(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
2021 年 6 月 17 日 (17.06.2021)

WIPO | PCT

(10) 国际公布号
WO 2021/114700 A1

(51) 国际专利分类号:
G08B 13/24 (2006.01)

(21) 国际申请号: PCT/CN2020/108537

(22) 国际申请日: 2020 年 8 月 11 日 (11.08.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201911255210.4 2019年12月9日 (09.12.2019) CN

(71) 申请人: **珠海格力电器股份有限公司 (GREE ELECTRIC APPLIANCES, INC.OF ZHUHAI)** [CN/CN]; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **珠海联云科技有限公司 (LEAYUN TECHNOLOGY CO., LTD.OF ZHUHAI)** [CN/CN]; 中国广东省珠海市吉大景山路莲花巷8号601室, Guangdong 519015 (CN)。

(72) 发明人: **叶盛世 (YE, Shengshi)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **谭泽汉 (TAN, Zehan)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **陈彦宇 (CHEN, Yanyu)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **李茹 (LI, Ru)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **朱鹏飞 (ZHU, Pengfei)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **马鑫磊 (MA, Xinlei)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **曾安福 (ZENG, Anfu)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **黎小坚 (LI, Xiaojian)**; 中国广东省珠海市前山金鸡西

(54) **Title:** SECURITY METHOD AND SYSTEM, ELECTRONIC DEVICE, STORAGE MEDIUM, AND SMART CONTROLLER

(54) **发明名称**: 一种安防方法、系统、电子设备、存储介质及智能控制器

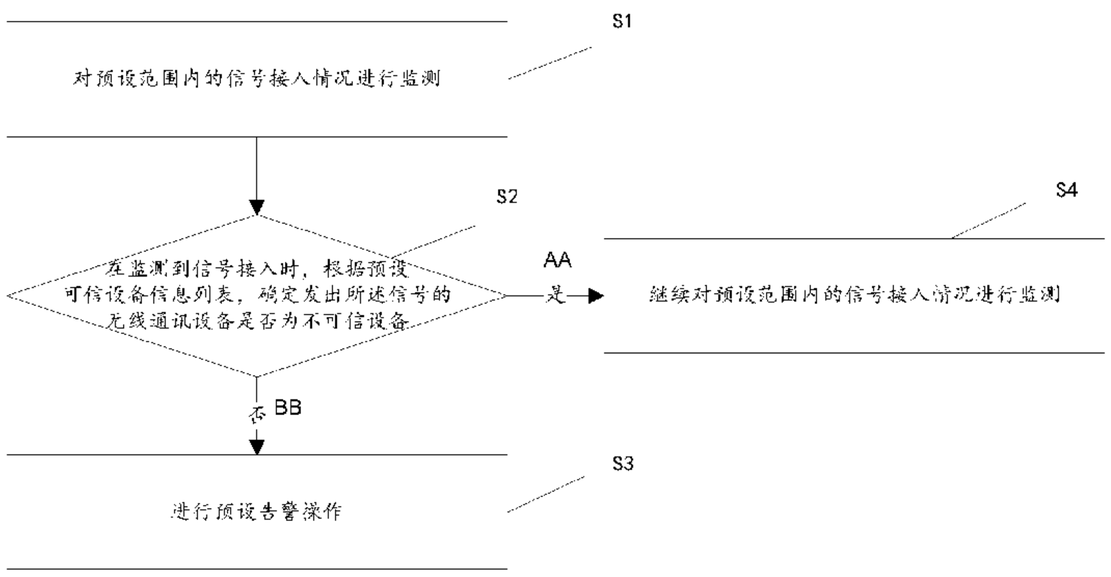

图 1

S1 Monitor signal access situation within a preset range
S2 Upon detecting signal access, determine according to a preset trusted device information list whether the wireless communication device transmitting the signal is an untrusted device
S3 Perform a preset alarm operation
S4 Continue to monitor the signal access situation within the preset range
AA Yes
BB No

(57) Abstract: A security method and system, electronic device, storage medium, and smart controller, the method comprising: monitoring signal access situation within a preset range (S1), the signal being a wireless communication signal; upon detecting signal access, determining according to a preset trusted device information list whether the wireless communication device transmitting the signal is an untrusted device (S2); and when it is determined that the wireless communication device is an untrusted device, performing a preset alarm operation (S3). Therefore, when a wireless communication device appears in the vicinity of a product in a home, whether the wireless communication device is safe can be determined directly by means of obtaining device information of the wireless communication device. If the wireless communication device is not safe, a user can immediately be aware of the situation and take countermea-

[见续页]

WO 2021/114700 A1

路, Guangdong 519070 (CN)。 **黄忠岐 (HUANG, Zhongqi)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **蔡琪 (CAI, Qi)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **刘郑宇 (LIU, Zhengyu)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (CN)。 **杜洋 (DU, Yang)**; 中国广东省珠海市前山金鸡西路, Guangdong 519070 (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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, IT, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, 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))。

sures, which can thus greatly improve the safety factor of the home and achieve concealed and trusted active monitoring of the home.

(57) 摘要: 一种安防方法、系统、电子设备、存储介质及智能控制器，其中，方法包括：对预设范围内的信号接入情况进行监测（S1），信号为无线通讯信号；在监测到信号接入时，根据预设可信设备信息列表，确定发出信号的无线通讯设备是否为不可信设备（S2）；在确定无线通讯设备为不可信设备的情况下，进行预设告警操作（S3）。就此，当家中产品附近出现无线通讯设备时，就可以直接通过获取到无线通讯设备的设备信息以确定无线通讯设备是否安全，若不安全，用户可以在第一时间知道情况并作出应对措施，由此可以大大提升家庭的安全系数，从而实现了对家里的隐蔽而可信的主动监控。

一种安防方法、系统、电子设备、存储介质及智能控制器

交叉援引

本公开基于申请号为201911255210.4、申请日为2019-12-09的中国专利申请提出，并要求该中国专利申请的优先权，该中国专利申请的全部内容在此引入本公开作为参考。

