(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102986193 B
(45)授权公告日 2016.01.27

(21)申请号 201180035860.3
(22)申请日 2011.06.22
(30)优先权数据
102010031931.7 2010.07.22 DE
(85)PCT国际申请进入国家阶段日
2013.01.22
(86)PCT国际申请的申请数据
PCT/EP2011/060489 2011.06.22
(87)PCT国际申请的公布数据
WO2012/010381 DE 2012.01.26
(73)专利权人 西门子公司
地址 德国慕尼黑
(72)发明人 R. 法尔克
(74)专利代理机构 中国专利代理(香港)有限公司 72001
代理人 丁永凡 刘春元
(51)Int.Cl.
H04L 29/06(2006.01)
H04W 12/06(2006.01)
(56)对比文件
US 2006282885 A1,2006.12.14, 说明书第24-30段、附图3.
审查员 石璐

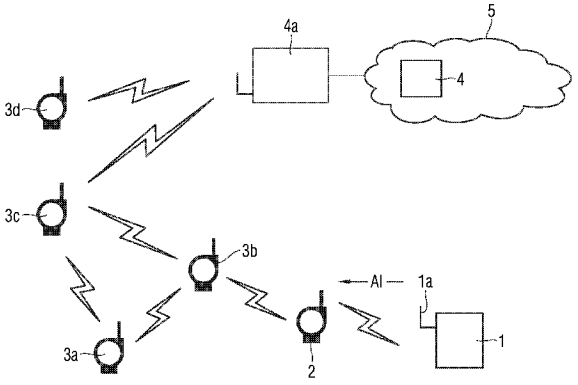
权利要求书1页 说明书4页 附图3页

(54)发明名称

用于向基站设备注册无线通信设备的方法以及相应的系统

(57)摘要

本发明涉及一种用于向基站设备注册无线通信设备的方法。该方法包括如下步骤:通过无线验证设备发送验证信息,通过无线通信设备尤其借助带内通信接收验证信息,将该验证信息通过无线通信设备传输至基站设备,通过基站设备检验所传输的验证信息,以及根据检验的结果将无线通信设备并入网络中。同样,本发明涉及一种相应的系统以及应用。



CN 102986193 B

1. 一种用于向基站设备(4)注册无线通信设备(2)的方法,具有如下步骤 :

(a)在对无线通信设备(2)和 / 或其他在验证设备(1)的无线电有效范围中的无线通信设备(3a,3b,3c,3d)的信号进行监控和 / 或分析之后,通过无线验证设备(1)发送验证信息(AI),

(b)通过无线通信设备(2)接收所发送的验证信息(AI),

(c)将所接收的验证信息(AI)通过无线通信设备(2)传输至基站设备(4),

(d)通过基站设备(4)检验所传输的验证信息(AI),以及

(e)根据检验的结果将无线通信设备(2)并入网络(5)中。

2. 根据权利要求 1 所述的方法,其中

借助带内通信来接收所发送的验证信息(AI)。

3. 根据权利要求 1 所述的方法,其中

借助减小的发射功率和 / 或定向进行验证信息(AI)的发送,使得验证信息只能够空间上受限地被接收。

4. 根据权利要求 1 所述的方法,其中

将无线通信设备(2)的被监控的和 / 或被分析的信号编码进验证信息(AI)中,其中被编码的被监控的通信由基站设备(4)进行分析。

5. 根据权利要求 1 至 4 中的任一项所述的方法,其中在发送验证信息(AI)之前对无线电环境的至少一个参数进行检验。

6. 根据权利要求 1 至 4 中的任一项所述的方法,其中在发送验证信息(AI)之前进行无线验证设备(1)的定位。

7. 一种用于注册无线通信设备(2)的系统,具有 :

(a)用于在对无线通信设备(2)和 / 或其他在验证设备(1)的无线电有效范围中的无线通信设备(3a,3b,3c,3d)的信号进行监控和 / 或分析之后发送验证信息(AI)的无线通信设备(1),以及具有

