

(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
2015 年 9 月 11 日 (11.09.2015)



(10) 国际公布号
WO 2015/131689 A1

- (51) 国际专利分类号:
H04L 12/66 (2006.01) *G08C 19/00* (2006.01)
H04L 29/08 (2006.01)
- (21) 国际申请号: PCT/CN2015/071257
- (22) 国际申请日: 2015 年 1 月 21 日 (21.01.2015)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201410476524.8 2014 年 9 月 17 日 (17.09.2014) CN
- (71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。
- (72) 发明人: 赵家伟 (ZHAO, Jiawei); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦,

Guangdong 518057 (CN)。 陈建林 (CHEN, Jianlin); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS, P. C.); 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 16 层, Beijing 100098 (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, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, 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。

[见续页]

(54) Title: SENSOR CODE-PAIRING PROCESSING METHOD, APPARATUS, NETWORK PLATFORM DEVICE, AND INTERNET OF THINGS GATEWAY

(54) 发明名称: 传感器对码处理方法、装置、网络平台设备及物联网网关

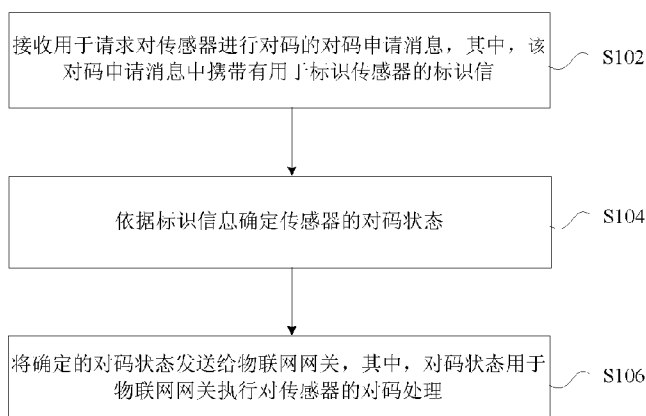


图 1 / FIG. 1

S102 RECEIVE A CODE-PAIRING APPLICATION MESSAGE FOR REQUESTING CODE-PAIRING TO BE CARRIED OUT IN RESPECT OF A SENSOR, WHEREIN THE CODE-PAIRING APPLICATION MESSAGE CARRIES MARKER INFORMATION FOR MARKING THE SENSOR

S104 ON THE BASIS OF SAID MARKER INFORMATION, DETERMINE THE CODE-PAIRING STATUS OF THE SENSOR

S106 SEND THE DETERMINED CODE-PAIRING STATUS TO AN INTERNET OF THINGS GATEWAY, WHEREIN THE CODE-PAIRING STATUS IS USED BY SAID GATEWAY TO EXECUTE CODE-PAIRING PROCESSING IN RESPECT OF THE SENSOR

(57) Abstract: A sensor code-pairing processing method, apparatus, network platform device, and an internet of things gateway are disclosed in the present invention. The method comprises: receiving a code-pairing application message requesting code-pairing to be carried out in respect of a sensor, wherein the code-pairing application message carries marker information for marking the sensor; on the basis of said marker information, determining the code-pairing status of the sensor; and sending the determined code-pairing status to an internet of things gateway, wherein the code-pairing status is used by said gateway to execute code-pairing processing in respect of the sensor. The present invention solves the problem in the art of hidden security dangers in the sensor code-pairing process potentially being exploited by illegal hackers. Thus, the invention improves the effects of sensor access security.

(57) 摘要: 本发明公开了一种传感器对码处理方法、装置、网络平台设备及物联网网关，其中，该方法包括：接收用于请求对传感器进行对码的对码申请消息，其中，对码申请消息中携带有用于标识传感器的标识信息；依据标识信息确定传感器的对码状态；将确定的对码状态发送给物联网网关，其中，对码状态用于物联网网关执行对传感器的对码处理，通过本发明，解决了相关技术中由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题，进而达到了有效提高传感器接入安全性的效果。



(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))。
- 在修改权利要求的期限届满之前进行, 在收到该修改后将重新公布(细则 48.2(h))。
- 根据申请人的请求, 在条约第 21 条(2)(a)所规定的期限届满之前进行。

传感器对码处理方法、装置、网络平台设备及物联网网关

技术领域

本发明涉及通信领域，具体而言，涉及一种传感器对码处理方法、装置、网络平台设备及物联网网关。

5 背景技术

物联网是新一代信息技术的重要组成部分，它利用局域网或互联网等通信技术把传感器、控制器、机器、人员和物等通过新的方式联在一起，形成人与物、物与物相联，实现信息化、远程管理控制和智能化的网络。

10 物联网网关和传感器是物联网系统中的重要组成部分，其中物联网网关是连接传感器和互联网的中枢，它后端管理和控制诸多传感器，前端连接因特网。物联网网关在转发传感器数据前，必须完成物联网网关和传感器之间的“对码”过程。所谓“对码”，是指传感器和物联网网关之间通过某种协议，互相交换对方的设备标识信息，达到双方互相认知的目的。也就是，物联网网关通过“对码”方式完成了传感器接入控制和管理。