技术领域

本公开涉及通讯领域，尤其涉及一种安防方法、系统、电子设备、存储介质及智能控制器。

背景技术

在日常生活中，安全总是人们最关心的一个需求点，用户总会担心自己如果出门在外办事，以致于家中无人看守，使家里的一些贵重物品被盗窃或其他损害用户利益的事情发生。随着科技的迅速发展，偷盗手段也是层出不穷，急需一些可靠实用的方法来提升家里的安全系数。

发明内容

本公开的主要目的在于提出一种安防方法、系统、电子设备、存储介质及智能控制器，有效避免了现有技术中无法对家中是否来人的情况进行主动获知的问题，本公开具有监测手段隐秘且不易被人发现的效果。

在本公开的其中一实施例中，提供了一种安防方法，所述方法包括：对预设范围内的信号接入情况进行监测，所述信号为无线通讯信号；在监测到所述信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是

否为不可信设备；在确定所述无线通讯设备为所述不可信设备的情况下，进行预设告警操作。

在一些可选实施例中，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为所述不可信设备，包括：获取发出所述信号的无线通讯设备的设备信息；确定所述预设可信设备信息列表中是否包括所述无线通讯设备的设备信息；在确定所述预设可信设备信息列表中不包括所述无线通讯设备的设备信息的情况下，确定所述无线通讯设备为所述不可信设备。

在一些可选实施例中，所述方法还包括：统计所述信号的接入时长；在确定所述无线通讯设备为所述不可信设备的情况下，判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；在确定所述接入时长超过所述预设阈值的情况下，确定进行预设告警操作。

在一些可选实施例中，所述方法还包括：将所述无线通讯设备的设备信息上传至云服务器；指示所述云服务器统计所述无线通讯设备的设备信息的接入时长，并在确定所述无线通讯设备为所述不可信设备的情况下，指示所述云服务器判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；在确定所述接入时长超过所述预设阈值的情况下，指示所述云服务器确定进行预设告警操作。

在一些可选实施例中，在对所述预设范围内的所述信号接入情况进行监测之前，所述方法还包括：获取控制终端发送的启动监测触发指令，所述启动监测触发指令是由所述控制终端周期性和在预设时间段进行发送，或者，由所述控制终端周期性进行发送，或者，由所述控制终端在预设时间段进行发送；根据所述启动监测触发指令，确定对所述预设范围内的所述信号接入情况进行监测。

在一些可选实施例中，在对所述预设范围内的所述信号接入情况进行监测之前，所述方法还包括：根据关联的智能设备的历史使用时间数据，得到高危时间段，并确定在所述高危时间段对所述预设范围内的所述信号接入情况进行监测。

在一些可选实施例中，在对所述预设范围内的所述信号接入情况进行监测之前，所述方法还包括：根据触发监测功能启动指令的历史记录，确认自动检测功能的启动时刻；判断当前时刻是否为所述启动时刻；如果所述当前时刻为所述启动时刻，则确定在当前时刻对所述预设范围内的所述信号接入情况进行监测；如果所述当前时刻并非为所述启动时刻，则确定在所述启动时刻对所述预设范围内的所述信号接入情况进行监测。

在一些可选实施例中，进行预设告警操作，包括：获取关联的智能设备上传的检测结果，其中，所述检测结果表征为所述无线通讯设备的危险等级；根据预设危险等级表，执行与所述检测结果对应的预设告警操作，其中，所述预设危险等级表包括：至少一个危险等级，所述至少一个危险等级中每个危险等级对应的预设告警操作。

在一些可选实施例中，所述设备信息包括：蓝牙 MAC 地址。

在本公开的其中一实施例中，还提供了一种安防系统，所述系统包括：监测模块，设置为对预设范围内的信号接入情况进行监测，所述信号为无线通讯信号；确定模块，设置为在监测到所述信号接入时，根据预设可信设备信息列表，确定发出信号的无线通讯设备是否为不可信设备；安防模块，设置为在确定所述无线通讯设备为所述不可信设备的情况下，进行预设告警操作。

在本公开的其中一实施例中，还提供了一种电子设备，包括处理器和存储器；所述存储器设置为存储计算机指令，所述处理器设置为运行所述存储器存

储的计算机指令，以实现上述的一种安防方法。

在本公开的其中一实施例中，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一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现上述的一种安防方法。

在本公开的其中一实施例中，还提供了一种智能控制器，包括：智能安防装置，设置为执行上述的一种安防方法；或，上述的一种安防系统。

本公开至少部分实施例具有如下有益效果：当家中产品附近出现无线通讯设备时，就可以直接通过获取到该无线通讯设备的设备信息以确定该无线通讯设备是否安全，若不安全，用户可以在第一时间知道该情况并作出应对措施，由此可以大大提升家庭的安全系数，从而实现了对家里的隐蔽而可信的主动监控。

附图说明

图 1 是根据本公开其中一实施例的一种安防方法的流程图。

图 2 是根据本公开其中一实施例的一种安防方法的实现过程示意图。

图 3 是根据本公开其中一可选实施例的一种安防方法的流程图。

图 4 是根据本公开其中一实施例的一种安防系统的结构框图。

具体实施方式

应当理解，此处所描述的具体实施例仅仅用以解释本公开，并不用于限定本公开。

在后续的描述中，使用用于表示元件的诸如“模块”、“部件”或“单元”的后缀仅为了有利于本公开的说明，其本身没有特定的意义。因此，“模块”、

“部件”或“单元”可以混合地使用。

为了便于理解本公开实施例，下面通过几个具体实施例对本公开的实施过程进行详细的阐述。

在本公开的其中一实施例中，提供了一种安防方法，所述方法包括：对预设范围内的信号接入情况进行监测，所述信号为无线通讯信号；在监测到所述信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为不可信设备；在确定所述无线通讯设备为所述不可信设备的情况下，进行预设告警操作。

因此，当家中产品附近出现无线通讯设备时，就可以直接通过获取到该无线通讯设备的设备信息以确定该无线通讯设备是否安全，若不安全，用户可以在第一时间知道该情况并作出应对措施，由此可以大大提升家庭的安全系数，从而实现了对家里的隐蔽而可信的主动监控。