(b)用于接收所发送的验证信息(AI)的无线通信设备(2),并且用于将验证信息(AI)发送至基站设备(4)以用于注册无线通信设备(2),

(c)其中基站设备(4)根据对验证信息(2)检验的结果将无线通信设备(2)并入网络(5)中。

8. 根据权利要求 7 所述的系统,其中

借助带内通信来接收所发送的验证信息(AI)。

9. 根据权利要求 7 所述的系统,其中

其中无线通信设备(1)具有用于监视无线电环境和 / 或定位无线验证设备(1)的监视装置(1a)。

10. 根据权利要求 7 至 9 中的任一项所述的系统,其中无线验证设备(1)具有用于适配发射功率的装置(2)。

用于向基站设备注册无线通信设备的方法以及相应的系统

技术领域

[0001] 本发明涉及一种用于注册无线通信设备的方法以及一种相应的系统。

背景技术

[0002] 控制设备、传感器、执行器目前越来越多地以无线方式彼此连接或连成网络，以便保证尽可能大的灵活性。在此，对设备和传感器的维护也更为简单，因为例如在干扰情况下没有线缆管道等要被打开，而是只要直接打开设备。为了连接所述的控制设备、传感器等等，通常使用开放协议如 IEEE 802.11、WLAN、IEEE 802.15.4、蓝牙、ZigBee 或其他无线 HART。为了尽可能避免在无线连接时对传感器或控制设备的指令的操纵，控制设备或传感器的通信被相应的点接口以密码方式加密，例如通过 WLAN 连接借助 TKIP 或 CCMP 来加密或在 802.15.4 的情况下借助 AES-CCM 加密。为了将控制设备、传感器或者类似设备与无线电站连接并且建立经加密的连接，控制设备、传感器或通常无线通信设备必须配置为使得使用相应的加密术，即例如建立加密密钥。密钥的这种建立也称作自展（Bootstrapping）或配对。

[0003] 在 US 2006/282885 中公开了，待配置的无线设备的管理设备以无线方式提供证书。管理设备以由管理设备提供的证书对无线设备进行配置。

[0004] 此外已知的是，在受保护弱的阶段期间进行带内通信。然而，相应的待建立的无线通信设备为此需要经修改的特殊传输方法。最后已知的是，通过带外通道譬如人机交互（menschliche Interaktion）（即 PIN 的输入或校验等等）安全地进行配对。

[0005] 在此不利的是，上述方法要求高工作开销并且设计复杂，尤其是在使用在工业领域的情况下，因为在工业领域中设置有大量的无线通信设备。在此情况下同时需要，配对受保护或安全地进行，因为在此建立安全配置参数。

发明内容

[0006] 本发明的技术问题因此是提供用于向基站设备注册无线通信设备的方法和系统，其中多个要注册的无线设备的配对过程更为简单并且可利用低的工作开销来执行并且同时安全地进行配对过程。

[0007] 该技术问题通过根据以下所述的方法和来得以解决。根据本发明的用于向基站设备注册无线通信设备的方法，具有如下步骤：(a)在对无线通信设备和 / 或其他在验证设备的无线电有效范围中的无线通信设备的信号进行监控和 / 或分析之后，通过无线验证设备发送验证信息，(b) 通过无线通信设备接收所发送的验证信息，(c) 将所接收的验证信息通过无线通信设备传输至基站设备，(d) 通过基站设备检验所传输的验证信息，以及 (e) 根据检验的结果将无线通信设备并入网络中。相应的，根据本发明的用于注册无线通信设备的系统，具有：(a)用于在对无线通信设备和 / 或其他在验证设备的无线电有效范围中的无线通信设备的信号进行监控和 / 或分析之后发送验证信息的无线通信设备，(b) 用于接收所发送的验证信息的无线通信设备，并且用于将验证信息发送至基站设备以用于注册无线通

