(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 103178966 B
(45)授权公告日 2015.08.12

(21)申请号 201310088668.1

(22)申请日 2013.03.19

(73)专利权人 北京经纬恒润科技有限公司
地址 100101 北京市朝阳区安翔北里11号B座8层

(72)发明人 付宽 郭光超 吴云平

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 王宝筠

(51)Int.Cl.
H04L 9/32(2006.01)
B60R 25/24(2013.01)

(56)对比文件
WO 2007074354 A1,2007.07.05,
EP 1916162 A2,2007.10.24,
US 20080061931 A1,2008.03.13,
CN 101290688 A,2008.10.22,
CN 201865426 U,2011.06.15,
CN 102542644 A,2012.07.04,
CN 102555991 A,2012.07.11,
CN 102649420 A,2012.08.29,

审查员 张浩

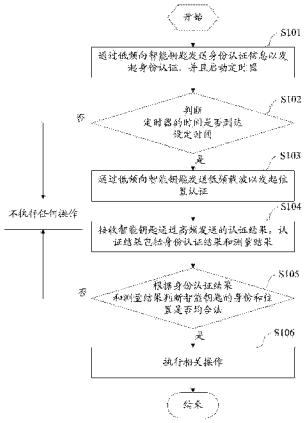
权利要求书2页 说明书8页 附图6页

(54)发明名称

车辆与智能钥匙的KPD认证方法、车辆基站及系统

(57)摘要

本申请提供一种车辆与智能钥匙的KPD认证方法、车辆基站及系统，认证方法包括：通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证，启动定时器；当定时器的时间到达设定时间时，通过低频向智能钥匙发送低频载波以发起位置认证；接收智能钥匙通过高频发送的认证结果，认证结果包括智能钥匙对身份认证信息进行解密解码得到的身份认证结果和测量低频载波的场强所得到的测量结果；根据身份认证结果和测量结果判断智能钥匙的身份和位置是否均合法，当智能钥匙的身份和位置均合法时，执行相关操作。本申请提供的方法、车辆基站及系统极大缩短了KPD认证的时间，减少了通讯过程中出现不稳定因素的可能性，增强了PEPS的实用性。



CN 103178966 B

1. 一种车辆与智能钥匙的 KPD 认证方法，其特征在于，车辆基站设置定时器，所述方法包括：

通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证，并且启动所述定时器；

当所述定时器的时间到达设定时间时，通过低频向所述智能钥匙发送低频载波以发起位置认证；

接收所述智能钥匙通过高频发送的认证结果，所述认证结果包括：所述智能钥匙对所述身份认证信息进行解密解码得到的身份认证结果，以及测量所述低频载波的场强所得到的测量结果；

根据所述身份认证结果和所述测量结果判断所述智能钥匙的身份和位置是否均合法，当所述智能钥匙的身份和位置均合法时，执行相关操作。

2. 根据权利要求 1 所述的方法，其特征在于，所述定时器为 1 ～ 20ms 的定时器。

3. 根据权利要求 1 所述的方法，其特征在于，所述身份认证信息包括：智能钥匙 ID、随机数组、第一密文和 CRC 校验字节，所述第一密文通过将原始数据利用第一加密算法加密生成，所述原始数据包括：智能钥匙 ID、智能钥匙密钥、随机数组和密码。

4. 根据权利要求 3 所述的方法，其特征在于，所述智能钥匙对所述身份认证信息进行解密解码得到身份认证结果的过程包括：

通过所述身份认证信息中的 CRC 校验字节判断接收的数据是否有效，如果接收的数据有效，则将身份认证信息中的第一密文通过与所述第一加密算法对应的第一解密算法进行解密，得到解密数据，将解密数据利用第二加密算法加密生成第二密文，生成包括 CRC 校验字节和第二密文的身份认证结果。

5. 根据权利要求 4 所述的方法，其特征在于，根据所述身份认证结果判断所述智能钥匙的身份是否合法的过程包括：

通过所述身份认证结果中的 CRC 校验字节判断接收的数据是否有效，如果接收的数据有效，则通过与第二加密算法对应的第二解密算法进行解密，得到解密数据，将解密数据与原始数据进行比对，如果解密数据与原始数据一致，则智能钥匙身份合法。

6. 根据权利要求 1 所述的方法，其特征在于，根据所述测量结果判断所述智能钥匙的位置是否合法的过程包括：

根据所述测量结果确定所述智能钥匙与车辆基站天线的距离，判断所述距离是否在预设范围内，如果所述距离在预设范围内，则所述智能钥匙的位置合法。

7. 一种车辆基站，其特征在于，所述车辆基站设置有定时器，所述车辆基站包括：第一发送单元、启动单元、第一判断单元、第二发送单元、接收单元、第二判断单元和执行单元；

所述第一发送单元，用于通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证；

所述启动单元，用于在所述第一发送单元向所述智能钥匙发送身份认证信息时启动所述定时器；

所述第一判断单元，用于判断所述定时器的时间是否到达设定时间；

所述第二发送单元，用于当所述定时器的时间到达设定时间时，通过低频向所述智能钥匙发送低频载波以发起位置认证；

所述接收单元，用于接收所述智能钥匙通过高频发送的认证结果，所述认证结果包括：所述智能钥匙对所述身份认证信息进行解密解码得到的身份认证结果，以及测量所述低频载波的场强所得到的测量结果；

所述第二判断单元，用于根据所述身份认证结果和所述测量结果判断所述智能钥匙的身份和位置是否均合法；

所述执行单元，用于当所述智能钥匙的身份和位置均合法时，执行相关操作。

8. 根据权利要求 7 所述的车辆基站，其特征在于，所述身份认证信息包括：智能钥匙 ID、随机数组、第一密文和 CRC 校验字节，所述第一密文通过将原始数据利用第一加密算法加密生成，所述原始数据包括：智能钥匙 ID、智能钥匙密钥、随机数组和密码。