图 1 是根据本公开其中一实施例的一种安防方法的流程图，如图 1 所示，该安防方法应用于智能产品，包括但不限于：魔方控制器、空调、智能门锁、智能冰箱和智能摄像头。具体的，该方法包括：

S1：对预设范围内的信号接入情况进行监测；

在另一实施例中，该信号为无线通讯信号。

首先，用户需要给该智能产品上电，并且打开预设用户终端上配套的产品 APP。然后，使得该智能产品可以对预设范围内的所有无线通讯信号进行监测。如：该智能产品监测其附近出现的无线通讯信号，从而监测到发出该信号的的无线通讯设备。

当然，在本实施例中，并不对该预设范围进行限定，其可由系统自动设定，

也可由用户自行设定。如：预设范围为以该智能产品为中心，且直径为 20m 的范围。

在本实施例中，并不对本文中涉及的对无线通讯信号进行监测的具体方式进行限定，其包括但不限于：BLE 蓝牙扫描技术和 WiFi 扫描技术。

该步骤 S1 的一种实现方式为：该智能产品会周期性扫描周围所有带蓝牙且已开启蓝牙的无线通讯设备所发出的蓝牙信号，并通过蓝牙与发出这些蓝牙信号的无线通讯设备进行蓝牙通讯。

在另一实施例中，并不对该 S1 的执行时机进行限定，该执行时机包括但不限于以下各项中的一项或多项：（1）获取控制终端发送的启动监测触发指令，所述启动监测触发指令是由所述控制终端周期性和在预设时间段进行发送，或者，由所述控制终端周期性进行发送，或者，由所述控制终端在预设时间段进行发送；根据所述启动监测触发指令，确定对所述预设范围内的所述信号接入情况进行监测。

其中，该控制终端包括但不限于以下一项或多项：PC、笔记本 PC、平板 PC、智能手机、可穿戴无线通讯设备、嵌入式无线通讯设备、智能家电或其任何组合。

如：获取智能手机每天早上八点发送的启动监测触发指令，或者获取智能手机每隔 12 小时发送的启动监测触发指令。

（2）根据关联的智能设备的历史使用时间数据，得到高危时间段，并确定在所述高危时间段对所述预设范围内的所述信号接入情况进行监测。

其中，该高危时间段指的是家中无人或家中只有小孩等时间段。

具体的，在本实施例中，并不对该关联的智能设备进行限定，其可为电视或空调。如：根据电视机的使用频率分析推断出家中高危时间段，在该时间段

内则需要启动对预设范围内的无线通讯信号进行监测。

如上班时间段是 8 点到下午 5 点，根据历史信息或者用户手机预设这个时间段是家中无人时间段，则到了 8 点就自动开启监测模式。

（3）根据触发所述监测功能启动指令的历史记录，确认自动检测功能的启动时刻；判断当前时刻是否为所述启动时刻；如果所述当前时刻为所述启动时刻，则确定在当前时刻对所述预设范围内的所述信号接入情况进行监测；如果所述当前时刻并非为所述启动时刻，则确定在所述启动时刻对所述预设范围内的所述信号接入情况进行监测。

S2：在监测到信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为不可信设备；若是，则执行以下步骤 S4，否则，执行以下步骤 S3；

在监测到有信号接入时，即可获取发出该信号的无线通讯设备的设备信息，然后根据预设可信设备信息列表，确定接入的所述无线通讯设备是否为不可信设备。

S3：进行预设告警操作；

如：推送信息给告警终端（如：用户终端）、自动通知物业进行告警、启动门锁进行锁门、或者调用家中的摄像头进行视频记录。当然，也可与其他关联的智能设备进行联动，具体详情在后续进行详述。其中，该预设用户终端包括但不限于：手机。

S4：继续对预设范围内的信号接入情况进行监测。

在本实施例中，在确定无线通讯设备为不可信设备的情况下，则智能产品进行预设告警操作。

当然，值得注意的是，在本实施例中，并不对该智能产品的数量进行限定，

如：至少有一个相同或相似的智能产品在进行上述操作。

因此，当家中产品附近出现无线通讯设备时，就可以直接通过获取到该无线通讯设备的设备信息以确定该无线通讯设备是否安全，若不安全，用户可以在第一时间知道该情况并作出应对措施，由此可以大大提升家庭的安全系数，从而实现了对家里的隐蔽而可信的主动监控。

具体的，在另一实施例中，上述步骤 S2 的一种实现方式包括：

S21：获取发出所述信号的无线通讯设备的设备信息；

在本实施例中，并不对该设备信息的获取方式进行限定，只需其满足本实施例的要求即可，如：该信号中包括发出该信号的无线通讯设备的设备信息，通过对这些信号进行解析，即可从中获取发出这些接入的信号的无线通讯设备的设备信息。其中，这些设备信息包括但不限于：蓝牙 MAC 地址。

S22：确定预设可信设备信息列表中是否包括所述无线通讯设备的设备信息；若是，则执行以下步骤 S4，否则，执行以上步骤 S23；

S23：确定所述无线通讯设备为不可信设备。

所述预设可信设备信息列表中预存有可信设备的设备信息，即：智能产品需要预存值得信任的无线通讯设备的设备信息，如：预存值得信任的无线通讯设备的蓝牙 MAC 地址。如果该接入的无线通讯设备的设备信息包含于预设可信设备信息列表中，则确定该无线通讯设备为可信任无线通讯设备，否则，则确定该无线通讯设备为不可信设备。

若该设备信息包括蓝牙 MAC 地址，则该预设可信设备信息列表中预存有可信设备的蓝牙 MAC 地址；在此情况下，如果该预设可信设备信息列表中未存储有该接入无线通讯设备的蓝牙 MAC 地址，则可以确定该接入的无线通讯设备为不可信设备；当然，如果该预设可信设备信息列表中存储有该接入无线通讯设