15 在相关技术中，传感器和物联网网关根据其 RF 方案的不同，对码方式包括单向对码和双向对码。其中双向对码是指物联网网关和传感器支持双向通讯，两者之间可以互相交换设备信息，互相完成对方的识别和认证。对码完成后，传感器设备里会保留已对码的物联网网关标识，物联网网关里会保留已对码的传感器的设备标识，后续的数据交互都基于设备标识互相寻址。

20 目前，双向对码的触发方式又分两种，第一种由传感器主动触发，第二种由物联网网关触发。物联网网关触发对码的基本原理是，物联网网关根据传感器的标识 ID 向特定传感器发送传感器唤醒消息，该传感器被唤醒后，物联网网关和传感器之间按协议交互顺序，互发对码消息和对码确认消息，对码消息中携带各自的设备标识信息，最后双方完成对方设备标识信息的识别和存储。特别对于第二种对码触发方式，存在
25 一定的安全隐患。例如，非法入侵者在获知用户的传感器标识 ID 后，可以在用户传感器附近搭建一个非法物联网网关，因为物联网网关和传感器对码过程的消息定义非标准，通常非法入侵者控制的物联网网关和用户的物联网网关版本相同，通过该物联网网关向已知标识 ID 的传感器触发双向对码流程，从而使用户的传感器脱离合法传感器的管理，接入到非法物联网网关，导致传感器数据的丢失。

因此，在相关技术中由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题。

发明内容

5 本发明提供了一种传感器对码处理方法、装置、网络平台设备及物联网网关，以至少解决相关技术中由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题。

10 根据本发明的一个方面，提供了一种传感器对码处理方法，包括：接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；依据所述标识信息确定所述传感器的对码状态；将确定的所述对码状态发送给物联网网关，其中，所述对码状态用于所述物联网网关执行对所述传感器的对码处理。

优选地，接收用于请求对所述传感器进行对码的所述对码申请消息包括以下至少之一：接收来自物联网网关的所述对码申请消息；接收来自移动终端应用 APP 的所述对码申请消息。

15 优选地，所述传感器的标识信息包括以下至少之一：所述传感器的唯一标识码 ID、所述传感器的类型、所述传感器的工作方式。

20 根据本发明的另一方面，提供了一种传感器对码处理方法，包括：接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；将所述对码申请消息发送给网络平台设备；接收所述网络平台设备依据所述标识信息确定的所述传感器的对码状态；依据确定的所述对码状态执行对所述传感器的对码处理。

25 优选地，依据确定的所述对码状态执行对所述传感器的对码处理包括：在所述对码状态为所述传感器已经对码或禁止对码的情况下，禁止对所述传感器执行对码处理；和/或，在所述对码状态为所述传感器未对码或允许对码的情况下，触发对所述传感器执行对码处理。

根据本发明的还一方面，提供了一种传感器对码处理装置，包括：第一接收模块，设置为接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；确定模块，设置为依据所述标识信息确

定所述传感器的对码状态；发送模块，设置为将确定的所述对码状态发送给物联网网关，其中，所述对码状态用于所述物联网网关执行对所述传感器的对码处理。

5 优选地，所述接收模块包括以下至少之一：第一接收单元，设置为接收来自物联网网关的所述对码申请消息；第二接收单元，设置为接收来自移动终端应用 APP 的所述对码申请消息。

根据本发明的再一方面，提供了一种网络平台设备，包括上述任一项所述的装置。

10 根据本发明的还一方面，提供了一种传感器对码处理装置，包括：第二接收模块，设置为接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；第一发送模块，设置为将所述对码申请消息发送给网络平台设备；第三接收模块，设置为接收所述网络平台设备依据所述标识信息确定的所述传感器的对码状态；处理模块，设置为依据确定的所述对码状态执行对所述传感器的对码处理。

15 优选地，所述处理模块包括：第一处理单元，设置为在所述对码状态为所述传感器已经对码或禁止对码的情况下，禁止对所述传感器执行对码处理；第二处理单元，设置为在所述对码状态为所述传感器未对码或允许对码的情况下，触发对所述传感器执行对码处理。

根据本发明的再一方面，提供了一种物联网网关，包括上述任一项所述的装置。

20 通过本发明，采用接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；依据所述标识信息确定所述传感器的对码状态；将确定的所述对码状态发送给物联网网关，其中，所述对码状态用于所述物联网网关执行对所述传感器的对码处理，解决了相关技术中由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题，进而达到了有效提高传感器接入安全性的效果。