9. 根据权利要求 7 所述的车辆基站，其特征在于，所述定时器为 1 ～ 20ms 的定时器。

10. 一种车辆与智能钥匙的 KPD 认证系统，其特征在于，包括：车辆基站和智能钥匙；

所述车辆基站，用于通过低频向所述智能钥匙发送已加密编码的身份认证信息，并且启动定时器，当所述定时器的时间到达设定时间时，通过低频向所述智能钥匙发送低频载波以发起位置认证；

所述智能钥匙，用于对所述身份认证信息进行解密解码得到身份认证结果，并且，测量所述低频载波的场强得到测量结果，将所述身份认证结果和测量结果通过高频发送往所述车辆基站，以使所述车辆基站在根据所述身份认证结果和所述测量结果判断出所述智能钥匙的身份和位置均合法时，执行相关操作。

车辆与智能钥匙的KPD认证方法、车辆基站及系统

技术领域

[0001] 本发明涉及PEPS技术领域，尤其涉及一种车辆与智能钥匙的KPD认证方法、车辆基站及系统。

背景技术

[0002] 随着科技的发展和汽车的普及，汽车朝着越来越智能的方向发展，PEPS技术成为智能汽车舒适性的重要配置。而车辆与智能钥匙的KPD认证作为PEPS的关键技术，有着巨大的应用前景。

[0003] 现有技术中，车辆与智能钥匙的KPD认证过程为：车辆基站通过低频发送身份认证信息；智能钥匙接收身份认证信息，并对身份认证信息进行解密解码认证，将得到的认证结果通过高频发送给车辆基站；车辆基站接收到高频认证结果，解析高频认证结果是否合法，如果合法，则发送低频载波，发起钥匙位置认证；智能钥匙测量低频载波场强，并将低频载波场强的测量结果发送给车辆基站；车辆基站解析低频载波场强的测量结果，根据解析结果判断智能钥匙的位置是否合法，如果合法则执行相关操作。

[0004] 发明人在实现本发明创造的过程中发现：现有技术中，车辆与智能钥匙的KPD认证过程比较繁琐，耗时较长，并且，增加了车辆基站与智能钥匙通讯过程中出现不稳定因素的可能性。

发明内容

[0005] 有鉴于此，本发明提供了一种车辆与智能钥匙的KPD认证方法、车辆基站及系统，用以解决现有技术中的车辆与智能钥匙的KPD认证过程比较繁琐，耗时较长，并且，增加了车辆基站与智能钥匙通讯过程中出现不稳定因素的可能性的问题，其技术方案如下：

[0006] 一种车辆与智能钥匙的KPD认证方法，车辆基站设置定时器，所述方法包括：

[0007] 通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证，并且启动所述定时器；

[0008] 当所述定时器的时间到达设定时间时，通过低频向所述智能钥匙发送低频载波以发起位置认证；

[0009] 接收所述智能钥匙通过高频发送的认证结果，所述认证结果包括：所述智能钥匙对所述身份认证信息进行解密解码得到的身份认证结果，以及测量所述低频载波的场强所得到的测量结果；

[0010] 根据所述身份认证结果和所述测量结果判断所述智能钥匙的身份和位置是否均合法，当所述智能钥匙的身份和位置均合法时，执行相关操作。

[0011] 优选的，所述定时器为1～20ms的定时器。

[0012] 其中，所述身份认证信息包括：智能钥匙ID、随机数组、第一密文和CRC校验字节，所述第一密文通过将原始数据利用第一加密算法加密生成，所述原始数据包括：智能钥匙ID、智能钥匙密钥、随机数组和密码。

[0013] 其中，所述智能钥匙对所述身份认证信息进行解密解码得到身份认证结果的过程包括：通过所述身份认证信息中的 CRC 校验字节判断接收的数据是否有效，如果接收的数据有效，则将身份认证信息中的第一密文通过与所述第一加密算法对应的第一解密算法进行解密，得到解密数据，将解密数据利用第二加密算法加密生成第二密文，生成包括 CRC 校验字节和第二密文的身份认证结果。

[0014] 其中，根据所述身份认证结果判断所述智能钥匙的身份是否合法的过程包括：

[0015] 通过所述身份认证结果中的 CRC 校验字节判断接收的数据是否有效，如果接收的数据有效，则通过与第二加密算法对应的第二解密算法进行解密，得到解密数据，将解密数据与原始数据进行比对，如果解密数据与原始数据一致，则智能钥匙身份合法。

[0016] 其中，根据所述测量结果判断所述智能钥匙的位置是否合法的过程包括：

[0017] 根据所述测量结果确定所述智能钥匙与车辆基站天线的距离，判断所述距离是否在预设范围内，如果所述距离在预设范围内，则所述智能钥匙的位置合法。

[0018] 一种车辆基站，所述车辆基站设置有定时器，所述车辆基站包括：第一发送单元、启动单元、第一判断单元、第二发送单元、接收单元、第二判断单元和执行单元；

[0019] 所述第一发送单元，用于通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证；

[0020] 所述启动单元，用于在所述第一发送单元向所述智能钥匙发送身份认证信息时启动所述定时器；

[0021] 所述第一判断单元，用于判断所述定时器的时间是否到达设定时间；

[0022] 所述第二发送单元，用于当所述定时器的时间到达设定时间时，通过低频向所述智能钥匙发送低频载波以发起位置认证；

[0023] 所述接收单元，用于接收所述智能钥匙通过高频发送的认证结果，所述认证结果包括：所述智能钥匙对所述身份认证信息进行解密解码得到的身份认证结果，以及测量所述低频载波的场强所得到的测量结果；