备的蓝牙 MAC 地址，则可以确定该接入的无线通讯设备为可信设备，

在另一实施例中，在确定所述无线通讯设备为不可信设备之后，且在进行预设告警操作之前，该方法还包括：

S231：统计所述信号的接入时长；

值得注意的是，在本实施例中并不对实际执行记录的时机进行限定，只需其满足本实施例的要求即可，如：在确定有信号接入时时开始记录，也可以是在根据预设可信设备信息列表确定该无线通讯设备是可信设备时开始记录，还可以是在根据预设可信设备信息列表确定该无线通讯设备为不可信设备时开始记录。

S232：在确定所述无线通讯设备为不可信设备的情况下，判断所述无线通讯设备发出的所述信号的接入时长是否超过预设阈值；若是，则执行以下步骤 S3，否则，执行以上步骤 S4；

具体的，该智能产品还会识别出该无线通讯设备的种类，当然，还会统计无线通讯设备的设备信息的接入时长，即：统计该无线通讯设备与该智能产品的连接时长，从而统计该无线通讯设备发出的信号在该预设范围内的接入时长，依据该接入时长可判断该设备信息所属的无线通讯设备在预设范围内的连接时长是否过长。当然，如果该无线通讯设备的连接时长过长，则在该无线通讯设备为不可信设备的基础上，从而可以确定执行以上步骤 S3 以进行预设告警操作。

如果该无线通讯设备的连接时长在预设时间范围之内，则会确定判定该无线通讯设备只是临时接入，从而可以执行以上步骤 S4，以免出现误报。

在另一实施例中，在确定所述无线通讯设备为不可信设备之后，且在进行预设告警操作之前，该方法还包括：

S2311：将所述无线通讯设备的设备信息上传至云服务器；

S2312：指示所述云服务器统计所述无线通讯设备的设备信息的接入时长，并在确定所述无线通讯设备为不可信设备的情况下，指示所述云服务器判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；若是，则执行以下步骤S2313，否则，执行以上步骤S4。

值得注意的是，在本实施例中并不对实际执行记录的开始时刻进行限定，只需其满足本实施例的要求即可，如：在确定有信号接入时时开始记录，也可以是在根据预设可信设备信息列表确定该无线通讯设备是可信设备时开始记录，还可以是在根据预设可信设备信息列表确定该无线通讯设备为不可信设备时开始记录。

S2313：指示所述云服务器确定进行预设告警操作。

具体的，该智能产品还会上传该无线通讯设备的设备信息到云服务器上，而该云服务器会通过互联网来匹配识别出该无线通讯设备的种类，当然，还会统计所述无线通讯设备的设备信息的接入时长，即：统计该无线通讯设备与该智能产品的连接时长，从而统计该无线通讯设备发出的信号在该预设范围内的接入时长，依据该接入时长可判断该设备信息所属的无线通讯设备的连接时长是否过长。当然，如果该无线通讯设备的连接时长过长，则在判定该无线通讯设备为不可信设备的基础上，从而可以确定执行以上步骤S3以进行预设告警操作。如果该无线通讯设备的连接时长在预设时间范围之内，则会确定判定该无线通讯设备只是临时接入，从而可以执行以上步骤S4，以免出现误报。

在本实施例中，可以通过上述步骤S231、步骤232、步骤S3及步骤S4替代该步骤S2311、步骤2312、步骤2313及步骤S4,反之亦然。

在另一实施例中，上述进行预设告警操作包括：

S31:获取关联的智能设备上传的检测结果；

其中，该检测结果表征为所述无线通讯设备的危险等级。

S32:根据预设危险等级表，执行与所述检测结果对应的预设告警操作，其中，所述预设危险等级表包括：至少一个危险等级，所述至少一个危险等级中每个危险等级对应的预设告警操作。

其中，该关联的智能设备与执行上述步骤 S1 至步骤 S4、步骤 S21 至步骤 S23、步骤 S231 至步骤 S232、和步骤 S2311 至步骤 S2313 所涉及的智能产品关联。该关联的智能设备包括房子里其他的智能安防产品。

具体的，该智能产品会获取关联的智能设备对所述无线通讯设备的危险等级进行检测的检测结果，然后，该智能产品会根据预设危险等级表，执行与所述检测结果对应的预设告警操作，其中，所述预设危险等级表包括：至少一个危险等级，所述至少一个危险等级中每个危险等级对应的预设告警操作，从而实现了联动房子里其他的智能安防产品，来进一步核实异常情况。

其中，该关联的智能设备为执行处理流程和/或计算操作的任何类型的机器，其包括但不限于以下一项或多项：PC、笔记本 PC、平板 PC、智能手机、可穿戴无线通讯设备、嵌入式无线通讯设备、智能家电或其任何组合。

当然，该智能产品还可上报上述判定为不可信设备的无线通讯设备的设备信息给用户终端。

当然，该智能产品会上报上述判定为不可信设备的无线通讯设备的设备信息云服务器，通过云服务器转发该设备信息给预设用户终端。

此外，该智能产品或该云服务器也获取与其关联的智能设备对所述无线通讯设备的检测结果，此处，该检测结果表征为无线通讯设备的危险等级；然后，根据预设危险等级表，执行与所述检测结果对应的预设告警操作。其中，其他产品对无线通讯设备的检测可参照上述步骤 S1 至步骤 S4、步骤 S21 至步骤 S23、

步骤 S231 至步骤 S233、和步骤 S2311 至步骤 S2313。

此外，在本实施例中，并不对本文中涉及的通讯方式进行限定，其包括但不限于：WiFi 通讯、有线以太网通讯、BLE 蓝牙通讯、蓝牙 Mesh 通讯、ZigBee 通讯、LoRa 通讯和 2G/3G/4G/5G 通讯。

就此，当家中产品附近出现无线通讯信号时，就可以直接通过获取发出该信号的设备信息以确定该无线通讯设备是否安全，若不安全，用户可以在第一时间知道该情况并作出应对措施，由此可以大大提升家庭的安全系数。

图 2 是根据本公开其中一实施例的一种安防方法的实现过程示意图，图 3 是根据本公开其中一可选实施例的一种安防方法的流程图，如图 2 和 3 所示，该安防方法需要该智能产品满足以下三个条件，第一：该智能产品内部集成 BLE 蓝牙功能，该功能可由该智能产品控制开启或关闭；第二该智能产品需要具备联网的功能,例如该智能产品自身集成WiFi 通讯功能或者可以通过网关利用BLE 蓝牙通讯技术进行数据中转等；第三需要后台服务器以及对应配套该智能产品 APP 来做整个智能家居安防系统的支撑。具体的方案设计框架图,如上图2所示。下面是详细的操作步骤：

