终端是所述控制设备,或者,所述第三终端是与所述控制设备建立通信连接的设备;所述第三终端与所述用户中心服务器建立通信连接,所述用户中心服务器独立于所述网络服务器,或者,所述网络服务器包括所述用户中心服务器。

进一步地,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数
15 据报协议 UDP 通道。

进一步地,所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的;

其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述原始数据为所述控制设备对所述移动平台的控制数据;或,当所述第一终端为
20 移动平台、且所述第二终端为控制设备时,所述原始数据为所述移动平台采集的工作数据。

进一步地,所述数据密钥是所述第一终端根据生成的随机数计算得到的。

进一步地,所述处理器还用于:

接收所述第一终端通过所述第一通信连接通道发送的加密密钥,并将所述
25 加密密钥发送给所述第二终端,以使得所述第二终端根据所述加密密钥对所述加密数据进行解密;

所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

进一步地,所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

30 进一步地,所述业务密钥是所述第一终端根据根密钥和预设类型的数据组

经过加密运算得到的。

进一步地，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

进一步地，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

本发明实施例中，业务设备可以建立与第一终端之间的第一通信连接通道，并接收所述第一终端通过所述第一通信连接通道发送的加密数据，以及将所述加密数据发送给第二终端，以使第二终端可以对所述加密数据进行解密得到原始数据。通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式，实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其是在无人机行业应用中

本发明实施例中提供了一种终端，包括：处理器和存储器；所述存储器，用于存储程序指令；所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与业务设备之间的第一通信连接通道；

通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

其中，当第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

进一步地，所述处理器建立与业务设备之间的第一通信连接通道时，具体用于：

向业务设备发送业务认证信息，所述业务认证信息是通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

进一步地,所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的;或,

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

5 进一步地,所述设备证书包括网络服务器证书和/或终端设备证书,所述网络服务器证书设置于网络服务器上,所述终端设备证书设置于所述第一终端上。

进一步地,所述第二通信连接通道包括 HTTPS 通道。

进一步地,所述登录认证信息携带了所述业务认证信息的获取请求;

10 其中,所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证,并在验证成功之后发送业务认证信息给所述第一终端。

进一步地,所述登录认证信息是第三终端通过用户中心服务器获取,并由所述第三终端发送给所述控制设备,以及由所述控制设备通过私有安全链路同步发送给所述移动平台的;

15 其中,所述第三终端是所述控制设备,或者,所述第三终端是与所述控制设备建立通信连接的设备;所述第三终端与所述用户中心服务器建立通信连接,所述用户中心服务器独立于所述网络服务器,或者,所述网络服务器包括所述用户中心服务器。

进一步地,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

进一步地,所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的;

25 其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述原始数据为所述控制设备对所述移动平台的控制数据;或,当所述第一终端为移动平台、且所述第二终端为控制设备时,所述原始数据为所述移动平台采集的工作数据。

进一步地,所述数据密钥是所述第一终端根据生成的随机数计算得到的。

进一步地,所述处理器还用于:

30 通过所述第二通信连接通道向所述网络服务器发送加密密钥,以使得所述第二终端根据从所述网络服务器获取的所述加密密钥对所述加密数据进行解

密；或者，

通过所述第一通信连接通道向所述业务设备发送加密密钥，以使得所述第二终端根据从所述业务设备获取的所述加密密钥对所述加密数据进行解密；

其中，所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

5 进一步地，所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

进一步地，所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

10 进一步地，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述所述第一终端的根密钥与所述第二终端的根密钥相同。

进一步地，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

15 所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

20 本发明实施例中，第一终端可以建立与业务设备之间的第一通信连接通道，并通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端，从而使第二终端可以根据同步的加密密钥对所述加密数据进行解密，得到原始数据。通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式，实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其是在无人机行业应用中。

25 本发明实施例中提供了一种网络服务器，包括：处理器和存储器；所述存储器，用于存储程序指令；所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与第一终端的第二通信连接通道；

30 接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所

述第二终端的加密数据进行解密；

其中，当所述第一终端为控制设备、所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

进一步地，所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

10 进一步地，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于所述网络服务器上，所述终端设备证书设置于所述第一终端上

进一步地，所述第二通信连接通道包括 HTTPS 通道。

15 进一步地，所述加密密钥是所述第一终端对数据密钥加密得到的，所述加密数据是所述第一终端根据所述数据密钥对待传输的原始数据进行加密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

20 进一步地，所述加密密钥是所述第一终端根据业务密码对数据密钥进行加密得到的。

进一步地，所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

25 进一步地，所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

进一步地，所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

30 所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成

的随机数。

进一步地，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

进一步地，所述处理器建立与第一终端的第二通信连接通道之后，还用于：

接收所述第一终端通过所述第二通信连接通道发送的登录认证信息；

- 5 将所述登录认证信息对应的业务认证信息给所述第一终端，以使得所述第一终端根据所述业务认证信息建立与业务设备之间的第一通信连接通道；

所述加密数据为所述第一终端通过所述第一通信连接通道发送至所述业务设备，并由所述业务设备发送至所述第二终端。

进一步地，所述登录认证信息携带了所述业务认证信息的获取请求；

- 10 其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送业务认证信息给所述第一终端。

进一步地，所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

- 15 其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括所述用户中心服务器。

- 20 进一步地，所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

- 25 本发明实施例中，网络服务器可以建立与第一终端的第二通信连接通道，并接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密，得到原始数据。通过这种结合第一终端与第二终端的私有安全链路以及公用无线通信网络的方式，实现了对公共无线通信网络中的数据传输进行加密控制，提高了公共无线通信网络中数据传输的安全性，也有利于第一终端和第二终端之间的远距离通信，尤其是在无人机行业应用中。

- 30 在本发明的实施例中还提供了一种计算机可读存储介质，所述计算机可读存储介质存储有计算机程序，所述计算机程序被处理器执行时实现本发明实施

例中描述的数据传输方法方式，在此不再赘述。

所述计算机可读存储介质可以是前述任一项实施例所述的设备的内部存储单元，例如设备的硬盘或内存。所述计算机可读存储介质也可以是所述设备的外部存储设备，例如所述设备上配备的插接式硬盘，智能存储卡（Smart Media Card, SMC），安全数字（Secure Digital, SD）卡，闪存卡（Flash Card）等。进一步地，所述计算机可读存储介质还可以既包括所述设备的内部存储单元也包括外部存储设备。所述计算机可读存储介质用于存储所述计算机程序以及所述设备所需的其他程序和数据。所述计算机可读存储介质还可以用于暂时地存储已经输出或者将要输出的数据。