[0024] 所述第二判断单元，用于根据所述身份认证结果和所述测量结果判断所述智能钥匙的身份和位置是否均合法；

[0025] 所述执行单元，用于当所述智能钥匙的身份和位置均合法时，执行相关操作。

[0026] 其中，所述身份认证信息包括：智能钥匙 ID、随机数组、第一密文和 CRC 校验字节，所述第一密文通过将原始数据利用第一加密算法加密生成，所述原始数据包括：智能钥匙 ID、智能钥匙密钥、随机数组和密码。

[0027] 优选的，所述定时器为 1 ～ 20ms 的定时器。

[0028] 一种车辆与智能钥匙的 KPD 认证系统，包括：车辆基站和智能钥匙；

[0029] 所述车辆基站，用于通过低频向所述智能钥匙发送已加密编码的身份认证信息，并且启动所述定时器，当所述定时器的时间到达设定时间时，通过低频向所述智能钥匙发送低频载波以发起位置认证；

[0030] 所述智能钥匙，用于对所述身份认证信息进行解密解码得到身份认证结果，并且，测量所述低频载波的场强得到测量结果，将所述身份认证结果和测量结果通过高频发送往所述车辆基站，以使所述车辆基站在根据所述身份认证结果和所述测量结果判断出所述智能钥匙的身份和位置均合法时，执行相关操作。

[0031] 上述技术方案中具有如下有益效果：

[0032] 本发明提供的车辆与智能钥匙的KPD认证方法、车辆基站及系统中，在车辆基站设置定时器，当车辆基站通过低频向智能钥匙发送身份认证信息时，启动定时器，当定时器的时间到达设定时间时，车辆基站通过低频向智能钥匙发送低频载波发起位置认证，而不用像现有技术那样，车辆基站在接收到智能钥匙通过高频发送的身份认证结果后，才向智能钥匙发送低频载波发起位置认证。与现有技术中的KPD认证方法相比，本发明减少了一个高频通讯过程，并且车辆基站对身份认证结果和测量结果的判断放在一个过程，这样极大缩短了KPD的认证时间，减少了通讯过程中出现不稳定因素的可能性，并且，更容易在设定时间内认证成功，快速实现解锁车门、启动车辆等操作，增强了PEPS的实用性。

附图说明

[0033] 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，下面将对实施例或现有技术描述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，还可以根据提供的附图获得其他的附图。

[0034] 图1为本发明实施例一提供的车辆与智能钥匙的KPD认证方法的流程示意图；

[0035] 图2为本发明实施例二提供的车辆与智能钥匙的KPD认证方法的流程示意图；

[0036] 图3为本发明实施例三提供的车辆基站的结构示意图；

[0037] 图4为本发明实施例四提供的车辆基站的结构示意图；

[0038] 图5为本发明实施例五提供的车辆与智能钥匙的KPD认证系统的结构示意图；

[0039] 图6为本发明实施例五提供的车辆与智能钥匙的KPD认证系统实现KPD认证的流程示意图。

具体实施方式

[0040] 为了引用和清楚起见，下文中使用的技术名词的说明、简写或缩写总结如下：

[0041] PEPS:Passive entry&push start systems无钥匙进入和启动系统

[0042] KPD:Key Position Detection钥匙位置检测

[0043] 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做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。

[0044] 实施例一

[0045] 本发明实施例一提供了一种车辆与智能钥匙的KPD认证方法，与智能钥匙对应的车辆基站设置有定时器，图1示出了该方法的流程示意图，该方法可以包括：

[0046] S101:通过低频向智能钥匙发送已加密编码的身份认证信息，并且启动定时器。

[0047] S102:判断定时器的时间是否到达设定时间，当定时器的时间到达设定时间时，转入步骤S103;否则，不执行任何操作。

[0048] S103:通过低频向智能钥匙发送低频载波以向智能钥匙发起位置认证。

[0049] S104:接收智能钥匙通过高频发送的认证结果，其中，认证结果包括:智能钥匙对

身份认证信息进行解密解码得到的身份认证结果，以及测量低频载波的场强所得到的测量结果。

[0050] S105：根据身份认证结果和测量结果判断智能钥匙的身份和位置是否均合法，当智能钥匙的身份和位置均合法时，执行步骤 S106；否则，不执行任何操作。

[0051] S106：执行相关操作，例如：解锁车门、启动车辆等。

[0052] 本发明实施例一提供的车辆与智能钥匙的 KPD 认证方法中，车辆基站设置有定时器，当车辆基站通过低频向智能钥匙发送身份认证信息时，启动定时器，在定时器的时间到达设定时间时，车辆基站通过低频向智能钥匙发送低频载波发起位置认证，而不用像现有技术那样，车辆基站在接收到智能钥匙通过高频发送的身份认证结果后，才向智能钥匙发送低频载波发起位置认证。与现有技术中的 KPD 认证方法相比，本发明实施例减少了一个高频通讯过程，并且，车辆基站对身份认证结果和测量结果的判断放在一个过程，这样极大缩短了 KPD 的认证时间，减少了通讯过程中出现不稳定因素的可能性，并且，更容易在设定时间内认证成功，快速实现解锁车门、启动车辆等操作，增强了 PEPS 的实用性。

[0053] 实施例二

[0054] 本发明实施例二提供了一种车辆与智能钥匙的 KPD 认证方法，与智能钥匙对应的车辆基站设置有定时器，图 2 示出了该方法的流程示意图，该方法可以包括：

[0055] S201：通过低频向智能钥匙发送已加密编码的身份认证信息，并且启动定时器。

[0056] 其中，车辆基站通过低频向智能钥匙发送的身份认证信息可以包括：报文头、第一数据和报文尾。第一数据包括：智能钥匙 ID、随机数组、第一密文和 CRC 校验字节。第一密文为车辆基站通过将原始数据利用第一加密算法加密生成，其中，原始数据包括：智能钥匙 ID、智能钥匙密钥 SK、随机数组和密码。