首先是用户需要给该智能产品进行上电并打开配套的该智能产品 APP 操作，然后在该智能产品 APP 的界面上添加信任无线通讯设备的蓝牙 MAC 地址，再点击开启 APP 上的布防功能，这时该智能产品会定时扫描周围所有的带蓝牙且已开启蓝牙的无线通讯设备，这样可以获取到周围的蓝牙无线通讯设备的 MAC 地址。然后通过判断所获取的蓝牙无线通讯设备 MAC 地址是否为信任无线通讯设备的蓝牙 MAC 地址，如果是信任无线通讯设备的蓝牙 MAC 地址，则该智能产品重新开始定时扫描；否则，则上传该蓝牙无线通讯设备的 MAC 地址到云服务器

上，云服务器再通过互联网来匹配识别该 MAC 地址是属于何种无线通讯设备并且开始计时该MAC地址的接入时长,然后再判断该MAC地址接入时长是否过长？如果不是，则该智能产品重新开始定时扫描；如果是则服务器会上报相关的陌生蓝牙设备信息给用户手机，并且联动房子里其他的智能安防该智能产品，来进一步核实异常情况。

其中，如图 2 所示，图中的 WiFi 通讯可以是其他通讯技术，例如有线以太网通讯、BLE 蓝牙通讯、蓝牙 Mesh 通讯、ZigBee 通讯、LoRa 通讯、2G/3G/4G/5G 通讯等等。

图 4 是根据本公开其中一实施例的一种安防系统的结构框图,如图 4 所示，在本公开的其中一实施例中，还提供了一种安防系统，其应设置为智能产品，该安防系统包括:监测模块 110,设置为对预设范围内的信号接入情况进行监测，所述信号为无线通讯信号；确定模块 120，设置为在监测到所述信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为不可信设备；安防模块 130，设置为在确定所述无线通讯设备为不可信设备的情况下，进行预设告警操作。

在一些可选实施例中，所述确定模块 120 包括：获取单元，设置为获取发出所述信号的无线通讯设备的设备信息；列表确定单元，设置为确定预设可信设备信息列表中是否包括所述无线通讯设备的设备信息；确定单元，设置为在确定所述预设可信设备信息列表中不包括所述无线通讯设备的设备信息的情况下，确定所述无线通讯设备为不可信设备，以及在确定所述预设可信设备信息列表中包括所述无线通讯设备的设备信息的情况下，确定所述无线通讯设备为可信设备。

在一些可选实施例中，所述装置还包括：第一统计模块，设置为统计所述信号的接入时长；第一判断模块，设置为在确定所述无线通讯设备为不可信设备的情况下，判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；在确定所述接入时长超过预设阈值的情况下，确定进行预设告警操作。

在一些可选实施例中，所述装置还包括：上传模块，设置为将所述无线通讯设备的设备信息上传至云服务器；第二判断模块，设置为指示所述云服务器统计所述无线通讯设备的设备信息的接入时长，并在确定所述无线通讯设备为不可信设备的情况下，指示所述云服务器判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；在确定所述接入时长超过预设阈值的情况下，指示所述云服务器确定进行预设告警操作。

在一些可选实施例中，所述系统还包括：第一启动监测模块，设置为获取控制终端发送的启动监测触发指令，所述启动监测触发指令是由所述控制终端周期性和在预设时间段进行发送，或者，由所述控制终端周期性进行发送，或者，由所述控制终端在预设时间段进行发送；根据所述启动监测触发指令，确定对预设范围内的信号接入情况进行监测。

在一些可选实施例中，所述系统还包括：第二启动监测模块，设置为根据关联的智能设备的历史使用时间数据，得到高危时间段，并确定在所述高危时间段对预设范围内的信号接入情况进行监测。

在一些可选实施例中，所述系统还包括：第三启动监测模块，设置为根据触发监测功能启动指令的历史记录，确认自动检测功能的启动时刻；判断当前时刻是否为所述启动时刻；如果所述当前时刻为所述启动时刻，则确定在当前时刻对预设范围内的信号接入情况进行监测；如果所述当前时刻并非为所述启动时刻，则确定在所述启动时刻对预设范围内的信号接入情况进行监测。

在一些可选实施例中，获取模块，设置为获取关联的智能设备上传的检测结果，其中，所述检测结果表征为所述无线通讯设备的危险等级；根据预设危险等级表，执行与所述检测结果对应的预设告警操作，其中，所述预设危险等级表包括：至少一个危险等级，所述至少一个危险等级中每个危险等级对应的预设告警操作。

在一些可选实施例中，所述设备信息包括：蓝牙 MAC 地址。

在本公开的其中一实施例中，还提供了一种智能控制器，包括：智能安防装置，设置为执行上述的一种安防方法；或，上述的一种安防系统。

当然，在本实施例中，该智能控制器包括但不限于以下各项中的一项或多项：智能控制器、遥控及智能魔方。

在本公开的其中一实施例中的一种智能控制器所涉及的名词及实现原理具体可以参照上述实施例的一种安防方法或上述实施例的一种安防系统，在此不再赘述。

在本公开的其中一实施例中，还提供了一种电子设备，包括处理器和存储器；所述存储器设置为存储计算机指令，所述处理器设置为运行所述存储器存储的计算机指令，以实现上述的一种安防方法。

在本公开的其中一实施例中的一种电子设备所涉及的名词及实现原理具体可以参照上述实施例中的一种安防方法，在此不再赘述。

在本公开的其中一实施例中，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一个或者多个模块，所述一个或者多个模块可被一个或者多个处理器执行，以实现上述的一种安防方法。

在本公开的其中一实施例中的一种计算机可读存储介质所涉及的名词及实现原理具体可以参照上述实施例中的一种安防方法，在此不再赘述。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