10 本领域普通技术人员可以理解实现上述实施例方法中的全部或部分流程，是可以通过计算机程序来指令相关的硬件来完成，所述的程序可存储于一计算机可读取存储介质中，该程序在执行时，可包括如上述各方法的实施例的流程。其中，所述的存储介质可为磁碟、光盘、只读存储记忆体（Read-Only Memory, ROM）或随机存储记忆体（Random Access Memory, RAM）等。

15 以上所揭露的仅为本发明部分实施例而已，当然不能以此来限定本发明之权利范围，因此依本发明权利要求所作的等同变化，仍属本发明所涵盖的范围。

权利要求

1. 一种基于公共通信网络的数据传输方法，其特征在于，应用于业务设备，所述方法包括：

5 建立与第一终端之间的第一通信连接通道；

接收所述第一终端通过所述第一通信连接通道发送的加密数据，并将所述加密数据发送给第二终端；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端
10 为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

2. 根据权利要求 1 所述的方法，其特征在于，所述建立与第一终端之间的第一通信连接通道，包括：

15 接收第一终端发送的业务认证信息，所述业务认证信息是所述第一终端通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

3. 根据权利要求 2 所述的方法，其特征在于，

20 所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

25 4. 根据权利要求 3 所述的方法，其特征在于，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，所述终端设备证书设置于所述第一终端上。

5. 根据权利要求 2 所述的方法，其特征在于，所述第二通信连接通道包
30 括超文本传输安全协议 HTTPS 通道。

6. 根据权利要求 2 所述的方法，其特征在于，

所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录
5 认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

7. 根据权利要求 6 所述的方法，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终
10 端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制
设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连
接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括
15 所述用户中心服务器。

8. 根据权利要求 1 所述的方法，其特征在于，所述第一通信连接通道包
括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

20 9. 根据权利要求 1 所述的方法，其特征在于，

所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加
密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述
原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为
25 移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集
的工作数据。

10. 根据权利要求 9 所述的方法，其特征在于，所述数据密钥是所述第一
终端根据生成的随机数计算得到的。

11. 根据权利要求 9 所述的方法, 其特征在于, 所述方法还包括:

接收所述第一终端通过所述第一通信连接通道发送的加密密钥, 并将所述加密密钥发送给所述第二终端, 以使得所述第二终端根据所述加密密钥对所述加密数据进行解密;

5 所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

12. 根据权利要求 11 所述的方法, 其特征在于,

所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

10

13. 根据权利要求 12 所述的方法, 其特征在于,

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

15 14. 根据权利要求 13 所述的方法, 其特征在于,

所述根密钥是所述第一终端和所述第二终端中预先设置的, 所述第一终端的根密钥与所述第二终端的根密钥相同。

15. 根据权利要求 13 所述的方法, 其特征在于,

20 所述预设类型的数据组是所述第一终端和所述第二终端在对频之后, 根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的;

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

25 16. 一种基于公共通信网络的数据传输方法, 其特征在于, 应用于第一终端, 所述方法包括:

建立与业务设备之间的第一通信连接通道;

通过所述第一通信连接通道向所述业务设备发送加密数据, 以使得所述业务设备将所述加密数据发送至第二终端;

30 其中, 当所述第一终端为控制设备、且所述第二终端为移动平台时, 所述

加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

5 17. 根据权利要求 16 所述的方法，其特征在于，所述建立与业务设备之间的第一通信连接通道，包括：

向业务设备发送业务认证信息，所述业务认证信息是通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

10

18. 根据权利要求 17 所述的方法，其特征在于，

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

15 所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

19. 根据权利要求 18 所述的方法，其特征在于，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，所述终端设备证书设置于所述第一终端上。

20

20. 根据权利要求 17 所述的方法，其特征在于，所述第二通信连接通道包括 HTTPS 通道。

21. 根据权利要求 17 所述的方法，其特征在于，

25 所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

30

22. 根据权利要求 21 所述的方法，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取,并由所述第三终端发送给所述控制设备,以及由所述控制设备通过私有安全链路同步发送给所述移动平台的;

其中,所述第三终端是所述控制设备,或者,所述第三终端是与所述控制设备建立通信连接的设备;所述第三终端与所述用户中心服务器建立通信连接,所述用户中心服务器独立于所述网络服务器,或者,所述网络服务器包括所述用户中心服务器。

23. 根据权利要求 16 所述的方法,其特征在于,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

24. 根据权利要求 16 所述的方法,其特征在于,

所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的;

其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述原始数据为所述控制设备对所述移动平台的控制数据;或,当所述第一终端为移动平台、且所述第二终端为控制设备时,所述原始数据为所述移动平台采集的工作数据。

25. 根据权利要求 24 所述的方法,其特征在于,所述数据密钥是所述第一终端根据生成的随机数计算得到的。

26. 根据权利要求 17 所述的方法,其特征在于,所述方法还包括:

通过所述第二通信连接通道向所述网络服务器发送加密密钥,以使得所述第二终端根据从所述网络服务器获取的所述加密密钥对所述加密数据进行解密;或者,

通过所述第一通信连接通道向所述业务设备发送加密密钥,以使得所述第二终端根据从所述业务设备获取的所述加密密钥对所述加密数据进行解密;

其中,所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

27. 根据权利要求 26 所述的方法，其特征在于，
所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

5 28. 根据权利要求 27 所述的方法，其特征在于，
所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

29. 根据权利要求 28 所述的方法，其特征在于，
10 所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

30. 根据权利要求 28 所述的方法，其特征在于，
所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据
15 通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；
所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

31. 一种基于公共通信网络的数据传输方法，其特征在于，应用于网络服
20 务器，所述方法包括：

建立与第一终端的第二通信连接通道；

接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密；

25 其中，当所述第一终端为控制设备、所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

30 32. 根据权利要求 31 所述的方法，其特征在于，

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

5

33. 根据权利要求 32 所述的方法，其特征在于，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于所述网络服务器上，所述终端设备证书设置于所述第一终端上。