信设备，(c)其中基站设备根据对验证信息检验的结果将无线通信设备并入网络中。所实现的优点在此是，为了向基站设备注册无线通信设备不需要附加的交互，仅必须携带相应的验证设备，例如由装配工等携带，以便为与基站设备配对而准备无线通信设备。

[0008] 有利地，验证信息的发送借助减小的发射功率和/或定向地进行，使得验证信息只能空间上受限地被接收。在此情况下有利的是，进一步改善了注册无线通信设备的安全性，因为验证信息仅能在确定的范围中被接收，该范围由于有效范围有限和/或发射定向而空间上受限。这样，使潜在攻击者难以窃听或偷听所传输的验证信息。

[0009] 最好，在发送验证信息之前对无线通信设备和/或其他在验证设备的无线电有效范围中的无线通信设备的信号尤其是通信信号进行监控和/或分析。所实现的优点在此是，一方面由此总体上改进了注册无线通信设备的安全性并且同时可以提高可靠性。例如，如果在无线通信装置的频域中对无电线信号进行监控并且检验由无线通信设备发送和/或接收在此非常见的无线电信号和/或通信信号，则向无线验证设备的使用者显示相应信息，使得验证信息的发送只有当找到非常见的无线电信号和/或通信信号的原因以便能排除对无线通信设备的操纵或对无线通信设备与无线验证设备的通信的窃听时才进行。

[0010] 有利地，将无线通信设备的被监控和/或被分析的信号编码到验证信息中，其中尤其是经编码的被监控的和/或被分析的信号通过基站设备来分析。在此优点是，由此进一步提高了安全性，因为无线通信设备拥有关于确定的无线电特征和/或信号特征的信息，使得可以确定对无线通信设备的操纵。如果被监控的和/或被分析的信号的信息被编码进通过基站设备分析的验证信息中，则避免了：被操纵的无线通信设备本身将想要的错误校验结果发送给基站设备，并且这样尽管有操纵仍向基站设备进行无线通信设备的注册。由此，进一步提高了安全性。

[0011] 最好，在发送验证信息之前对无线电环境的至少一个参数进行检验。通过监控无线电环境的至少一个参数例如可以简单地识别出在该环境中的其他无线设备或干扰信号，使得在该环境中有干扰信号或其他设备的情况下必要时可以阻止验证信息的发送，以便避免操纵或验证信息从无线通信设备到无线通信设备的有错误的传输。