上述本公开实施例序号仅仅为了描述，不代表实施例的优劣。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本公开的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端（可以是手机，计算机，服务器，空调器，或者网络无线通讯设备等）执行本公开各个实施例所述的方法。

上面结合附图对本公开的实施例进行了描述，但是本公开并不局限于上述的具体实施方式，上述的具体实施方式仅仅是示意性的，而不是限制性的，本领域的普通技术人员在本公开的启示下，在不脱离本公开宗旨和权利要求所保护的范围情况下，还可做出很多形式，这些均属于本公开的保护之内。

1、一种安防方法，所述方法包括：

对预设范围内的信号接入情况进行监测，所述信号为无线通讯信号；

在监测到所述信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为不可信设备；

在确定所述无线通讯设备为不可信设备的情况下，进行预设告警操作。

2、根据权利要求 1 所述的方法，其中，所述预设可信设备信息列表中预存有可信设备的设备信息，

根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为所述不可信设备，包括：

获取发出所述信号的无线通讯设备的设备信息；

确定所述预设可信设备信息列表中是否包括所述无线通讯设备的设备信息；

在确定所述预设可信设备信息列表中不包括所述无线通讯设备的设备信息的情况下，确定所述无线通讯设备为所述不可信设备。

3、根据权利要求 1 所述的方法，其中，所述方法还包括：

统计所述信号的接入时长；

在确定所述无线通讯设备为所述不可信设备的情况下，判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；

在确定所述接入时长超过所述预设阈值的情况下，确定进行预设告警操作。

4、根据权利要求 2 所述的方法，其中，所述方法还包括：

将所述无线通讯设备的设备信息上传至云服务器；

指示所述云服务器统计所述无线通讯设备的设备信息的接入时长，并在确定所述无线通讯设备为所述不可信设备的情况下，指示所述云服务器判断所述无线通讯设备发出的信号的接入时长是否超过预设阈值；

在确定所述接入时长超过所述预设阈值的情况下，指示所述云服务器确定进行预设告警操作。

5、根据权利要求 1 所述的方法，其中，在对所述预设范围内的所述信号接入情况进行监测之前，所述方法还包括：

获取控制终端发送的启动监测触发指令，所述启动监测触发指令是由所述控制终端周期性和在预设时间段进行发送，或者，由所述控制终端周期性进行发送，或者，由所述控制终端在预设时间段进行发送；

根据所述启动监测触发指令，确定对所述预设范围内的所述信号接入情况进行监测。

6、根据权利要求 1 所述的方法，其中，在对所述预设范围内的所述信号接入情况进行监测之前，所述方法还包括：

根据关联的智能设备的历史使用时间数据，得到高危时间段，并确定在所述高危时间段对预设范围内的信号接入情况进行监测。

7、根据权利要求 1 所述的方法，其中，在对所述预设范围内的所述信号接入情况进行监测之前，所述方法还包括：

根据触发监测功能启动指令的历史记录，确认自动检测功能的启动时刻；

判断当前时刻是否为所述启动时刻；

如果所述当前时刻为所述启动时刻，则确定在所述当前时刻对所述预设范围内的所述信号接入情况进行监测；

如果所述当前时刻并非为所述启动时刻，则确定在所述启动时刻对所述预设范围内的所述信号接入情况进行监测。

8、根据权利要求 1 所述的方法，其中，进行预设告警操作，包括：

获取关联的智能设备上传的检测结果，其中，所述检测结果表征为所述无

线通讯设备的危险等级；

根据预设危险等级表，执行与所述检测结果对应的预设告警操作，其中，所述预设危险等级表包括：至少一个危险等级，所述至少一个危险等级中每个危险等级对应的预设告警操作。

9、根据权利要求 1 所述的方法，其中，所述设备信息包括：蓝牙媒体接入控制 MAC 地址。

10、一种安防系统，所述系统包括：

监测模块，设置为对预设范围内的信号接入情况进行监测，所述信号为无线通讯信号；

确定模块，设置为在监测到所述信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为不可信设备；

安防模块，设置为在确定所述无线通讯设备为所述不可信设备的情况下，进行预设告警操作。

11、一种电子设备，包括处理器和存储器；

所述存储器设置为存储计算机指令，所述处理器设置为运行所述存储器存储的计算机指令，以实现权利要求 1 至 9 中任一项所述的一种安防方法。

12、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一个或者多个程序，所述一个或者多个程序可被一个或者多个处理器执行，以实现权利要求 1 至 9 中任一项所述的一种安防方法。