10

34. 根据权利要求 32 所述的方法，其特征在于，所述第二通信连接通道包括 HTTPS 通道。

35. 根据权利要求 31 所述的方法，其特征在于，

15

所述加密密钥是所述第一终端对数据密钥加密得到的，所述加密数据是所述第一终端根据所述数据密钥对待传输的原始数据进行加密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

20

36. 根据权利要求 35 所述的方法，其特征在于，

所述加密密钥是所述第一终端根据业务密码对数据密钥进行加密得到的。

37. 根据权利要求 36 所述的方法，其特征在于，

25

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

38. 根据权利要求 37 所述的方法，其特征在于，

30

所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

39. 根据权利要求 37 所述的方法，其特征在于，

所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

5 所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

40. 根据权利要求 35 所述的方法，其特征在于，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

10

41. 根据权利要求 31 所述的方法，其特征在于，所述建立与第一终端的第二通信连接通道之后，还包括：

接收所述第一终端通过所述第二通信连接通道发送的登录认证信息；

15 将所述登录认证信息对应的业务认证信息给所述第一终端，以使得所述第一终端根据所述业务认证信息建立与业务设备之间的第一通信连接通道；

所述加密数据为所述第一终端通过所述第一通信连接通道发送至所述业务设备，并由所述业务设备发送至所述第二终端。

42. 根据权利要求 41 所述的方法，其特征在于，

20 所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

25 43. 根据权利要求 42 所述的方法，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

30 其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连

接, 所述用户中心服务器独立于所述网络服务器, 或者, 所述网络服务器包括所述用户中心服务器。

44. 根据权利要求 41 所述的方法, 其特征在于, 所述第一通信连接通道
5 包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

45. 一种基于公共通信网络的数据传输设备, 其特征在于, 应用于业务设备, 所述设备包括: 处理器和存储器;

所述存储器, 用于存储程序指令;

10 所述处理器, 执行所述存储器存储的程序指令, 当程序指令被执行时, 所述处理器用于执行如下步骤:

建立与第一终端之间的第一通信连接通道;

接收所述第一终端通过所述第一通信连接通道发送的加密数据, 并将所述加密数据发送给第二终端;

15 其中, 当所述第一终端为控制设备、且所述第二终端为移动平台时, 所述加密数据包括所述控制设备对所述移动平台的控制数据; 或, 当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时, 所述加密数据包括所述移动平台采集的工作数据。

20 46. 根据权利要求 45 所述的设备, 其特征在于, 所述处理器建立与第一终端之间的第一通信连接通道时, 具体用于:

接收第一终端发送的业务认证信息, 所述业务认证信息是所述第一终端通过第二通信连接通道和登录认证信息从网络服务器中获取到的;

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

25

47. 根据权利要求 46 所述的设备, 其特征在于,

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的; 或,

30 所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

48. 根据权利要求 47 所述的设备, 其特征在于, 所述设备证书包括网络服务器证书和/或终端设备证书, 所述网络服务器证书设置于网络服务器上, 所述终端设备证书设置于所述第一终端上。

5

49. 根据权利要求 46 所述的设备, 其特征在于, 所述第二通信连接通道包括超文本传输安全协议 HTTPS 通道。

50. 根据权利要求 46 所述的设备, 其特征在于,

10 所述登录认证信息携带了所述业务认证信息的获取请求;

其中, 所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证, 并在验证成功之后发送所述业务认证信息给所述第一终端。

15 51. 根据权利要求 50 所述的设备, 其特征在于,

所述登录认证信息是第三终端通过用户中心服务器获取, 并由所述第三终端发送给所述控制设备, 以及由所述控制设备通过私有安全链路同步发送给所述移动平台的;

20 其中, 所述第三终端是所述控制设备, 或者, 所述第三终端是与所述控制设备建立通信连接的设备; 所述第三终端与所述用户中心服务器建立通信连接, 所述用户中心服务器独立于所述网络服务器, 或者, 所述网络服务器包括所述用户中心服务器。

25 52. 根据权利要求 45 所述的设备, 其特征在于, 所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

53. 根据权利要求 45 所述的设备, 其特征在于,

所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的;

30 其中, 当所述第一终端为控制设备、且所述第二终端为移动平台时, 所述

原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

5 54. 根据权利要求 53 所述的设备，其特征在于，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

55. 根据权利要求 53 所述的设备，其特征在于，所述处理器还用于：

10 接收所述第一终端通过所述第一通信连接通道发送的加密密钥，并将所述加密密钥发送给所述第二终端，以使得所述第二终端根据所述加密密钥对所述加密数据进行解密；

所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

56. 根据权利要求 55 所述的设备，其特征在于，

15 所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

57. 根据权利要求 56 所述的设备，其特征在于，

20 所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

58. 根据权利要求 57 所述的设备，其特征在于，

25 所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

59. 根据权利要求 57 所述的设备，其特征在于，

所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

30 所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

60. 一种基于公共通信网络的数据传输设备，其特征在于，应用于第一终端，所述设备包括：处理器和存储器；

所述存储器，用于存储程序指令；

5 所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与业务设备之间的第一通信连接通道；

通过所述第一通信连接通道向业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

10 其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

15 61. 根据权利要求 60 所述的设备，其特征在于，所述处理器建立与业务设备之间的第一通信连接通道时，具体用于：

向业务设备发送业务认证信息，所述业务认证信息是通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

20

62. 根据权利要求 61 所述的设备，其特征在于，

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

25 所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

63. 根据权利要求 62 所述的设备，其特征在于，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，所述终端设备证书设置于所述第一终端上。

30

64. 根据权利要求 61 所述的设备，其特征在于，所述第二通信连接通道包括 HTTPS 通道。

65. 根据权利要求 61 所述的设备，其特征在于，

5 所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

10 66. 根据权利要求 65 所述的设备，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

15 其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括所述用户中心服务器。

20 67. 根据权利要求 60 所述的设备，其特征在于，所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