附图说明

25 此处所说明的附图用来提供对本发明的进一步理解，构成本申请的一部分，本发明的示意性实施例及其说明用于解释本发明，并不构成对本发明的不当限定。在附图中：

图 1 是根据本发明实施例的传感器对码处理方法一的流程图；

图 2 是根据本发明实施例的传感器对码处理方法二的流程图；

图 3 是根据本发明实施例的传感器对码处理装置一的结构框图；

图 4 是根据本发明实施例的传感器对码处理装置一中第一接收模块 32 的优选结构框图；

5 图 5 是根据本发明实施例的网络平台设备的结构框图；

图 6 是根据本发明实施例的传感器对码处理装置二的结构框图；

图 7 是根据本发明实施例的传感器对码处理装置二中处理模块 68 的优选结构框图；

图 8 是根据本发明实施例的物联网网关的结构框图；

10 图 9 是根据本发明优选实施方式的组网架构示意图；

图 10 是根据本发明实施例的传感器控制方法流程图；

图 11 是根据本发明实施方式的网络平台设备的结构示意图；

图 12 是根据本发明优选实施方式的物联网网关的结构示意图。

具体实施方式

15 下文中将参考附图并结合实施例来详细说明本发明。需要说明的是，在不冲突的情况下，本申请中的实施例及实施例中的特征可以相互组合。

在本实施例中提供了一种传感器对码处理方法，图 1 是根据本发明实施例的传感器对码处理方法一的流程图，如图 1 所示，该流程包括如下步骤：

20 步骤 S102，接收用于请求对传感器进行对码的对码申请消息，其中，该对码申请消息中携带有用于标识传感器的标识信；

步骤 S104，依据标识信息确定传感器的对码状态；

步骤 S106，将确定的对码状态发送给物联网网关，其中，对码状态用于物联网网关执行对传感器的对码处理。

通过上述步骤，依据传感器的标识信息确定传感器的对码状态，依据对码状态执行对码处理，相对于相关技术中直接由物联网网关执行对码处理，如果存在非法入侵者，则导致安全隐患的问题，不仅有效地解决了由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题，进而达到了有效提高传感器接入安全性的效果。

5 接收用于请求对传感器进行对码的对码申请消息可以采用多种方式，即对码申请的来源可以多种，例如，可以包括以下至少之一：接收来自物联网网关的对码申请消息；接收来自移动终端应用 APP 的对码申请消息。其中，上述传感器的标识信息也可以包括多种，例如，可以包括以下至少之一：传感器的唯一标识码 ID、传感器的类型、传感器的工作方式。

10 图 2 是根据本发明实施例的传感器对码处理方法二的流程图，如图 2 所示，该流程包括如下步骤：

步骤 S202，接收用于请求对传感器进行对码的对码申请消息，其中，对码申请消息中携带有用于标识传感器的标识信息；

步骤 S204，将对码申请消息发送给网络平台设备；

15 步骤 S206，接收网络平台设备依据标识信息确定的传感器的对码状态；

步骤 S208，依据确定的对码状态执行对传感器的对码处理。

通过上述步骤，依据传感器的标识信息确定传感器的对码状态，依据对码状态执行对码处理，相对于相关技术中直接由物联网网关执行对码处理，如果存在非法入侵者，则导致安全隐患的问题，不仅有效地解决了由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题，进而达到了有效提高传感器接入安全性的效果。

20

依据确定的对码状态执行对传感器的对码处理时，可以包括以下处理：在对码状态为传感器已经对码或禁止对码的情况下，禁止对传感器执行对码处理；和/或，在对码状态为传感器未对码或允许对码的情况下，触发对传感器执行对码处理。

在本实施例中还提供了一种传感器对码处理装置，该装置用于实现上述实施例及
25 优选实施方式，已经进行过说明的不再赘述。如以下所使用的，术语“模块”可以实现预定功能的软件和/或硬件的组合。尽管以下实施例所描述的装置较佳地以软件来实现，但是硬件，或者软件和硬件的组合的实现也是可能并被构想的。

图 3 是根据本发明实施例的传感器对码处理装置一的结构框图，如图 3 所示，该装置包括第一接收模块 32、确定模块 34 和发送模块 36，下面对该装置进行说明。

第一接收模块 32，设置为接收用于请求对传感器进行对码的对码申请消息，其中，对码申请消息中携带有用于标识传感器的标识信息；确定模块 34，连接至上述第一接收模块 32，设置为依据标识信息确定传感器的对码状态；发送模块 36，连接至上述确定模块 34，设置为将确定的对码状态发送给物联网网关，其中，对码状态用于物联网网关执行对传感器的对码处理。

图 4 是根据本发明实施例的传感器对码处理装置一中第一接收模块 32 的优选结构框图，如图 4 所示，该第一接收模块 32 包括以下至少之一：第一接收单元 42、第二接收单元 44，下面对该第一接收模块 32 进行说明。