13、一种智能控制器，包括：

智能安防装置，设置为执行权利要求 1 至 9 中任一项所述的一种安防方法；或，权利要求 10 所述的一种安防系统。

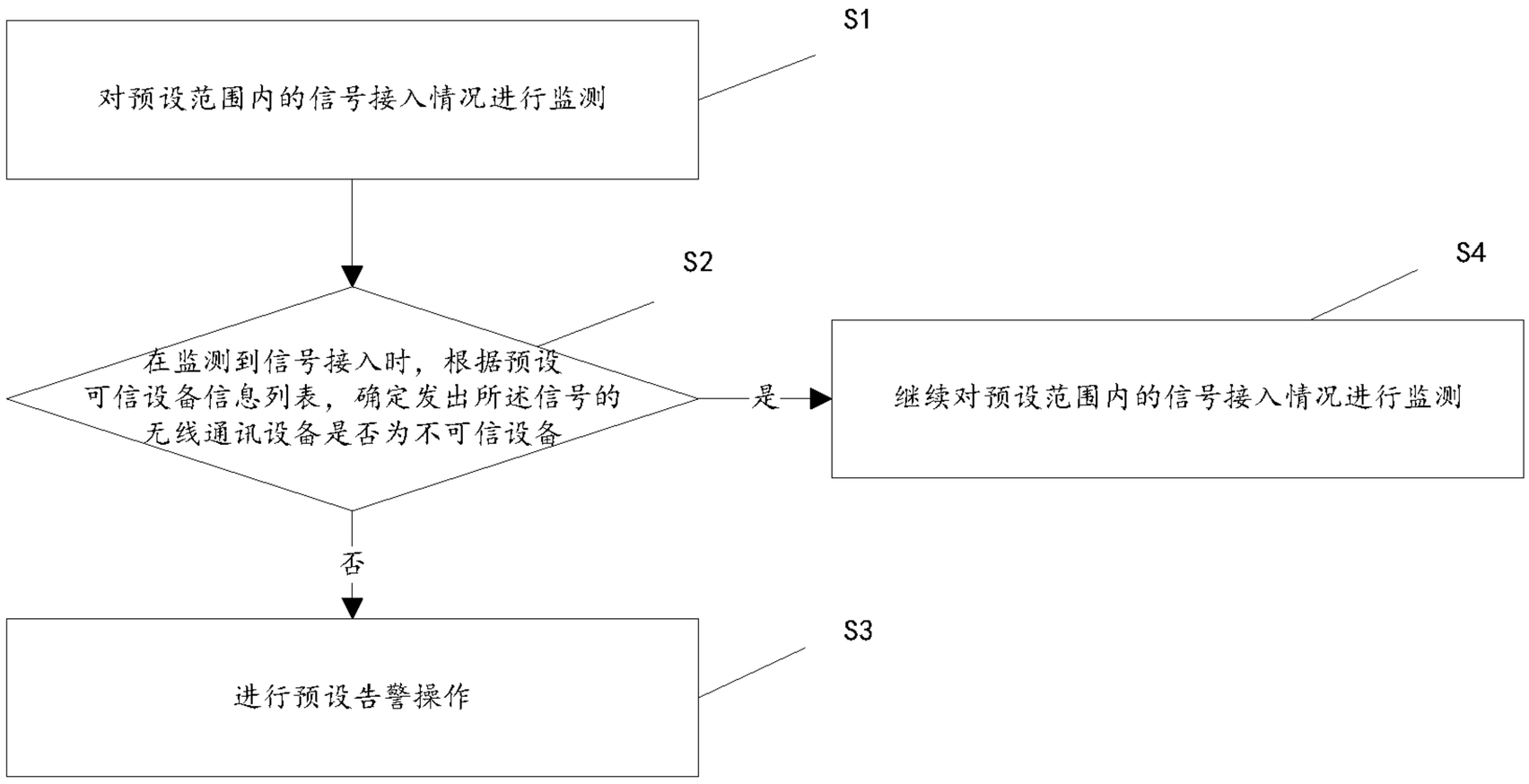
S1
对预设范围内的信号接入情况进行监测
S2
在监测到信号接入时，根据预设可信设备信息列表，确定发出所述信号的无线通讯设备是否为不可信设备
是
S4
继续对预设范围内的信号接入情况进行监测
否
S3
进行预设告警操作

图 1

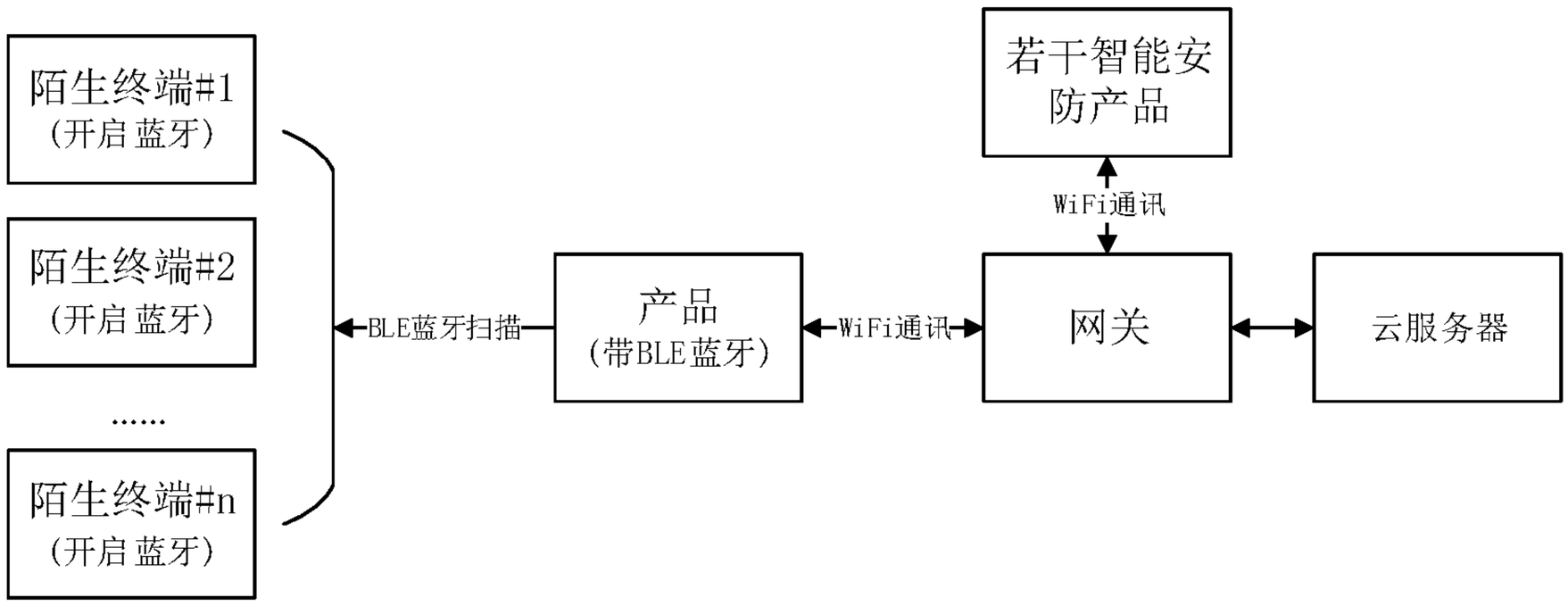
陌生终端#1
(开启蓝牙)
陌生终端#2
(开启蓝牙)
.....
陌生终端#n
(开启蓝牙)
BLE蓝牙扫描
产品
(带BLE蓝牙)
WiFi通讯
若干智能安防产品
WiFi通讯
网关
云服务器