68. 根据权利要求 60 所述的设备，其特征在于，

所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的；

25 其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

30 69. 根据权利要求 68 所述的设备，其特征在于，所述数据密钥是所述第

一终端根据生成的随机数计算得到的。

70. 根据权利要求 61 所述的设备，其特征在于，所述处理器还用于：

通过所述第二通信连接通道向所述网络服务器发送加密密钥，以使得所述
5 第二终端根据从所述网络服务器获取的所述加密密钥对所述加密数据进行解密；或者，

通过所述第一通信连接通道向所述业务设备发送加密密钥，以使得所述第二终端根据从所述业务设备获取的所述加密密钥对所述加密数据进行解密；

其中，所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

10

71. 根据权利要求 70 所述的设备，其特征在于，

所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

15

72. 根据权利要求 71 所述的设备，其特征在于，

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

73. 根据权利要求 72 所述的设备，其特征在于，

20 所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

74. 根据权利要求 72 所述的设备，其特征在于，

25 所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

75. 一种基于公共通信网络的数据传输设备，其特征在于，应用于网络服
30 务器，所述设备包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与第一终端的第二通信连接通道；

- 5 接收所述第一终端通过所述第二通信连接通道发送的加密密钥，以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密；

其中，当所述第一终端为控制设备、所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为
10 所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

76. 根据权利要求 75 所述的设备，其特征在于，

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验
15 双方的设备证书建立的；或，

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

77. 根据权利要求 76 所述的设备，其特征在于，所述设备证书包括网络
20 服务器证书和/或终端设备证书，所述网络服务器证书设置于所述网络服务器上，所述终端设备证书设置于所述第一终端上。

78. 根据权利要求 76 所述的设备，其特征在于，所述第二通信连接通道
包括 HTTPS 通道。

25

79. 根据权利要求 75 所述的设备，其特征在于，

所述加密密钥是所述第一终端对数据密钥加密得到的，所述加密数据是所述第一终端根据所述数据密钥对待传输的原始数据进行加密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述
30 原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为

移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

80. 根据权利要求 79 所述的设备，其特征在于，

5 所述加密密钥是所述第一终端根据业务密码对数据密钥进行加密得到的。

81. 根据权利要求 80 所述的设备，其特征在于，

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

10

82. 根据权利要求 81 所述的设备，其特征在于，

所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

15

83. 根据权利要求 81 所述的设备，其特征在于，

所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

20

84. 根据权利要求 79 所述的设备，其特征在于，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

85. 根据权利要求 75 所述的设备，其特征在于，所述处理器建立与第一

25 终端的第二通信连接通道之后，还用于：

接收所述第一终端通过所述第二通信连接通道发送的登录认证信息；

将所述登录认证信息对应的业务认证信息给所述第一终端，以使得所述第一终端根据所述业务认证信息建立与业务设备之间的第一通信连接通道；

30 所述加密数据为所述第一终端通过所述第一通信连接通道发送至所述业务设备，并由所述业务设备发送至所述第二终端。

86. 根据权利要求 85 所述的设备，其特征在于，

所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录
5 认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

87. 根据权利要求 86 所述的设备，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终
10 端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制
设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连
接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括
15 所述用户中心服务器。

88. 根据权利要求 85 所述的设备，其特征在于，所述第一通信连接通道
包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

20 89. 一种业务设备，其特征在于，包括：处理器和存储器；

所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所
述处理器用于执行如下步骤：

建立与第一终端之间的第一通信连接通道；

25 接收所述第一终端通过所述第一通信连接通道发送的加密数据，并将所述
加密数据发送给第二终端；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述
加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端
为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述
30 移动平台采集的工作数据。

90. 根据权利要求 89 所述的业务设备, 其特征在于, 所述处理器建立与第一终端之间的第一通信连接通道时, 具体用于:

接收第一终端发送的业务认证信息, 所述业务认证信息是所述第一终端通过第二通信连接通道和登录认证信息从网络服务器中获取到的;

根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

91. 根据权利要求 90 所述的业务设备, 其特征在于,

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的; 或,

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

92. 根据权利要求 91 所述的业务设备, 其特征在于, 所述设备证书包括网络服务器证书和/或终端设备证书, 所述网络服务器证书设置于网络服务器上, 所述终端设备证书设置于所述第一终端上。

93. 根据权利要求 90 所述的业务设备, 其特征在于, 所述第二通信连接通道包括超文本传输安全协议 HTTPS 通道。

94. 根据权利要求 90 所述的业务设备, 其特征在于,

所述登录认证信息携带了所述业务认证信息的获取请求;

其中, 所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证, 并在验证成功之后发送所述业务认证信息给所述第一终端。

95. 根据权利要求 94 所述的业务设备, 其特征在于,

所述登录认证信息是第三终端通过用户中心服务器获取, 并由所述第三终端发送给所述控制设备, 以及由所述控制设备通过私有安全链路同步发送给所述移动平台的;

其中,所述第三终端是所述控制设备,或者,所述第三终端是与所述控制设备建立通信连接的设备;所述第三终端与所述用户中心服务器建立通信连接,所述用户中心服务器独立于所述网络服务器,或者,所述网络服务器包括所述用户中心服务器。

5

96. 根据权利要求 89 所述的业务设备,其特征在于,所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

97. 根据权利要求 89 所述的业务设备,其特征在于,

10 所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的;

其中,当所述第一终端为控制设备、且所述第二终端为移动平台时,所述原始数据为所述控制设备对所述移动平台的控制数据;或,当所述第一终端为移动平台、且所述第二终端为控制设备时,所述原始数据为所述移动平台采集
15 的工作数据。

98. 根据权利要求 97 所述的业务设备,其特征在于,所述数据密钥是所述第一终端根据生成的随机数计算得到的。

20 99. 根据权利要求 97 所述的业务设备,其特征在于,所述处理器还用于:
接收所述第一终端通过所述第一通信连接通道发送的加密密钥,并将所述加密密钥发送给所述第二终端,以使得所述第二终端根据所述加密密钥对所述加密数据进行解密;

所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

25

100. 根据权利要求 99 所述的业务设备,其特征在于,

所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

30 101. 根据权利要求 100 所述的业务设备,其特征在于,

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

102. 根据权利要求 101 所述的业务设备，其特征在于，

5 所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

103. 根据权利要求 101 所述的业务设备，其特征在于，

10 所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

104. 一种终端，其特征在于，包括：处理器和存储器；

15 所述存储器，用于存储程序指令；

所述处理器，执行所述存储器存储的程序指令，当程序指令被执行时，所述处理器用于执行如下步骤：

建立与业务设备之间的第一通信连接通道；

20 通过所述第一通信连接通道向所述业务设备发送加密数据，以使得所述业务设备将所述加密数据发送至第二终端；

其中，当第一终端为控制设备、且所述第二终端为移动平台时，所述加密数据包括所述控制设备对所述移动平台的控制数据；或，当所述第一终端为所述移动平台、且所述第二终端为所述控制设备时，所述加密数据包括所述移动平台采集的工作数据。