[0012] 为了保证并非出于操纵目的例如而从建筑物或预定义的环境中去除无线通信设备，有利的是，在发送验证信息之前进行无线验证设备的定位。

附图说明

[0013] 本发明的其他特征和优点从以下借助附图对优选实施例的描述中得到。

[0014] 在此示出

[0015] 图 1：在本发明的一个实施形式中用于注册无线通信设备的方法或系统；

[0016] 图 2A：根据本发明的第一实施形式的传输方法；

[0017] 图 2B：用于根据本发明的第二实施形式的方法的传输方法；以及

[0018] 图 3：用于根据本发明的第三实施形式的方法的传输图。。

具体实施方式

[0019] 图 1 示出了在本发明的第一实施形式中的用于注册无线通信设备的方法或系统。

[0020] 在图 1 中，附图标记 1 表示无线验证设备 1，其拥有无线电接口 1a。无线验证设备

1 将验证信息 AI 通过无线电接口 1a 传输至无线通信设备 2，该无线通信设备 2 应向基站设备 4 注册。已向基站设备 4 注册传感器节点 3a、3b、3c、3d 形式的其他无线通信设备，这些其他无线通信设备彼此无线连接，用于传输传感器数据，并且必要时还直接与基站设备 4 的无线电接口 4a 连接。基站设备 4 又与网络 5 连接并且在向基站设备 4 成功登记或验证（Network Join：网络加入）之后允许传感器节点 3a、3b、3c、3d 访问网络 5。只有向基站设备 4 注册过的传感器节点 3a、3b、3c、3d 可以向基站设备 4 成功地登记。基站设备 4 为此访问所存储的关于所注册的传感器节点 3a、3b、3c、3d 的信息。在将验证信息 AI 从无线验证设备 1 传输至无线通信设备 2 之后，无线通信设备将所获得的验证信息 AI 根据图 1 经过传感器节点 3b 和 3c 以及经过无线电接口 4a 发送到基站设备 4，该基站设备 4 检验验证信息 AI。为此，例如在验证信息 AI 中包含的加密校验和（消息验证码，数字签名）可以被校验。加密校验和可以通过无线验证设备 1 通过使用所存储的加密密钥来计算。如果验证信息 AI 有效，则通过基站设备 4 产生访问密钥 JK（加入密钥）并且通过相应的传感器节点 3a、3b、3c、3d 最后被传回给无线通信设备 2。无线通信设备 2 现在注册在基站设备 4 处并且现在访问基站设备 4 的网络 5。

[0021] 图 2A 示出了根据本发明的第一实施形式的传输方法。

[0022] 在图 2A 中详细地按时间顺序示出了至各设备的信息的传输。无线验证设备 1 将验证信息 AI 发送给待注册的无线通信设备 2。无线通信设备 2 现在将所接收的验证信息 AI 与待注册的无线通信设备 2 的相应标识号一起发送至相邻的传感器节点 3b，该传感器节点 3b 必要时又通过其他相邻的传感器节点 3a、3c、3d 和基站设备 4 的无线电接口 4a 将待注册的无线通信设备 2 的相应标识号和验证信息 AI 发送给基站设备 4。基站设备 4 在注册 R1 时现在检验所获得的验证信息 AI 并且在成功检验时产生访问密钥 JK 并且将待注册的无线通信设备 2 的标识号记入基站设备 4 的内部表中，在该表中同样记有有权访问的传感器节点 3a、3b、3c、3d。所产生的访问密钥 JK 于是通过无线电接口 4a、必要时通过传感器节点 3a、3c、3d 和无线通信设备 2 的相邻的传感器节点 3b 传输至该无线通信设备 2。由此，注册过程结束。在一个变型方案中，基站设备 4 在注册 R1 时还将访问密钥 JK 记入基站设备 4 的内部表中。在另一未示出的变型方案中，通过基站设备 4 使用基站设备 4 的外部表，例如数据库或目录服务，而不是基站设备 4 的内部表。

[0023] 在图 2B 中，由无线通信设备 2 与图 2A 不同还由无线通信设备 2 将预配置的或自产生的访问密钥 JK 经过相邻的传感器节点 3b，必要时经过其他传感器节点 3a、3b、3c 和经过基站设备 4 的无线电接口 4a 与验证信息 AI 和标识号一起传输至基站设备 4。在基站设备 4 上的注册 R2 现在如下地进行：基站设备 4 校验所获得的验证信息 AI 并且在检验为肯定的情况下将标识号和访问密钥 JK 记入有权访问的传感器节点的表中。最后，基站 4 通过无线电接口 4a 和传感器节点 3a、3b、3c、3 将相应的信号（曾经注册成功）传送至无线通信设备 2。

[0024] 图 3 示出了用于根据本发明的第二实施形式的方法的传输图。在图 3 中，无线验证设备 1 执行无线通信设备 2 的预登记方法的监视 B。该无线通信设备 2 将其标识号和访问密钥 JK 通过相邻的传感器节点 3b 并且必要时通过其他传感器节点 3a、3c、3d、通过无线电接口 4a 传送给基站设备 4。通过基站设备 4 对标识号和访问密钥进行存储 R3。基站设备 4 进一步将包含信息的预登记信号（曾经预注册成功）传回给无线通信设备 2。预登记方法