[0057] S202：判断定时器的时间是否到达设定时间，当定时器的时间到达设定时间时，转入步骤 S203；否则，不执行任何操作。

[0058] 其中，本实施例中的定时器优选为 2ms 的定时器，即步骤 S102 中的设定时间可以为 2ms。本实施例并不限定设定时间可以 2ms，设定时间可根据具体情况而设定。

[0059] S203：通过低频向智能钥匙发送低频载波以向智能钥匙发起位置认证。

[0060] 其中，本实施例中的低频载波可以为正弦波。

[0061] S204：接收智能钥匙通过高频发送的认证结果，其中，认证结果包括：智能钥匙对身份认证信息进行解密解码得到的身份认证结果，以及测量低频载波的场强所得到的测量结果。

[0062] 其中，智能钥匙接收到身份认证信息后，通过 CRC 校验字节判断接收的数据是否有效，如果接收的数据有效，则将身份认证信息中的第一数据中的第一密文通过与第一加密算法对应的第一解密算法进行解密，得到解密数数据，即智能钥匙 ID、智能钥匙密钥 SK、随机数组和密码，然后将解密数据利用第二加密算法加密生成第二密文，再将身份认证结果通过高频发送给车辆基站，其中，身份认证结果包括：报文头、第二数据和报文尾，第二数据包括：智能钥匙 ID、随机数组、第二密文和 CRC 校验字节。

[0063] S205：根据身份认证结果和测量结果判断智能钥匙的身份和位置是否均合法，当智能钥匙的身份和位置均合法时，执行步骤 S206；否则，不执行任何操作。

[0064] 车辆基站接收到身份认证结果后，通过身份认证结果中的 CRC 校验字节判断接收

的数据是否有效，如果接收的数据有效，则通过与第二加密算法对应的第二解密算法进行解密，得到解密数据，将解密数据与原始数据进行比对，如果解密数据与原始数据一致，则智能钥匙身份合法。

[0065] 车辆基站接收到低频载波的场强的测量结果后，根据测量结果确定智能钥匙与车辆基站天线的距离，如果距离在预设范围内，则表明智能钥匙的位置合法。其中，预设范围可以但不限定为以某个车门为圆心的方圆 n 米的范围。

[0066] 需要说明的是，高频通讯时间通常为在 20 ～ 60ms，为了节省认证时间，本实施例中定时器的设定时间小于 20ms。

[0067] S206 ：执行相关操作，例如 ：解锁车门、启动车辆等。

[0068] 本发明实施例二提供的车辆与智能钥匙的 KPD 认证方法中，车辆基站设置有定时器，当车辆基站通过低频向智能钥匙发送身份认证信息时，启动定时器，在定时器的时间到达设定时间时，车辆基站通过低频向智能钥匙发送低频载波发起位置认证，而不用像现有技术那样，车辆基站在接收到智能钥匙通过高频发送的身份认证结果后，才向智能钥匙发送低频载波发起位置认证。与现有技术中的 KPD 认证方法相比，本发明实施例减少了一个高频通讯过程，并且车辆基站对身份认证结果和测量结果的判断放在一个过程，这样极大缩短了 KPD 的认证时间，减少了通讯过程中出现不稳定因素的可能性，并且，更容易在设定时间内认证成功，快速实现解锁车门、启动车辆等操作，增强了 PEPS 的实用性。

[0069] 实施例三

[0070] 本发明实施例三提供了一种车辆基站，该车辆基站设置有定时器，图 3 示出了该车辆基站的结构示意图，该车辆基站可以包括 ：第一发送单元 101、启动单元 102、第一判断单元 103、第二发送单元 104、接收单元 105、第二判断单元 106 和执行单元 107。其中 ：

[0071] 第一发送单元 101，用于通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证。

[0072] 启动单元 102，用于在第一发送单元 101 向智能钥匙发送身份认证信息时启动定时器。

[0073] 第一判断单元 103，用于判断定时器的时间是否到达设定时间。

[0074] 第二发送单元 104，用于当定时器的时间到达设定时间时，通过低频向智能钥匙发送低频载波以发起位置认证。

[0075] 接收单元 105，用于接收智能钥匙通过高频发送的认证结果，认证结果包括 ：智能钥匙对身份认证信息进行解密解码得到的身份认证结果，以及测量低频载波的场强所得到的测量结果。

[0076] 第二判断单元 106，用于根据身份认证结果和测量结果判断智能钥匙的身份和位置是否均合法。

[0077] 执行单元 107，用于当智能钥匙的身份和位置均合法时，执行相关操作。

[0078] 本发明实施例三提供的车辆基站设置有定时器，当车辆基站通过低频向智能钥匙发送身份认证信息时，启动定时器，在定时器的时间到达设定时间时，车辆基站通过低频向智能钥匙发送低频载波发起位置认证，而不用像现有技术那样，车辆基站在接收到智能钥匙通过高频发送的身份认证结果后，才向智能钥匙发送低频载波发起位置认证。与现有技术中相比，本发明实施例三提供的车辆基站使得 KPD 认证过程减少了一个高频通讯过程，

并且车辆基站对身份认证结果和测量结果的判断放在一个过程，这样极大缩短了 KPD 的认证时间，减少了通讯过程中出现不稳定因素的可能性，并且，更容易在设定时间内认证成功，快速实现解锁车门、启动车辆等操作，增强了 PEPS 的实用性。

[0079] 实施例四

[0080] 本发明实施例四提供了一种车辆基站，该车辆基站设置有定时器，图 4 示出了该车辆基站的结构示意图，该车辆基站可以包括：第一发送单元 201、启动单元 202、第一判断单元 203、第二发送单元 204、接收单元 205、第二判断单元 206 和执行单元 207。其中：