25

105. 根据权利要求 104 所述的终端，其特征在于，所述处理器建立与业务设备之间的第一通信连接通道时，具体用于：

向业务设备发送业务认证信息，所述业务认证信息是通过第二通信连接通道和登录认证信息从网络服务器中获取到的；

30 根据所述业务认证信息建立与所述第一终端之间的第一通信连接通道。

106. 根据权利要求 105 所述的终端，其特征在于，

所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的；或，

5 所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

107. 根据权利要求 106 所述的终端，其特征在于，所述设备证书包括网络服务器证书和/或终端设备证书，所述网络服务器证书设置于网络服务器上，
10 所述终端设备证书设置于所述第一终端上。

108. 根据权利要求 105 所述的终端，其特征在于，所述第二通信连接通道包括 HTTPS 通道。

15 109. 根据权利要求 105 所述的终端，其特征在于，

所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

20

110. 根据权利要求 109 所述的终端，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

25 其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括所述用户中心服务器。

30 111. 根据权利要求 104 所述的终端，其特征在于，所述第一通信连接通

道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

112. 根据权利要求 104 所述的终端，其特征在于，

5 所述加密数据是所述第一终端根据数据密钥对待传输的原始数据进行加密得到的；

其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

10

113. 根据权利要求 112 所述的终端，其特征在于，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

114. 根据权利要求 105 所述的终端，其特征在于，所述处理器还用于：

15

通过所述第二通信连接通道向所述网络服务器发送加密密钥，以使得所述第二终端根据从所述网络服务器获取的所述加密密钥对所述加密数据进行解密；或者，

通过所述第一通信连接通道向所述业务设备发送加密密钥，以使得所述第二终端根据从所述业务设备获取的所述加密密钥对所述加密数据进行解密；

20

其中，所述加密密钥是所述第一终端对所述数据密钥进行加密得到的。

115. 根据权利要求 114 所述的终端，其特征在于，

所述加密密钥是所述第一终端根据业务密码对所述数据密钥进行加密得到的。

25

116. 根据权利要求 115 所述的终端，其特征在于，

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

30

117. 根据权利要求 116 所述的终端，其特征在于，

所述根密钥是所述第一终端和所述第二终端中预先设置的,所述第一终端的根密钥与所述第二终端的根密钥相同。

118. 根据权利要求 116 所述的终端, 其特征在于,

5 所述预设类型的数据组是所述第一终端和所述第二终端在对频之后, 根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的;

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

10 119. 一种网络服务器, 其特征在于, 包括: 处理器和存储器;

所述存储器, 用于存储程序指令;

所述处理器, 执行所述存储器存储的程序指令, 当程序指令被执行时, 所述处理器用于执行如下步骤:

建立与第一终端的第二通信连接通道;

15 接收所述第一终端通过所述第二通信连接通道发送的加密密钥, 以使得第二终端根据从所述网络服务器获取的所述加密密钥对所述第一终端发送至所述第二终端的加密数据进行解密;

其中, 当所述第一终端为控制设备、所述第二终端为移动平台时, 所述加密数据包括所述控制设备对所述移动平台的控制数据; 或, 当所述第一终端为
20 所述移动平台、且所述第二终端为所述控制设备时, 所述加密数据包括所述移动平台采集的工作数据。

120. 根据权利要求 119 所述的服务器, 其特征在于,

25 所述第二通信连接通道是所述第一终端和所述网络服务器之间通过校验双方的设备证书建立的; 或,

所述第二通信连接通道是所述第一终端通过校验所述网络服务器的设备证书建立的。

121. 根据权利要求 120 所述的服务器, 其特征在于, 所述设备证书包括
30 网络服务器证书和/或终端设备证书, 所述网络服务器证书设置于所述网络服

务器上，所述终端设备证书设置于所述第一终端上。

122. 根据权利要求 120 所述的服务器，其特征在于，所述第二通信连接通道包括 HTTPS 通道。

5

123. 根据权利要求 119 所述的服务器，其特征在于，

所述加密密钥是所述第一终端对数据密钥加密得到的，所述加密数据是所述第一终端根据所述数据密钥对待传输的原始数据进行加密得到的；

10 其中，当所述第一终端为控制设备、且所述第二终端为移动平台时，所述原始数据为所述控制设备对所述移动平台的控制数据；或，当所述第一终端为移动平台、且所述第二终端为控制设备时，所述原始数据为所述移动平台采集的工作数据。

124. 根据权利要求 123 所述的服务器，其特征在于，

15 所述加密密钥是所述第一终端根据业务密码对数据密钥进行加密得到的。

125. 根据权利要求 124 所述的服务器，其特征在于，

所述业务密钥是所述第一终端根据根密钥和预设类型的数据组经过加密运算得到的。

20

126. 根据权利要求 125 所述的服务器，其特征在于，

所述根密钥是所述第一终端和所述第二终端中预先设置的，所述第一终端的根密钥与所述第二终端的根密钥相同。

25

127. 根据权利要求 125 所述的服务器，其特征在于，

所述预设类型的数据组是所述第一终端和所述第二终端在对频之后，根据通过私有安全链路进行同步处理后的同步随机数和/或验证码生成的；

所述同步随机数包括所述第一终端生成的随机数和/或所述第二终端生成的随机数。

30

128. 根据权利要求 123 所述的服务器，其特征在于，所述数据密钥是所述第一终端根据生成的随机数计算得到的。

129. 根据权利要求 119 所述的服务器，其特征在于，所述处理器建立与
5 第一终端的第二通信连接通道之后，还用于：

接收所述第一终端通过所述第二通信连接通道发送的登录认证信息；

将所述登录认证信息对应的业务认证信息给所述第一终端，以使得所述第一终端根据所述业务认证信息建立与业务设备之间的第一通信连接通道；

所述加密数据为所述第一终端通过所述第一通信连接通道发送至所述业
10 务设备，并由所述业务设备发送至所述第二终端。

130. 根据权利要求 129 所述的服务器，其特征在于，

所述登录认证信息携带了所述业务认证信息的获取请求；

其中，所述业务认证信息的获取请求用于指示所述网络服务器对所述登录
15 认证信息进行验证，并在验证成功之后发送所述业务认证信息给所述第一终端。

131. 根据权利要求 130 所述的服务器，其特征在于，

所述登录认证信息是第三终端通过用户中心服务器获取，并由所述第三终
20 端发送给所述控制设备，以及由所述控制设备通过私有安全链路同步发送给所述移动平台的；

其中，所述第三终端是所述控制设备，或者，所述第三终端是与所述控制设备建立通信连接的设备；所述第三终端与所述用户中心服务器建立通信连接，所述用户中心服务器独立于所述网络服务器，或者，所述网络服务器包括
25 所述用户中心服务器。