通过无线验证设备 1 来监视(监视 B)和分析。根据分析的结果于是判断验证信息 AI 是否被传送至无线通信设备 2。在分析 A 的结果为肯定的情况下,验证信息 AI 被传送至无线通信设备 2。无线通信设备 2 将所获得的验证信息和无线通信设备 2 的标识号通过传感器节点 3b、3a、3c、3d 和无线电接口 4a 又传送至基站设备 4。在基站设备 4 上进行注册 R4,其中验证信息 AI 被校验,并且在校验结果为肯定的情况下将无线通信设备 2 的标识号和访问密钥 JK 记入根据对前面的附图的描述的相应访问表中。此外,基站设备 4 将相应的信息(无线通信设备 2 曾向基站设备 4 注册成功)传回给无线通信设备 2。

[0025] 尽管本发明通过前面的优选的实施例来描述,但本发明并不限于此而是可以以多种方式进行修改。

[0026] 例如可以将验证信息作为广播来传输。以此方式,所有位于附近的通信设备可以接收验证信息。此外,可以将验证信息作为单播传输至某一无线通信设备,例如在以传感器节点的设备证书或一般而言的无线通信设备的设备证书进行验证之后。在此,进行其他与节点有关的传输特性的测量,例如将其信号强度与预给定的值比较或可以借助远程测量检验在无线验证信息与无线通信设备之间的距离。验证信息 AI 例如可以包括口令,在带有加密校验和的时间戳的情况下随时间变化的随机序列(消息验证码 MAC 或数字签名)。此外,由无线验证设备提供的验证信息可以由多个子信息组成。例如可能的是,仅一子信息从无线通信设备被传输给基站设备。例如可能的是,无线验证设备例如提供多元组,包括操作信息或断言(例如 SAML 断言)和密钥。无线通信设备于是将断言传输给基站设备并且验证密钥的知识,而不将密钥传输给基站设备。这例如可以如下地进行 :基站设备将随机数传输至无线通信设备中。无线通信设备于是进行计算,将随机数和密钥例如 HMAC-SHA(密钥,随机数)作为参数输入到计算中并且将结果传回给基站设备,基站设备于是又检验 :根据结果该无线通信设备是否应获得对基站设备的网络的访问。