[0081] 第一发送单元 201，用于通过低频向智能钥匙发送已加密编码的身份认证信息以发起身份认证。进一步的，第一发送单元 201 包括：加密子单元 2011 和发送子单元 2012，其中，加密子单元 2011，用于将原始数据利用第一加密算法加密生成第一密文，发送子单元 2012，用于将包括第一密文的身份认证信息发送往智能钥匙，身份认证信息除了包括第一密文外，还包括智能钥匙 ID、随机数组和 CRC 校验字节。

[0082] 启动单元 202，用于在第一发送单元 201 向智能钥匙发送身份认证信息时启动定时器。

[0083] 第一判断单元 203，用于判断定时器的时间是否到达设定时间。

[0084] 第二发送单元 204，用于当定时器的时间到达设定时间时，通过低频向智能钥匙发送低频载波以发起位置认证。其中，定时器的设定时间小于 20ms，优选为 2ms。

[0085] 智能钥匙接收到身份认证信息后，通过 CRC 校验字节判断接收的数据是否有效，如果接收的数据有效，则将身份认证信息中的第一数据中的第一密文通过与第一加密算法对应的第一解密算法进行解密，得到解密数数据，即智能钥匙 ID、智能钥匙密钥 SK、随机数组和密码，然后将解密数据利用第二加密算法加密生成第二密文，再将身份认证结果通过高频发送给车辆基站，其中，身份认证结果包括：报文头、第二数据和报文尾，第二数据包括：智能钥匙 ID、随机数组、第二密文和 CRC 校验字节。

[0086] 接收单元 205，用于接收智能钥匙通过高频发送的认证结果，认证结果包括：智能钥匙对身份认证信息进行解密解码得到的身份认证结果，以及测量低频载波的场强所得到的测量结果。

[0087] 第二判断单元 206，用于根据身份认证结果和测量结果判断智能钥匙的身份和位置是否均合法。进一步的，第二判断单元 206 包括：第一判断子单元 2061、解密子单元 2062、第二判断子单元 2063、确定子单元 2064 和第三判断子单元 2065。第一判断子单元 2061，用于判断身份认证结果中的 CRC 校验字节判断接收的数据是否有效，解密子单元 2062，用于当接收的数据有效时，通过与第二加密算法对应的第二解密算法进行解密，得到解密数据，第二判断子单元 2063，用于判断解密数据与原始数据是否一致，如果一致则表明智能钥匙的身份合法。确定子单元 2064，用于根据测量结果确定智能钥匙与车辆基站天线的距离；第三判断子单元 2065，用于判断智能钥匙与车辆基站天线的距离是否在预设范围，如果在预设范围，则表明智能钥匙的位置合法，其中，预设范围可以为以某个车门为圆心的方圆 n 米的范围。

[0088] 执行单元 207，用于当智能钥匙的身份和位置均合法时，执行相关操作。

[0089] 本发明实施例四提供的车辆基站设置有定时器，当车辆基站通过低频向智能钥匙发送身份认证信息时，启动定时器，在定时器的时间到达设定时间时，车辆基站通过低频向

智能钥匙发送低频载波发起位置认证，而不用像现有技术那样，车辆基站在接收到智能钥匙通过高频发送的身份认证结果后，才向智能钥匙发送低频载波发起位置认证。与现有技术中相比，本实施例提供的车辆基站使得 KPD 认证过程减少了一个高频通讯过程，并且车辆基站对身份认证结果和测量结果的判断放在一个过程，这样极大缩短了 KPD 的认证时间，减少了通讯过程中出现不稳定因素的可能性，并且，更容易在设定时间内认证成功，快速实现解锁车门、启动车辆等操作，增强了 PEPS 的实用性。

[0090] 实施例五

[0091] 本发明实施例五提供了一种车辆与智能钥匙的 KPD 认证系统，图 5 示出了该系统的结构示意图，该系统可以包括：车辆基站 1 和智能钥匙 2。

[0092] 图 6 示出了本发明实施例五提供的系统实现 KPD 认证的过程：

[0093] 车辆基站 1 通过低频向智能钥匙 2 发送已加密编码的身份认证信息，并且启动定时器，当定时器的时间到达设定时间时，通过低频向智能钥匙 2 发送低频载波以发起位置认证。

[0094] 智能钥匙 2 在接收到身份认证信息时，对身份认证信息进行解密解码得到身份认证结果，并且，在接收到低频载波时，测量低频载波的场强得到测量结果，将身份认证结果和测量结果通过高频发送往车辆基站 1。

[0095] 车辆基站 1 根据身份认证结果和测量结果判断智能钥匙 2 的身份和位置是否均合法，当智能钥匙 2 的身份和位置均合法时，执行相关操作。

[0096] 本发明实施例五提供的车辆与智能钥匙的 KPD 认证系统，在车辆基站设置定时器，当车辆基站通过低频向智能钥匙发送身份认证信息时，启动定时器，在定时器的时间到达设定时间时，车辆基站通过低频向智能钥匙发送低频载波发起位置认证，而不用像现有技术那样，车辆基站在接收到智能钥匙通过高频发送的身份认证结果后，才向智能钥匙发送低频载波发起位置认证。与现有技术中相比，本发明实施例提供的系统使得 KPD 认证过程减少了一个高频通讯过程，并且车辆基站对身份认证结果和测量结果的判断放在一个过程，这样极大缩短了 KPD 的认证时间，减少了通讯过程中出现不稳定因素的可能性，并且，更容易在设定时间内认证成功，快速实现解锁车门、启动车辆等操作，增强了 PEPS 的实用性。

[0097] 为了描述的方便，描述以上装置时以功能分为各种单元分别描述。当然，在实施本发明时可以把各单元的功能在同一个或多个软件和 / 或硬件中实现。

[0098] 通过以上的实施方式的描述可知，本领域的技术人员可以清楚地了解到本发明可借助软件加必需的通用硬件平台的方式来实现。基于这样的理解，本发明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，该计算机软件产品可以存储在存储介质中，如 ROM/RAM、磁碟、光盘等，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本发明各个实施例或者实施例的某些部分所述的方法。