第一接收单元 42，设置为接收来自物联网网关的对码申请消息；第二接收单元 44，设置为接收来自移动终端应用 APP 的对码申请消息。

图 5 是根据本发明实施例的网络平台设备的结构框图，如图 5 所示，该网络平台设备 50 包括上述任一项的传感器对码处理装置一 52。

图 6 是根据本发明实施例的传感器对码处理装置二的结构框图，如图 6 所示，该装置包括：第二接收模块 62、第一发送模块 64、第三接收模块 66 和处理模块 68，下面对该装置进行说明。

第二接收模块 62，设置为接收用于请求对传感器进行对码的对码申请消息，其中，对码申请消息中携带有用于标识传感器的标识信息；第一发送模块 64，连接至上述第二接收模块 62，设置为将对码申请消息发送给网络平台设备；第三接收模块 66，连接至上述第一发送模块 64，设置为接收网络平台设备依据标识信息确定的传感器的对码状态；处理模块 68，连接至上述第三接收模块 66，设置为依据确定的对码状态执行对传感器的对码处理。

图 7 是根据本发明实施例的传感器对码处理装置二中处理模块 68 的优选结构框图，如图 7 所示，该处理模块 68 包括第一处理单元 72 和/或第二处理单元 74，下面对该处理模块 68 进行说明。

第一处理单元 72，设置为在对码状态为传感器已经对码或禁止对码的情况下，禁止对传感器执行对码处理；第二处理单元 74，设置为在对码状态为传感器未对码或允许对码的情况下，触发对传感器执行对码处理。

图 8 是根据本发明实施例的物联网网关的结构框图，如图 8 所示，该物联网网关 80 包括上述任一项的传感器对码处理装置二 82。

针对相关技术中，传感器双向对码存在的安全隐患，在本实施例中，提供了一种传感器控制方案，基于非法入侵者未侵入物联网的网络平台前提下，在双向对码过程
5 实际执行前，通过网络平台实现传感器对码状态识别，从而实现对传感器接入的安全控制。通过上述方案，可以有效提高传感器接入安全性。

基于传感器和物联网网关之间的双向对码存在安全隐患，特别是物联网网关的双向对码触发方式。该对码方案包括如下处理：网络平台设备接收传感器对码申请消息；网络平台设备依据传感器标识信息确定出传感器对码状态；网络平台设备根据传感器
10 对码状态信息，发送传感器对码控制消息。

其中，该传感器标识信息和对应的传感器对码状态信息存储在网络平台设备中；传感器对码状态信息至少记录传感器最新对码结果，包括已对码或未对码；其中，网络平台接收的传感器对码申请消息，来自于发起对码申请的外部网络设备，外部网络设备包括但不限于物联网网关、移动智能终端 APP、其他第三方通讯设备及软件。

15 其中，传感器对码申请消息包括至少一个传感器标识信息，传感器标识信息包括但不限于传感器标识 ID、传感器类型、传感器工作方式等。

对码控制消息内容根据对码状态生成，其消息内容包括但不限于传感器对码状态、是否允许传感器对码。

20 外部网络设备接收到传感器对码控制消息后，解析消息内容，根据传感器对码状态或是否允许传感器对码信息，控制传感器对码的触发。一般，如果传感器对码状态为已经对码（或禁止对码），则不触发传感器对码；如果传感器对码状态为未对码（或允许对码），则触发传感器对码。

下面结合附图对本发明优选实施方式进行说明。

25 在该实施例中，传感器对码申请消息发起者是物联网网关，但由智能手机 APP 控制物联网网关发起该传感器对码功能。在对对码处理之前：智能手机开启 Wi-Fi 模块，默认连接到用户家里的无线路由器设备，物联网网关通过 Wi-Fi 或有线连接方式也连接到该无线路由器设备。智能手机 APP 应用中提供传感器对码功能，用户通过在 APP 上手动输入待对码的传感器标识 ID 信息（通常标识 ID 为固定长度的数字和字符混合的字符串，例如“S0134001001002”），或通过 APP 自带的二维码扫描工具，自动扫描

传感器标识 ID 对应的二维码信息，APP 获取到传感器标识 ID 后，通过自定义封装的 HTTP 协议向物联网网关触发对码命令，物联网网关收到对码命令后，解析出待对码的传感器标识 ID，再封装出传感器对码申请消息，对码申请消息中包含该传感器标识 ID，然后通过 TCP/IP 协议，发送到网络平台设备。其中，物联网网关可以通过域名查询获取到对应的网络平台设备 IP 地址，通过自定义协议传送对码申请消息。

图 9 是根据本发明优选实施方式的组网架构示意图，如图 9 所示，该网络架构包括网络平台设备 92、物联网网关 94、智能手机 APP96，以及一个或多个传感器。

图 10 是根据本发明实施例的传感器控制方法流程图，如图 10 所示，该流程包括如下步骤：

10 步骤 S1002，网络平台设备接收传感器对码申请消息，在本实施例中，网络平台设备接收到物联网网关发送的传感器对码申请消息。

步骤 S1004，网络平台设备依据传感器标识信息确定出传感器对码状态。本实施例中，网络平台设备通过协议解析，获取到该传感器的标识 ID 信息，通过软件查询存储模块，获取到该传感器对应的对码状态为“已经对码”，从而完成对码状态的确认。