132. 根据权利要求 129 所述的服务器，其特征在于，所述第一通信连接通道包括传输控制协议 TCP 通道或用户数据报协议 UDP 通道。

30 133. 一种计算机可读存储介质，所述计算机可读存储介质存储有计算机

程序，其特征在于，所述计算机程序被处理器执行时实现如权利要求 1 至 44 任一项所述方法。

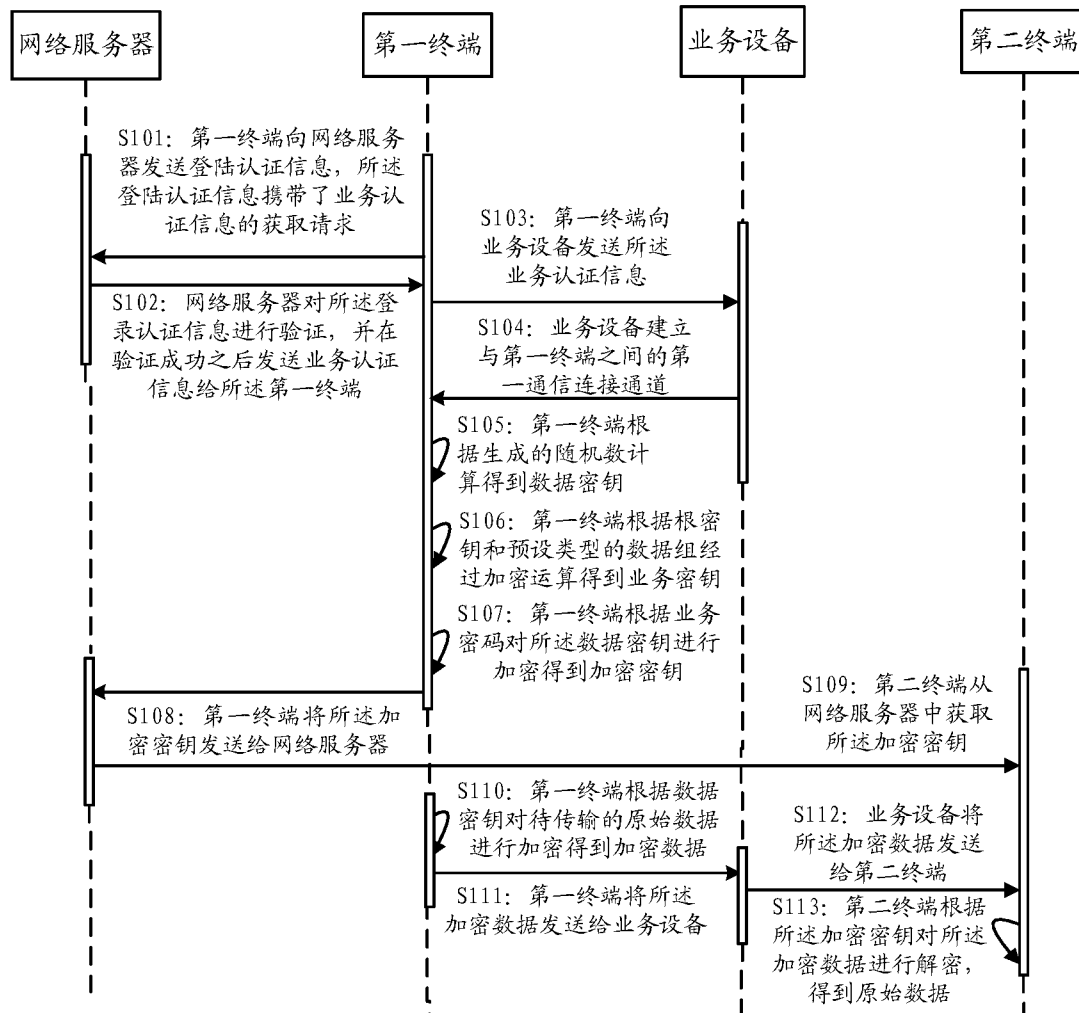


图 1

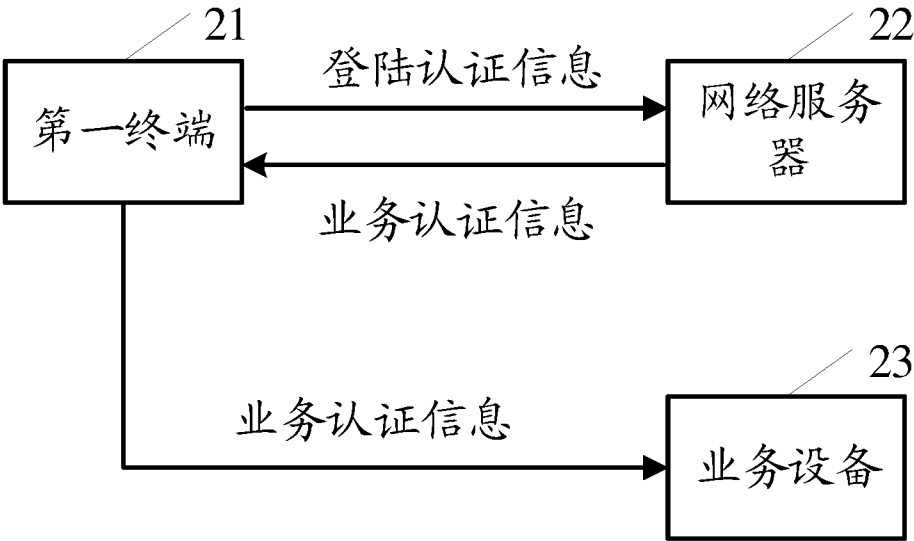


图 2a

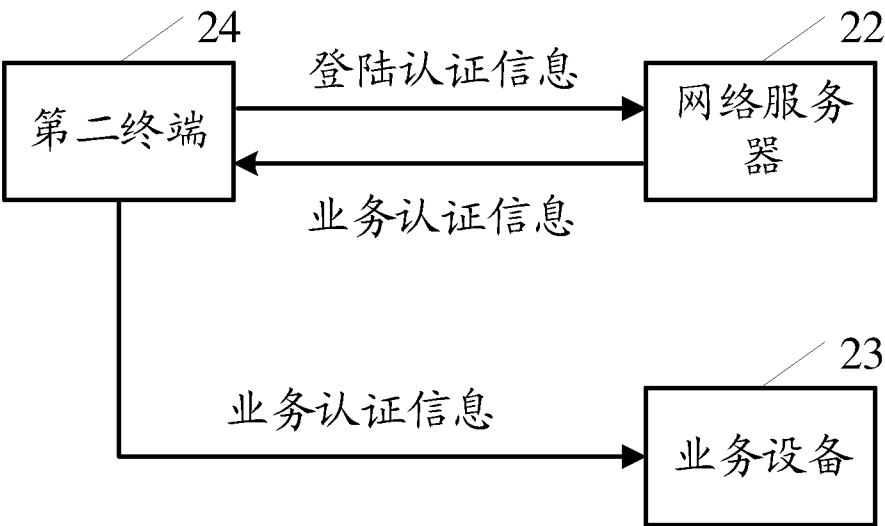


图 2b

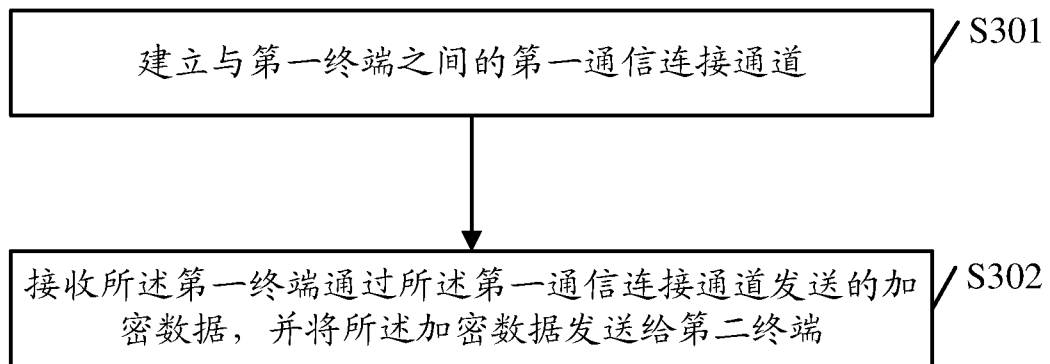


图 3

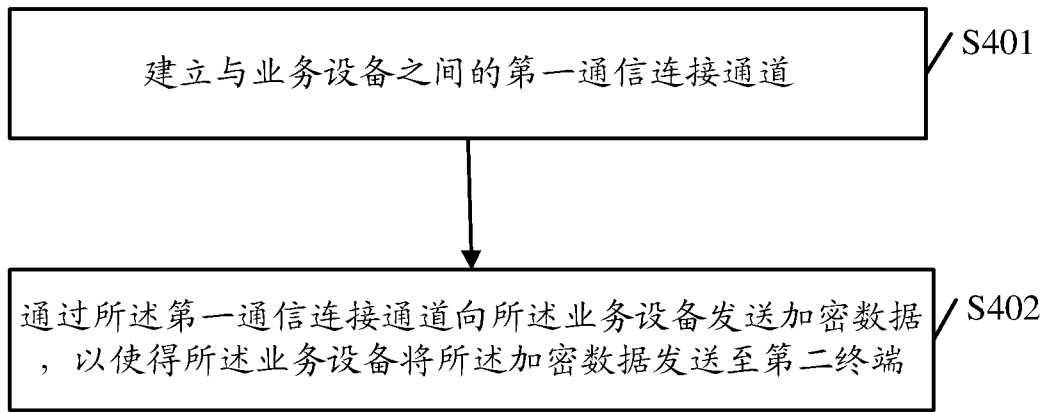


图 4

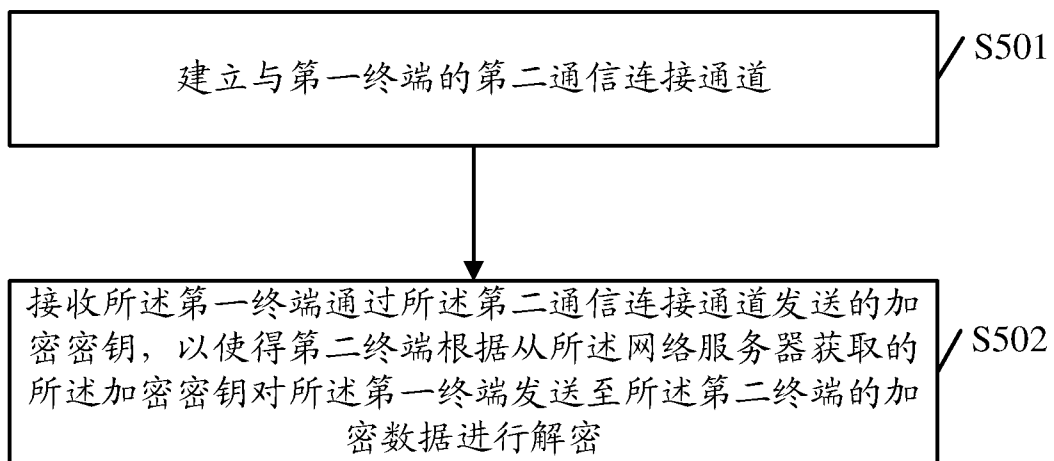


图 5

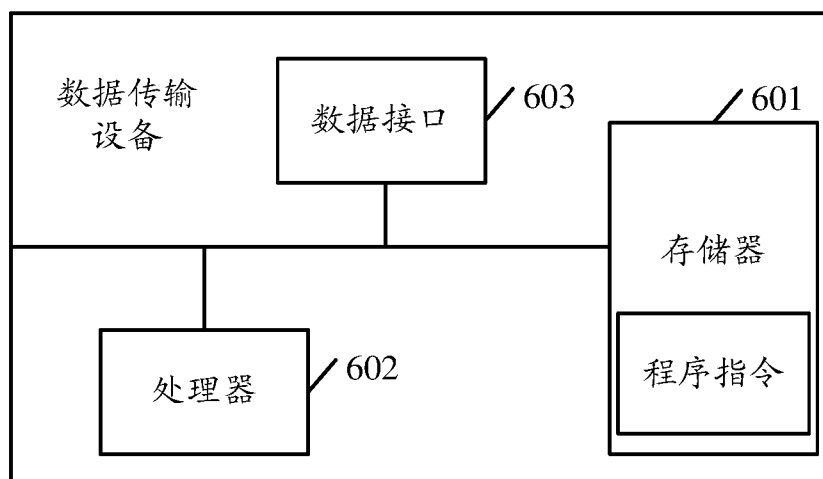


图 6

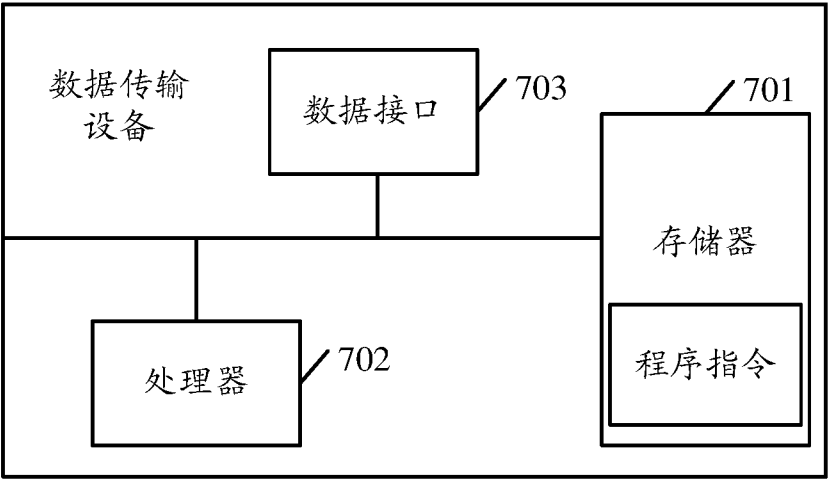


图 7

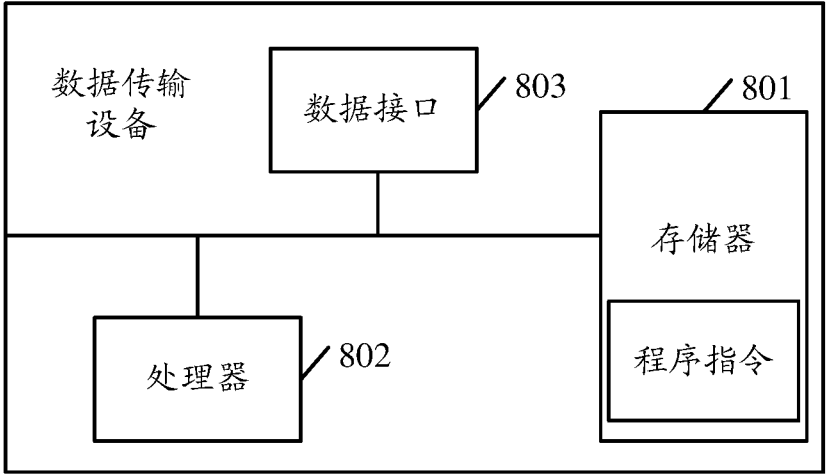


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2018/118784

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/02(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)

H04L; H04W; H04B

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; CNPAT; WPI; EPODOC; IEEE; 加密, 移动, 网络, 链路, 无人机, 备份, 蜂窝, 公共, 备用, 服务器, 认证, 控制, 遥控, encrypt+, mobile, network, link, connect+, unman+ aerial, backup, common, server, authoriz+, control, remote

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 207070091 U (YANG, Zhuo) 02 March 2018 (2018-03-02) description, paragraphs 5-54, and figure 1	1-133