[0099] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述得比较简单，相关之处参见方法实施例的部分说明即可。以上所描述的系统实施例仅仅是示意性的，其中所述作为分离部件说明

的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个网络单元上。可以根据实际的需要选择其中的部分或者全部模块来实现本实施例方案的目的。本领域普通技术人员在不付出创造性劳动的情况下，即可以理解并实施。

[0100] 本发明可用于众多通用或专用的计算系统环境或配置中。例如：个人计算机、服务器计算机、手持设备或便携式设备、平板型设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络 PC、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境等等。

[0101] 本发明可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本发明，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0102] 需要说明的是，在本文中，诸如第一和第二等之类的关系术语仅仅用来将一个实体或者操作与另一个实体或操作区分开来，而不一定要求或者暗示这些实体或操作之间存在任何这种实际的关系或者顺序。

[0103] 对所公开的实施例的上述说明，使本领域专业技术人员能够实现或使用本发明。对这些实施例的多种修改对本领域的专业技术人员来说将是显而易见的，本文中所定义的一般原理可以在不脱离本发明的精神或范围的情况下，在其它实施例中实现。因此，本发明将不会被限制于本文所示的这些实施例，而是要符合与本文所公开的原理和新颖特点相一致的最宽的范围。

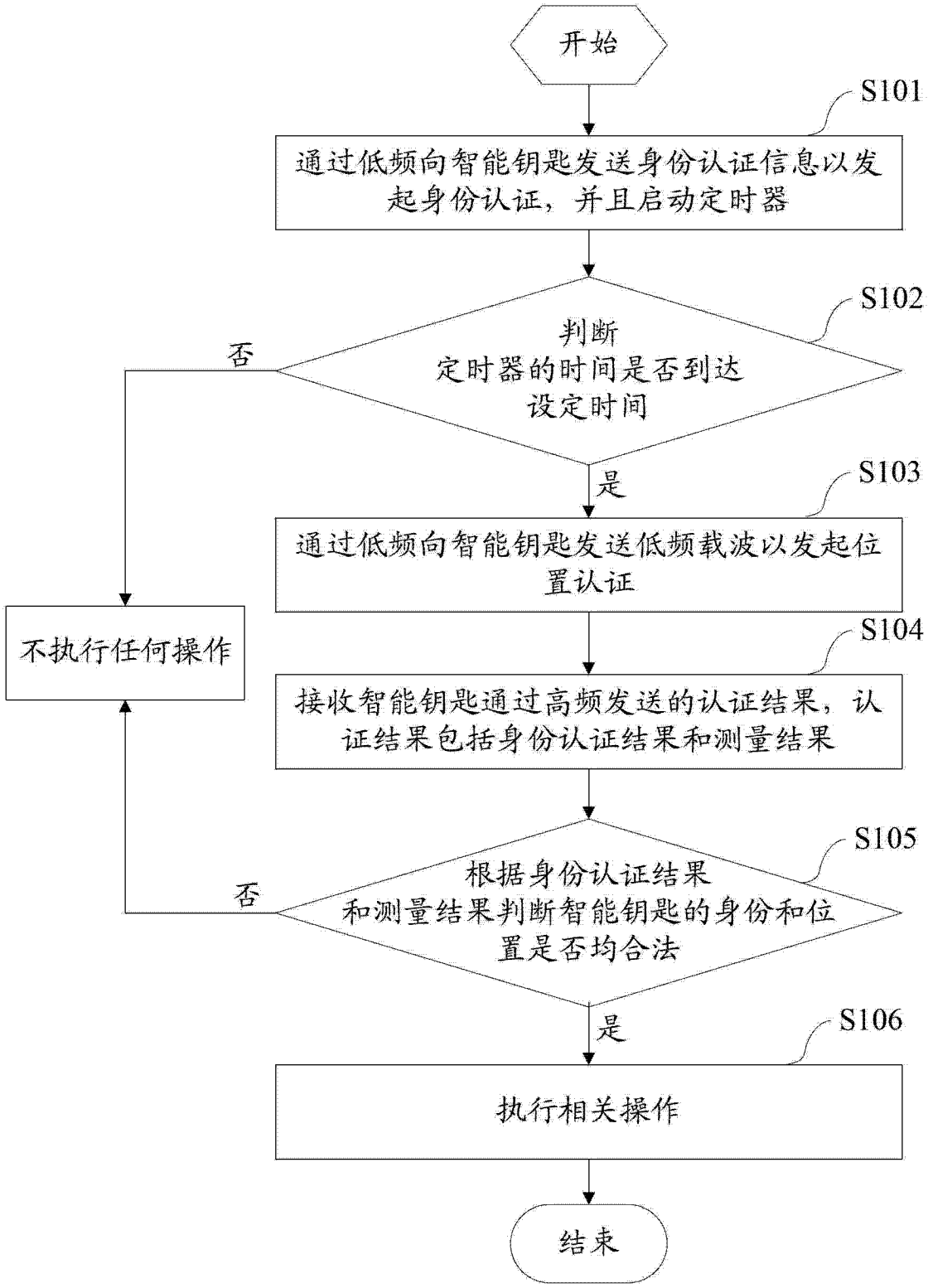

开始
S101
通过低频向智能钥匙发送身份认证信息以发起身份认证，并且启动定时器
S102
判断
定时器的时间是否到达
设定时间
否
是
S103
通过低频向智能钥匙发送低频载波以发起位置认证
不执行任何操作
S104
接收智能钥匙通过高频发送的认证结果，认证结果包括身份认证结果和测量结果
S105
根据身份认证结果
和测量结果判断智能钥匙的身份和位置是否均合法
否
是
S106
执行相关操作
结束