图 2

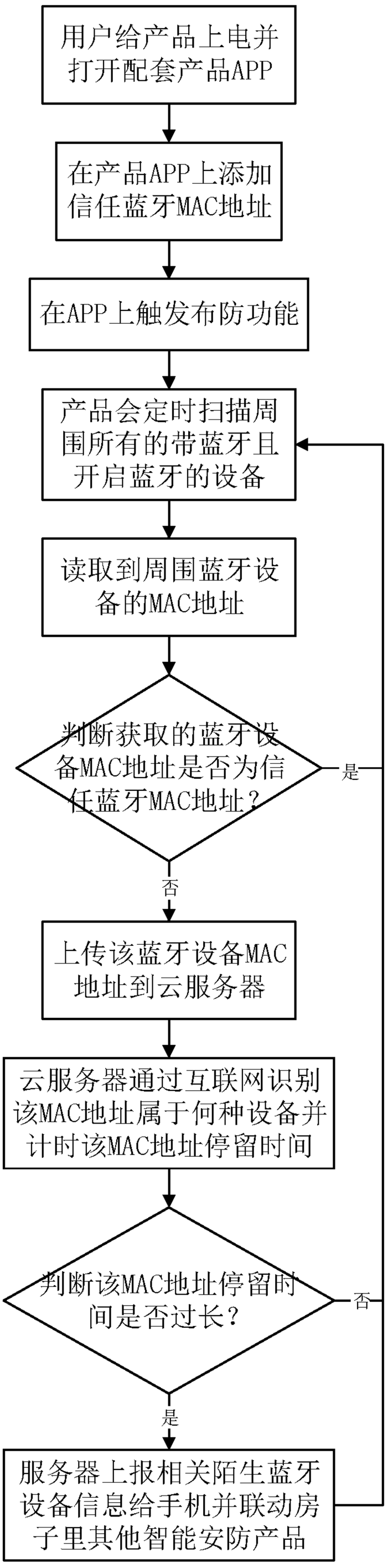
用户给产品上电并打开配套产品APP
在产品APP上添加信任蓝牙MAC地址
在APP上触发布防功能
产品会定时扫描周围所有的带蓝牙且开启蓝牙的设备
读取到周围蓝牙设备的MAC地址
判断获取的蓝牙设备MAC地址是否为信任蓝牙MAC地址？
是
否
上传该蓝牙设备MAC地址到云服务器
云服务器通过互联网识别该MAC地址属于何种设备并计时该MAC地址停留时间
判断该MAC地址停留时间是否过长？
否
是
服务器上报相关陌生蓝牙设备信息给手机并联动房子里其他智能安防产品

图 3

图 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2020/108537

A. CLASSIFICATION OF SUBJECT MATTER

G08B 13/24(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)

G08B; H04W

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)

CNPAT, CNKI, EPODOC, WPI: 安防, 无线, mac, 警, security, wireless, alarm+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 111047810 A (GREE ELECTRIC APPLIANCES, INC. OF ZHUHAI et al.) 21 April 2020 (2020-04-21) claims 1-13	1-13
X	CN 107623898 A (COMPUTER NETWORK INFORMATION CENTER, CHINESE ACADEMY OF SCIENCES, GUANGZHOU) 23 January 2018 (2018-01-23) description, paragraphs [0055]-[0136], and figures 1-5	1-13
X	CN 105741510 A (YUNDING NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 06 July 2016 (2016-07-06) description, paragraphs [0018]-[0025], and figures 1-4	1-13
X	CN 206058435 U (BEIJING XINDATAI TECHNOLOGY CO., LTD.) 29 March 2017 (2017-03-29) description, paragraphs [0029]-[0042], and figures 1-3	1-13
A	CN 107170185 A (SHANGHAI PHICOMM COMMUNICATION CO., LTD.) 15 September 2017 (2017-09-15) entire document	1-13
A	US 2019347925 A1 (OLARM ALARM SERVICE, INC.) 14 November 2019 (2019-11-14) entire document	1-13

☐ 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	Date of mailing of the international search report
22 October 2020	**12 November 2020**
Name and mailing address of the ISA/CN **China National Intellectual Property Administration (ISA/CN)** **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088** **China**	Authorized officer
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2020/108537

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN	111047810	A	21 April 2020	None	
CN	107623898	A	23 January 2018	None	
CN	105741510	A	06 July 2016	None	
CN	206058435	U	29 March 2017	None	
CN	107170185	A	15 September 2017	None	
US	2019347925	A1	14 November 2019	None	

国际检索报告

国际申请号
PCT/CN2020/108537

A. 主题的分类

G08B 13/24(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)

G08B; H04W

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））

CNPAT, CNKI, EPODOC, WPI: 安防，无线，mac，警，security, wireless, alarm+

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
PX	CN 111047810 A (珠海格力电器股份有限公司 等) 2020年 4月 21日 (2020-04-21) 权利要求1-13	1-13
X	CN 107623898 A (广州中国科学院计算机网络信息中心) 2018年 1月 23日 (2018-01-23) 说明书第[0055]-[0136]段，附图1-5	1-13
X	CN 105741510 A (云丁网络技术北京有限公司) 2016年 7月 6日 (2016-07-06) 说明书第[0018]-[0025]段，附图1-4	1-13
X	CN 206058435 U (北京信达泰科技有限公司) 2017年 3月 29日 (2017-03-29) 说明书第[0029]-[0042]段，附图1-3	1-13
A	CN 107170185 A (上海斐讯数据通信技术有限公司) 2017年 9月 15日 (2017-09-15) 全文	1-13
A	US 2019347925 A1 (OLARM ALARM SERVICE, INC.) 2019年 11月 14日 (2019-11-14) 全文	1-13

☐ 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
2020年 10月 22日	2020年 11月 12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 传真号 (86-10)62019451	受权官员 朱晓琳 电话号码 86-(10)-53962507

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2020/108537

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 111047810 A	2020年 4月 21日	无	
CN 107623898 A	2018年 1月 23日	无	
CN 105741510 A	2016年 7月 6日	无	
CN 206058435 U	2017年 3月 29日	无	
CN 107170185 A	2017年 9月 15日	无	
US 2019347925 A1	2019年 11月 14日	无	