A	CN 106713491 A (EHANG INTELLIGENT EQUIPMENT (GUANGZHOU) CO., LTD.) 24 May 2017 (2017-05-24) entire document	1-133
A	US 2017270314 A1 (ACRONIS INTERNATIONAL GMBH) 21 September 2017 (2017-09-21) entire document	1-133



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“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)

“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

“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

“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

“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

“&” document member of the same patent family

Date of the actual completion of the international search

09 August 2019

Date of mailing of the international search report

27 August 2019

Name and mailing address of the ISA/CN

National Intellectual Property Administration, PRC (ISA/
CN)
No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing
100088
China

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2018/118784

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
CN	207070091	U	02 March 2018	None		
CN	106713491	A	24 May 2017	WO	2018133592	A1
US	2017270314	A1	21 September 2017	None		26 July 2018

国际检索报告

国际申请号

PCT/CN2018/118784

A. 主题的分类

H04L 29/02 (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)

H04L; H04W; H04B

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; CNPAT; WPI; EPDOC; IEEE: 加密, 移动, 网络, 链路, 无人机, 备份, 蜂窝, 公共, 备用, 服务器, 认证, 控制, 遥控, encrypt+, mobile, network, link, connect+, unman+ aerial, backup, common, server, authoriz+, control, remote

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

CN 207070091 U (杨卓) 2018年 3月 2日 (2018 - 03 - 02)
说明书第5-54段、图1

1-133

A

CN 106713491 A (亿航智能设备广州有限公司) 2017年 5月 24日 (2017 - 05 - 24)
全文

1-133

A

US 2017270314 A1 (ACRONIS INTERNATIONAL GMBH) 2017年 9月 21日 (2017 - 09 - 21)
全文

1-133

☐ 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

2019年 8月 9日

国际检索报告邮寄日期

2019年 8月 27日

ISA/CN的名称和邮寄地址

中国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

受权官员

汪德闯

传真号 (86-10)62019451

电话号码 86-(10)-53961791

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/118784

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)
CN	207070091	U	2018年 3月 2日	无	
CN	106713491	A	2017年 5月 24日	W0	2018133592 A1 2018年 7月 26日
US	2017270314	A1	2017年 9月 21日	无	