图 1

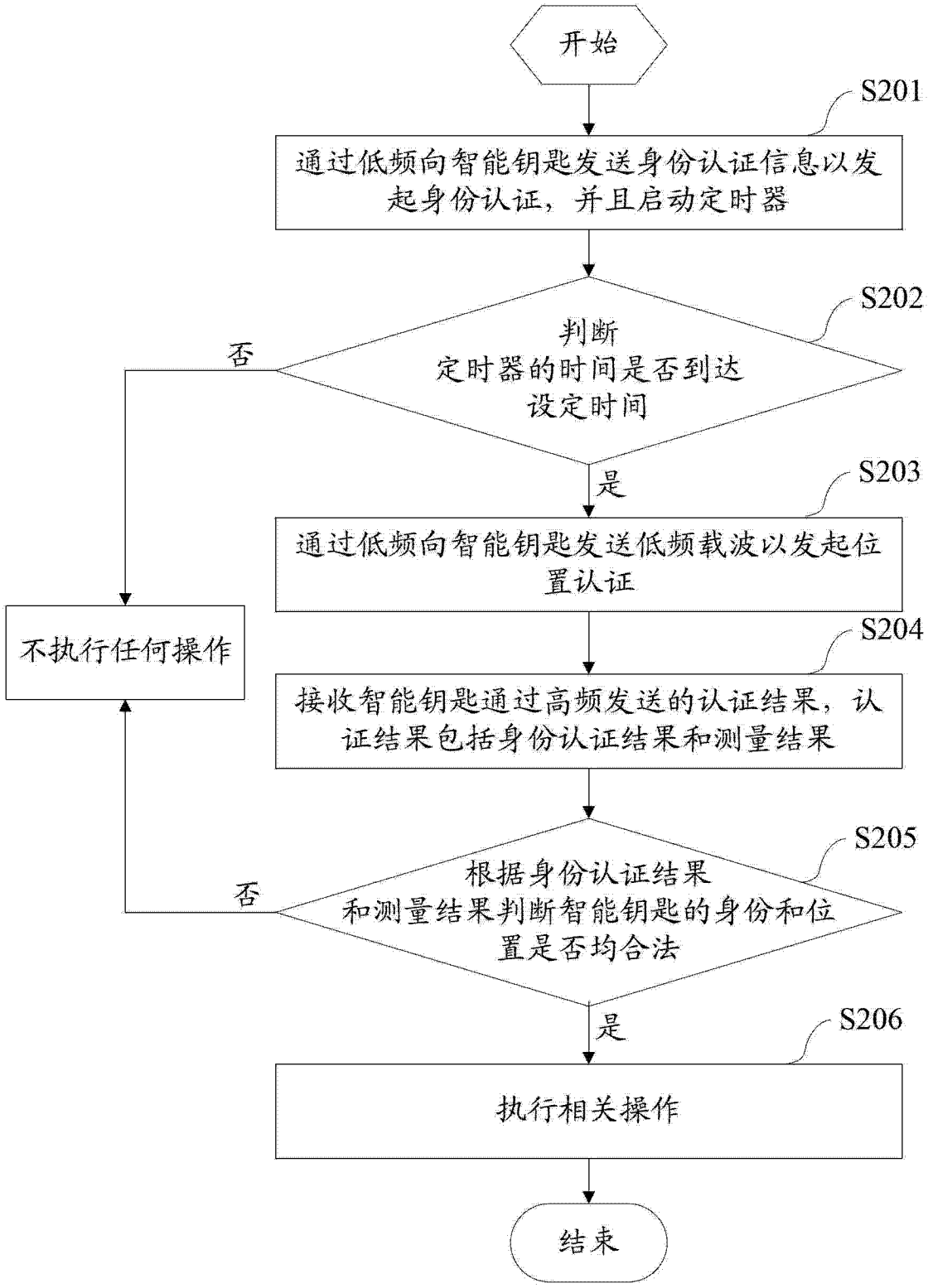

开始
S201
通过低频向智能钥匙发送身份认证信息以发起身份认证，并且启动定时器
S202
判断
定时器的时间是否到达
设定时间
否
是
S203
通过低频向智能钥匙发送低频载波以发起位置认证
不执行任何操作
S204
接收智能钥匙通过高频发送的认证结果，认证结果包括身份认证结果和测量结果
S205
根据身份认证结果
和测量结果判断智能钥匙的身份和位置是否均合法
否
是
S206
执行相关操作
结束