15 网络平台设备需要存储传感器的对码状态信息，存储的方式是在传感器对码环节完成并确认后，新增或更新对码状态。存储通常采用数据库技术。本实施方法中，该传感器在网络平台里存储的对码状态是“已经对码”，表明该传感器在此次对码之前，已完成过至少一次对码过程且对码成功，处于服务状态。

20 步骤 S1006，网络平台根据传感器对码状态信息，发送传感器对码控制消息；在本实施例中，传感器对码状态是“已经对码”，根据该对码状态信息，网络平台设备生成对码控制消息，传感器对码控制消息字段包括传感器标识 ID、对码状态=“已经对码”，是否允许对码=“否”；之后，网络平台设备通过 TCP/IP 自定义协议向物联网网关发送该传感器的对码控制消息。

25 物联网网关接收到该传感器的对码控制消息后，解析对码控制消息，判断是否允许对码字段为“否”后，不会触发与传感器的双向对码过程。且通过自定义 HTTP 接口向智能手机 APP 发送该传感器的对码结果，本实施例中的对码结果是“该传感器已经对码，请先解绑后再进行对码”。

在本实施例中，如果网络平台设备中存储的传感器对码状态是“未对码”或没有该传感器的对码记录，则网络平台设备生成对码控制消息字段包括传感器标识 ID、对

码状态=“未对码”，是否允许对码=“是”；之后，网络平台设备通过 TCP/IP 自定义协议向物联网网关发送该传感器的对码控制消息。

物联网网关接收到该传感器的对码控制消息后，解析对码控制消息，判断是否允许对码字段为“是”后，主动触发与传感器的双向对码过程，包括传感器的唤醒、标识 ID 的交互和识别。最后，物联网网关通过自定义 HTTP 接口向智能手机 APP 发送该传感器的对码结果为“该传感器已成功对码”。同时，物联网网关将“成功对码”的消息发送给网络设备平台，网络设备平台更新该传感器的对码状态为“已经对码”。

通过上述处理，网络平台设备在不改变硬件的前提下，软件上增加如下功能。图 11 是根据本发明实施方式的网络平台设备的结构示意图，如图 11 所示，该网络平台设备 110 包括存储模块 112、第一消息接收模块 114（功能相当于上述第一接收模块 32）、状态查询模块 116（功能同上述确定模块 34）和第一消息发送模块 118（功能同上述发送模块 36），下面对该网络平台设备 110 进行说明。

存储模块 112，设置为存储传感器最新的对码状态和相应的传感器标识信息。在本实施例中，存储模块采用数据库技术，通过表方式存储传感器 ID 和对码状态信息，本传感器存储的对码状态信息是“已经对码”。

第一消息接收模块 114，接收传感器对码申请消息；本实施例中，网络平台设备通过 TCP/IP 技术接收到物联网网关的传感器对码申请消息。

状态查询模块 116，根据传感器标识信息查询传感器最新对码状态；网络网关设备解析传感器对码申请消息，获取到传感器的标识 ID，并调用存储模块，确认该传感器的当前对码状态是“已经对码”。

第一消息发送模块 118，根据状态查询模块产生的传感器对码状态信息，生成传感器对码控制消息，并发送给发起对码申请的外部网络设备。本实施例中，传感器对码状态是“已经对码”，根据该对码状态信息，网络平台设备生成对码控制消息，传感器对码控制消息字段包括传感器标识 ID、对码状态=“已经对码”，是否允许对码=“否”；之后，网络平台设备通过 TCP/IP 自定义协议向物联网网关发送该传感器的对码控制消息。

根据上述实施例提供的方法，物联网网关在不改变硬件的前提下，软件上增加：图 12 是根据本发明优选实施方式的物联网网关的结构示意图，如图 12 所示，该物联网网关 120 包括第二消息发送模块 122（功能同上述第一发送模块 64）、第二消息接收

模块 124（功能同上述第三接收模块 66）和对码触发模块 126，下面对该装置进行说明。

第二消息发送模块 122，向网络平台发送传感器对码申请消息；在此实施例中，物联网网关收到智能手机 APP 的对码命令后，解析出待对码的传感器标识 ID，再封装出传感器对码申请消息，对码申请消息中包含该传感器标识 ID，然后通过 TCP/IP 协议，发送到网络平台设备。

第二消息接收模块 124，接收来自网络平台发送的传感器对码控制消息；在此实施例中，物联网网关接收该传感器的对码控制消息。

对码触发模块 126，根据传感器对码控制消息，解析消息内容，根据传感器对码状态或是否允许传感器对码信息，控制传感器对码的触发。一般，如果传感器对码状态为已经对码（或禁止对码），则不触发传感器对码；如果传感器对码状态为未对码（或允许对码），则触发传感器对码。在此实施例中，因为是否允许对码为“否”，不会触发与传感器的双向对码过程。之后，通过自定义 HTTP 接口向智能手机 APP 发送该传感器的对码结果，“该传感器已经对码，请先解绑后再进行对码”。