[0027] 无线通信设备的无线通信例如可以借助 WLAN 或蓝牙来进行。

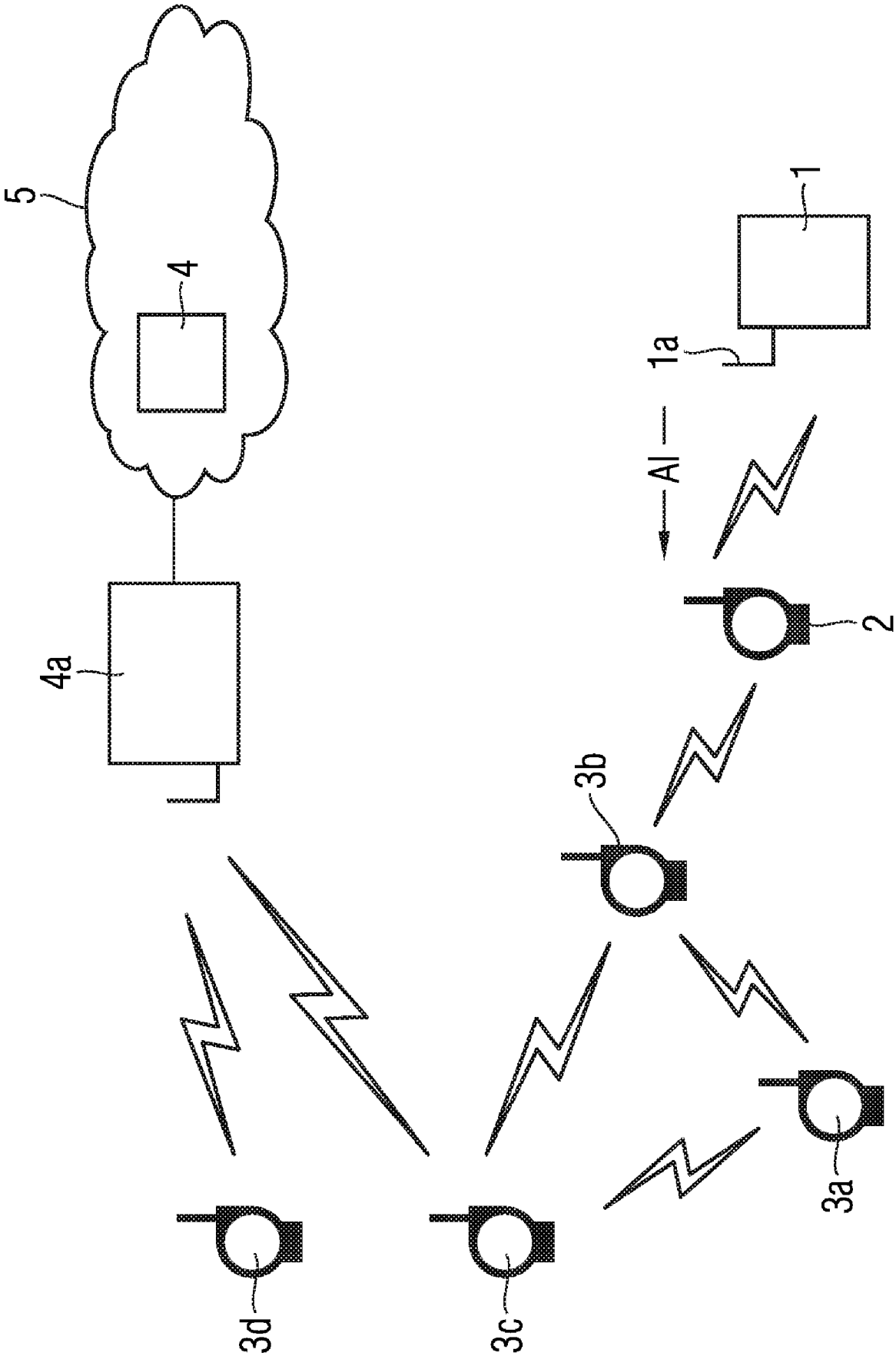


图 1