显然，本领域的技术人员应该明白，上述的本发明的各模块或各步骤可以用通用的计算装置来实现，它们可以集中在单个的计算装置上，或者分布在多个计算装置所组成的网络上，可选地，它们可以用计算装置可执行的程序代码来实现，从而，可以将它们存储在存储装置中由计算装置来执行，并且在某些情况下，可以以不同于此处的顺序执行所示出或描述的步骤，或者将它们分别制作成各个集成电路模块，或者将它们中的多个模块或步骤制作成单个集成电路模块来实现。这样，本发明不限制于任何特定的硬件和软件结合。

以上仅为本发明的优选实施例而已，并不用于限制本发明，对于本领域的技术人员来说，本发明可以有各种更改和变化。凡在本发明的精神和原则之内，所作的任何修改、等同替换、改进等，均应包含在本发明的保护范围之内。

25 工业实用性

通过上述实施例及优选实施方式，解决了相关技术中由于存在非法入侵者，导致在传感器对码过程中存在安全隐患的问题，进而达到了有效提高传感器接入安全性的效果。

权 利 要 求 书

1. 一种传感器对码处理方法，包括：

接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；

依据所述标识信息确定所述传感器的对码状态；

将确定的所述对码状态发送给物联网网关，其中，所述对码状态用于所述物联网网关执行对所述传感器的对码处理。
2. 根据权利要求 1 所述的方法，其中，接收用于请求对所述传感器进行对码的所述对码申请消息包括以下至少之一：

接收来自物联网网关的所述对码申请消息；

接收来自移动终端应用 APP 的所述对码申请消息。
3. 根据权利要求 1 所述的方法，其中，所述传感器的标识信息包括以下至少之一：

所述传感器的唯一标识码 ID、所述传感器的类型、所述传感器的工作方式。
4. 一种传感器对码处理方法，包括：

接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；

将所述对码申请消息发送给网络平台设备；

接收所述网络平台设备依据所述标识信息确定的所述传感器的对码状态；

依据确定的所述对码状态执行对所述传感器的对码处理。
5. 根据权利要求 4 所述的方法，其中，依据确定的所述对码状态执行对所述传感器的对码处理包括：

在所述对码状态为所述传感器已经对码或禁止对码的情况下，禁止对所述传感器执行对码处理；和/或，

在所述对码状态为所述传感器未对码或允许对码的情况下，触发对所述传感器执行对码处理。
6. 一种传感器对码处理装置，包括：

第一接收模块，设置为接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；

确定模块，设置为依据所述标识信息确定所述传感器的对码状态；

发送模块，设置为将确定的所述对码状态发送给物联网网关，其中，所述对码状态用于所述物联网网关执行对所述传感器的对码处理。

7. 根据权利要求 6 所述的装置，其中，所述接收模块包括以下至少之一：

第一接收单元，设置为接收来自物联网网关的所述对码申请消息；

第二接收单元，设置为接收来自移动终端应用 APP 的所述对码申请消息。

8. 一种网络平台设备，包括权利要求 6 至 7 中任一项所述的装置。

9. 一种传感器对码处理装置，包括：

第二接收模块，设置为接收用于请求对所述传感器进行对码的对码申请消息，其中，所述对码申请消息中携带有用于标识所述传感器的标识信息；

第一发送模块，设置为将所述对码申请消息发送给网络平台设备；

第三接收模块，设置为接收所述网络平台设备依据所述标识信息确定的所述传感器的对码状态；

处理模块，设置为依据确定的所述对码状态执行对所述传感器的对码处理。

10. 根据权利要求 9 所述的装置，其中，所述处理模块包括：

第一处理单元，设置为在所述对码状态为所述传感器已经对码或禁止对码的情况下，禁止对所述传感器执行对码处理；

第二处理单元，设置为在所述对码状态为所述传感器未对码或允许对码的情况下，触发对所述传感器执行对码处理。

11. 一种物联网网关，包括权利要求 9 至 10 中任一项所述的装置。

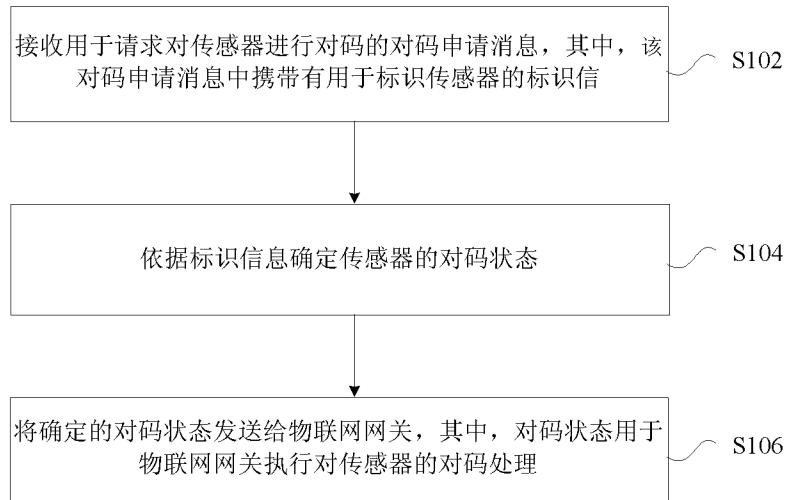


图 1

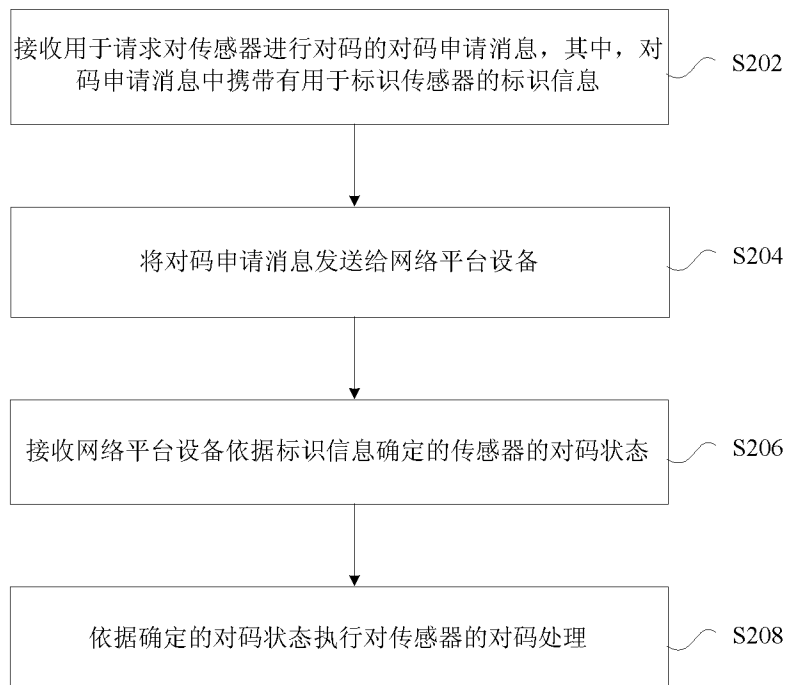


图 2



图 3



图 4

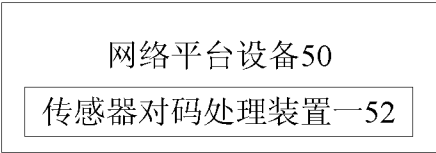


图 5



图 6



图 7

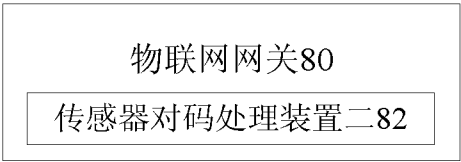


图 8

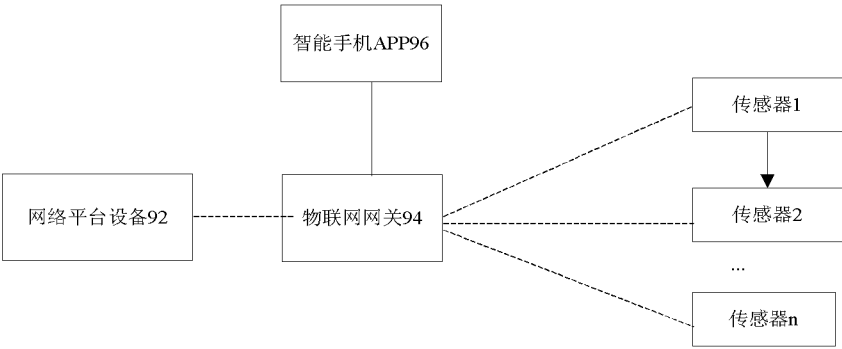


图 9

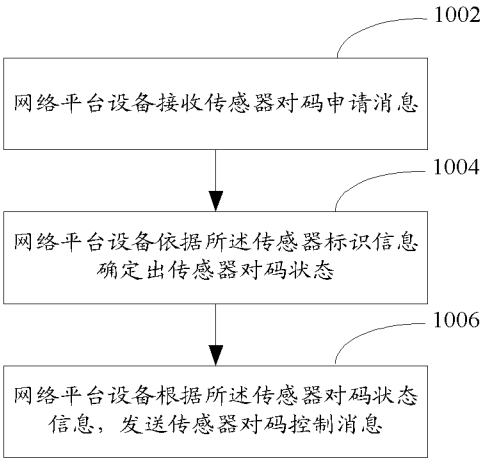


图 10

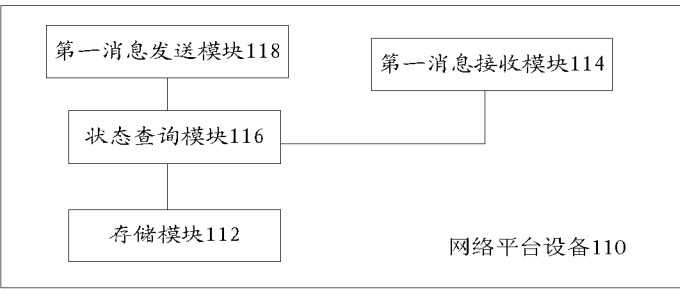


图 11

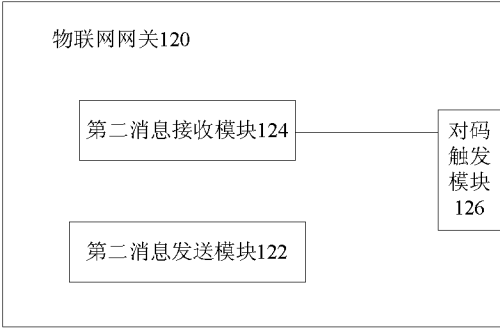


图 12

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2015/071257**A. CLASSIFICATION OF SUBJECT MATTER**

H04L 12/66 (2006.01) i; H04L 29/08 (2006.01) i; G08C 19/00 (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)

H04L; H04W; G08C

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)

CNTXT, CNABS, VEN, CNKI: match code, state, security, code, match+, cod+, sensor?, gateway, identif+, recogni+, distinguish+, ID, fake, forge?, illegal, internet of things, associat+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 103118046 A (CHINA MOBILE COMMUNICATIONS CORPORATION), 22 May 2013 (22.05.2013), see the whole document	1-11
A	CN 103139083 A (ALCATEL-LUCENT SHANGHAI BELL CO., LTD.), 05 June 2013 (05.06.2013), see the whole document	1-11