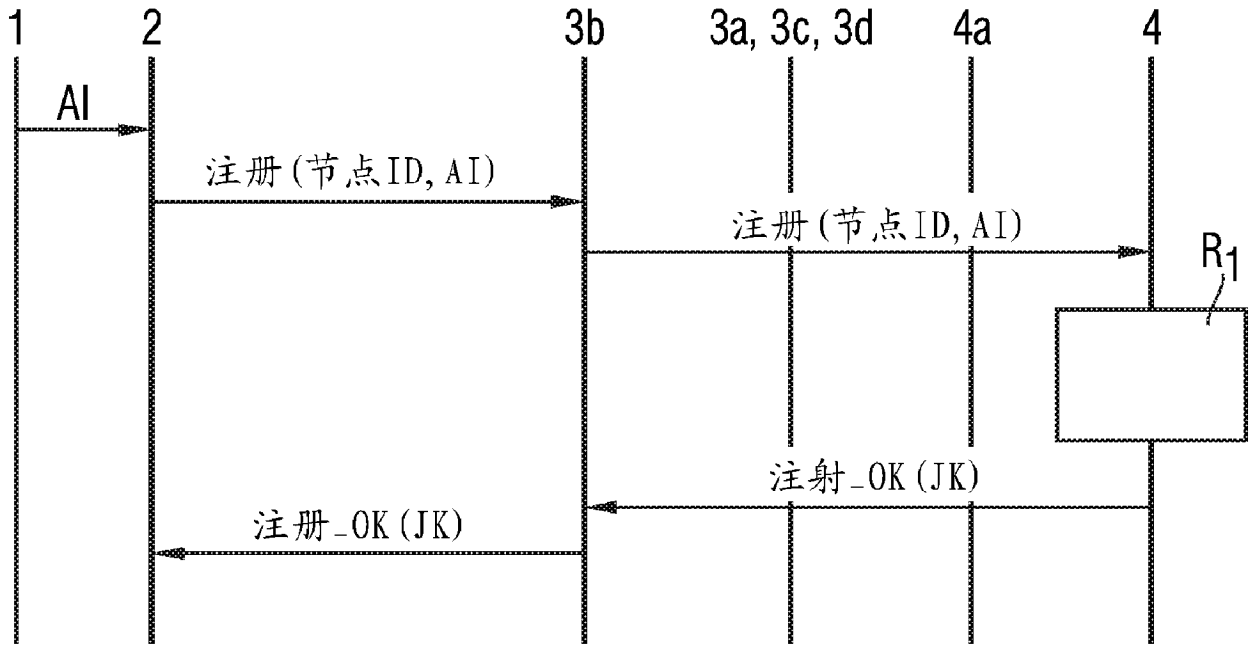

1
2
3b
3a, 3c, 3d
4a
4
AI
注册(节点ID, AI)
注册(节点ID, AI)
R1
注射_OK(JK)
注册_OK(JK)