A	CN 102231739 A (NANJING ZHONGXING NEW SOFTWARE COMPANY LIMITED), 02 November 2011 (02.11.2011), see the whole document	1-11
A	WO 2011025358 A1 (MIMOS, B. et al.), 03 March 2011 (03.03.2011), see the whole document	1-11

☐ 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 19 May 2015 (19.05.2015)	Date of mailing of the international search report 23 June 2015 (23.06.2015)
Name and mailing address of the ISA/CN: 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 ZOU, Ting Telephone No.: (86-10) 62089393

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2015/071257

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103118046 A	22 May 2013	None	
CN 103139083 A	05 June 2013	TW 201330679 A	16 July 2013
		TW I466576 B	21 December 2014
		WO 2013080034 A2	06 June 2013
		WO 2013080034 A3	08 August 2013
CN 102231739 A	02 November 2011	WO 2012175032 A1	27 December 2012
WO 2011025358 A1	03 March 2011	None	

国际检索报告

国际申请号

PCT/CN2015/071257

A. 主题的分类

H04L 12/66(2006.01)i; H04L 29/08(2006.01)i; G08C 19/00(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)

H04L; H04W; G08C

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))

CNTXT;CNABS;VEN;CNKI: 对码, 码, 传感器, 网关, 标识, 状态, 安全, 伪装, 假冒, 非法, 物联网, 关联, code, match+, cod+, sensor?, gateway, identifi+, recogni+, distinguish+, ID, fake, forge?, illegal, internet of things, associat+

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
A	CN 103118046 A (中国移动通信集团公司) 2013年 5月 22日 (2013 - 05 - 22) 参见全文	1-11
A	CN 103139083 A (上海贝尔股份有限公司) 2013年 6月 5日 (2013 - 06 - 05) 参见全文	1-11
A	CN 102231739 A (南京中兴新软件有限责任公司) 2011年 11月 2日 (2011 - 11 - 02) 参见全文	1-11
A	WO 2011025358 A1 (MIMOS BERHAD, ET AL.) 2011年 3月 3日 (2011 - 03 - 03) 参见全文	1-11

☐ 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

2015年 5月 19日

国际检索报告邮寄日期

2015年 6月 23日

ISA/CN的名称和邮寄地址

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

传真号 (86-10)62019451

授权官员

邹婷

电话号码 (86-10)62089393

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2015/071257

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	103118046	A	2013年 5月 22日	无			
CN	103139083	A	2013年 6月 5日	TW	201330679	A	2013年 7月 16日
				TW	I466576	B	2014年 12月 21日
				WO	2013080034	A2	2013年 6月 6日
				WO	2013080034	A3	2013年 8月 8日
CN	102231739	A	2011年 11月 2日	WO	2012175032	A1	2012年 12月 27日
WO	2011025358	A1	2011年 3月 3日	无			

表 PCT/ISA/210 (同族专利附件) (2009年7月)