图 2A

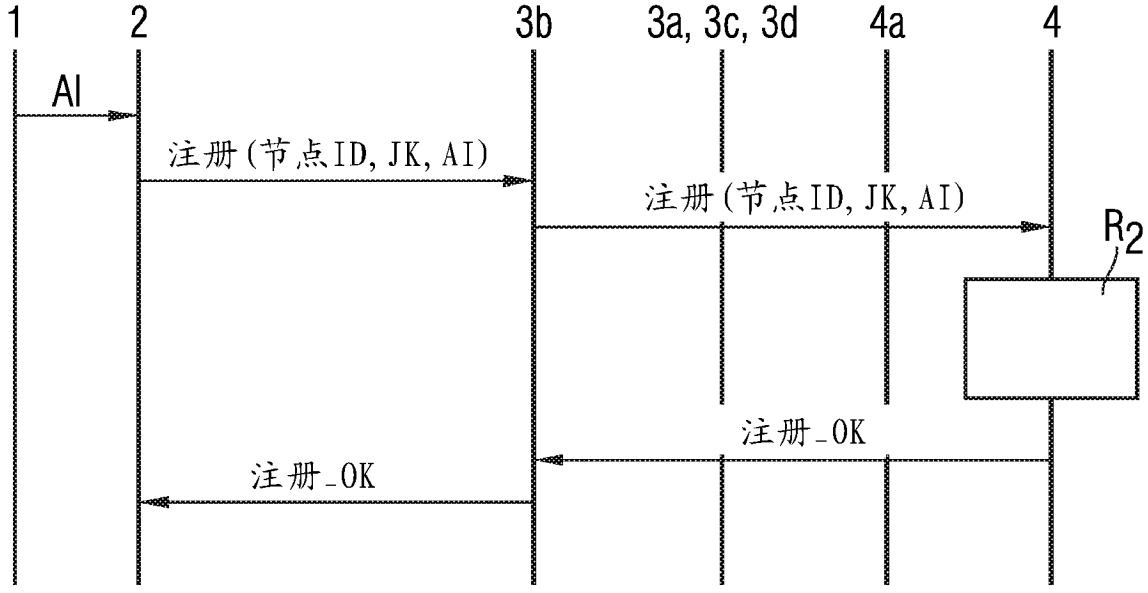

1
2
3b
3a, 3c, 3d
4a
4
AI
注册(节点ID, JK, AI)
注册(节点ID, JK, AI)
R2
注册_OK
注册_OK

图 2B

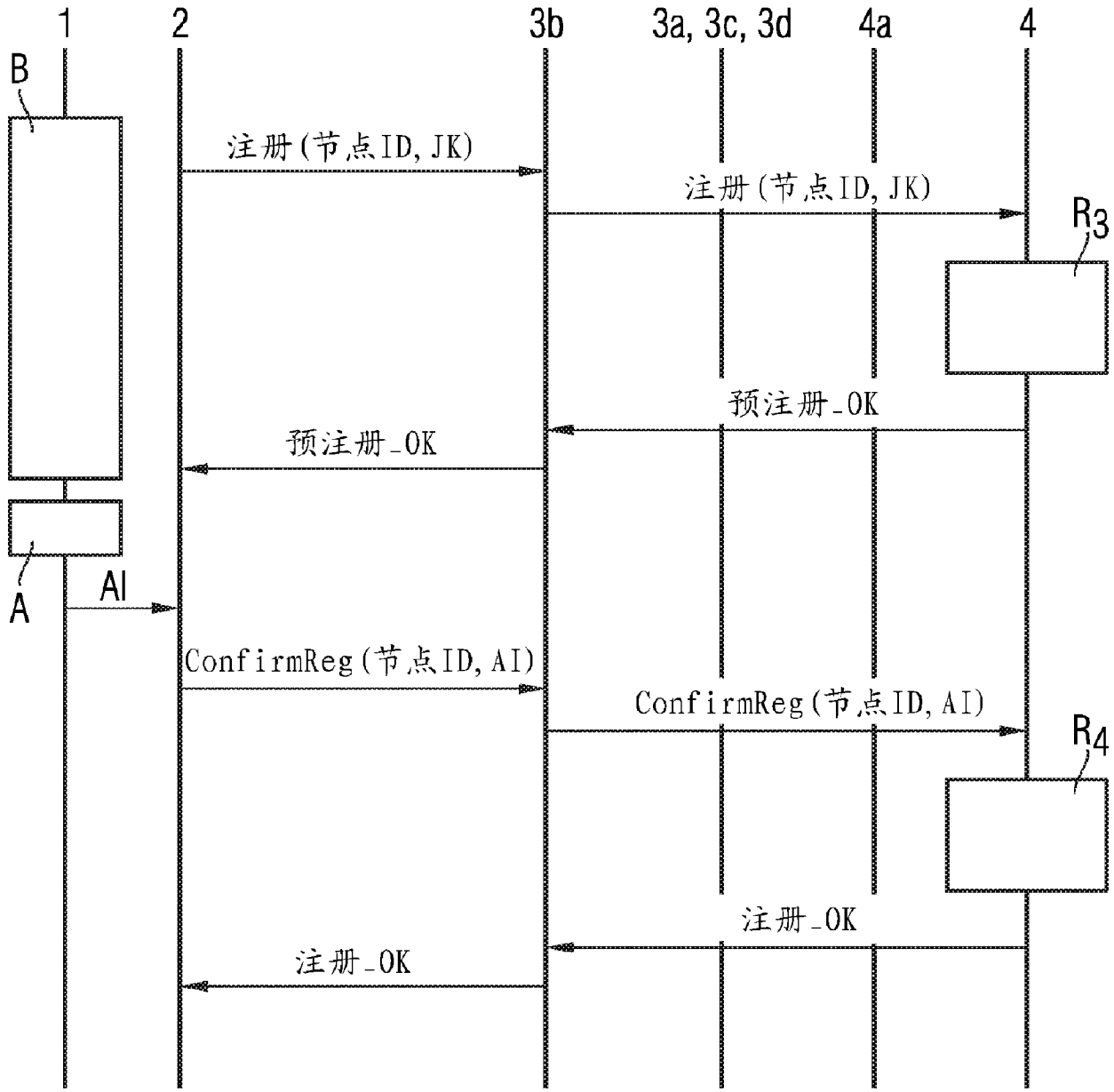

1
2
3b
3a, 3c, 3d
4a
4
B
注册(节点ID, JK)
注册(节点ID, JK)
R3
预注册_OK
预注册_OK
A
AI
ConfirmReg(节点ID, AI)
ConfirmReg(节点ID, AI)
R4
注册_OK
注册_OK

图 3