图 2

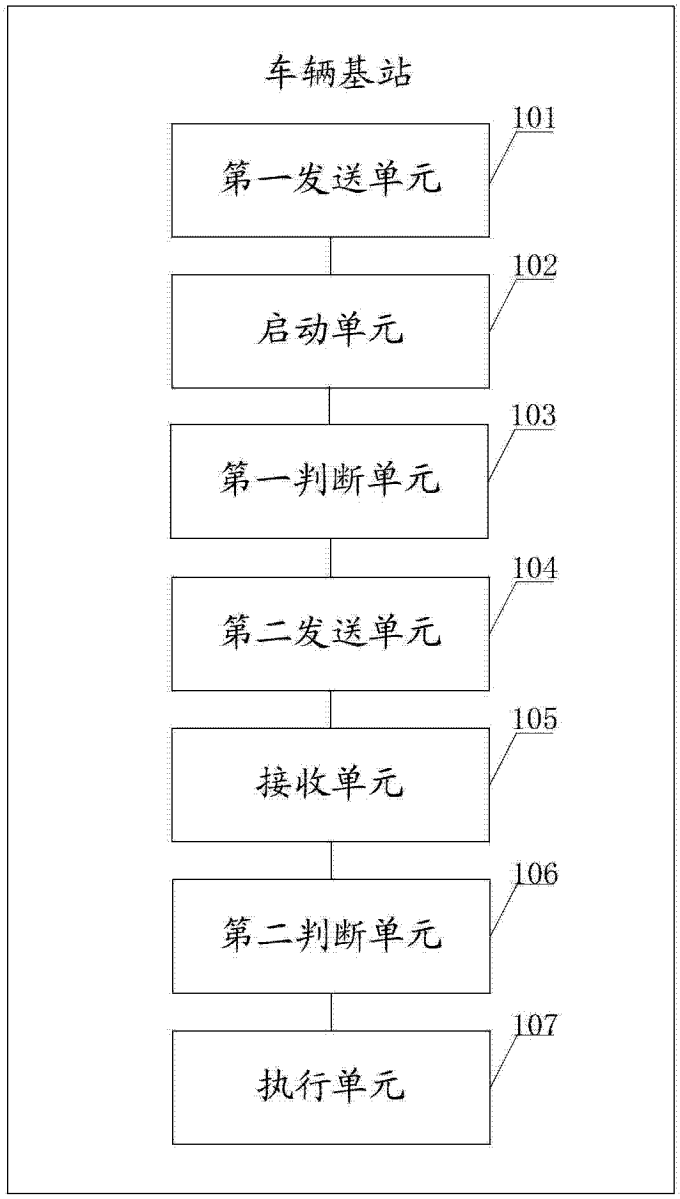

车辆基站
101
第一发送单元
102
启动单元
103
第一判断单元
104
第二发送单元
105
接收单元
106
第二判断单元
107
执行单元

图 3

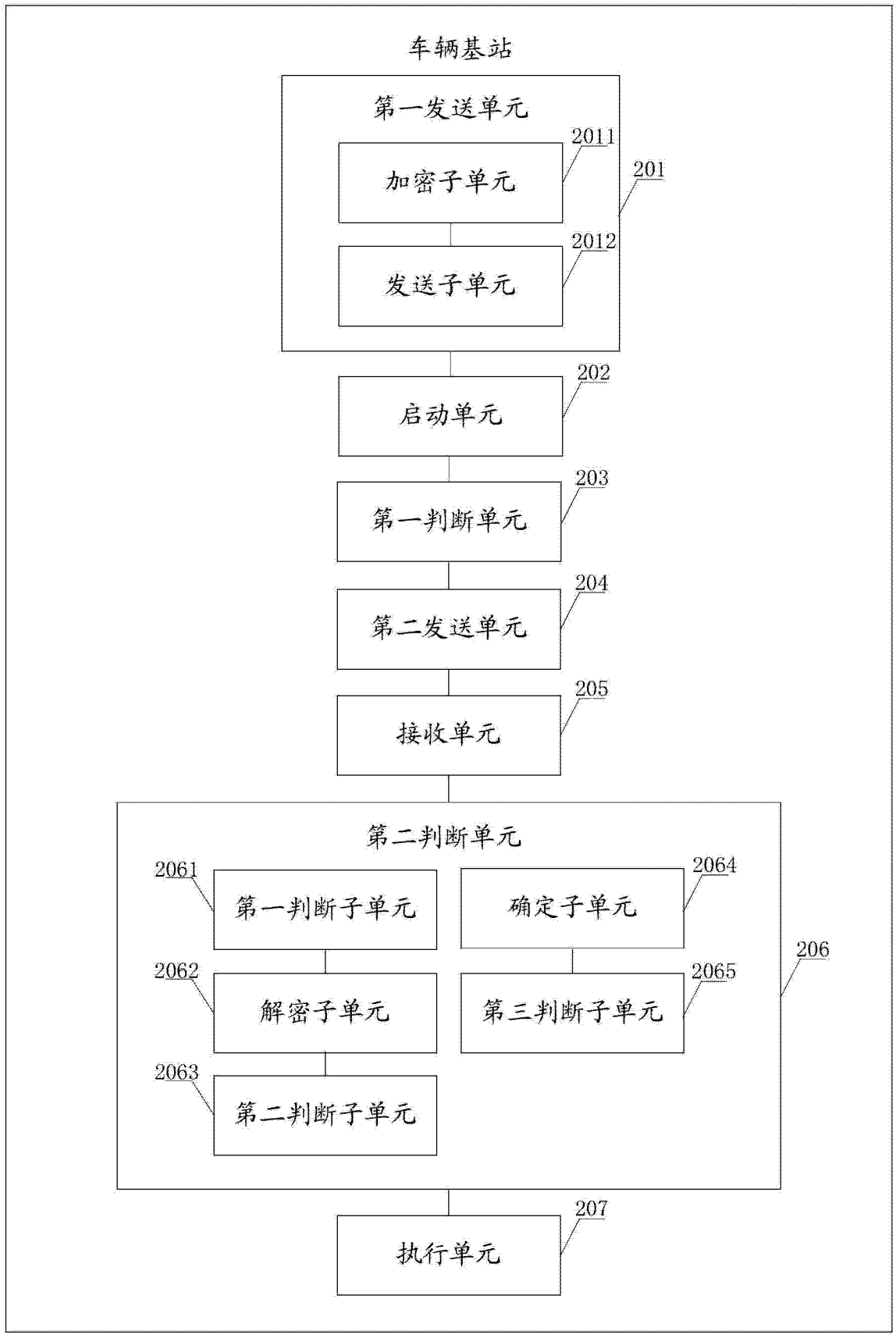

车辆基站
第一发送单元
2011
加密子单元
201
2012
发送子单元
202
启动单元
203
第一判断单元
204
第二发送单元
205
接收单元
第二判断单元
2061
第一判断子单元
2064
确定子单元
206
2062
解密子单元
2065
第三判断子单元
2063
第二判断子单元
207
执行单元

图 4

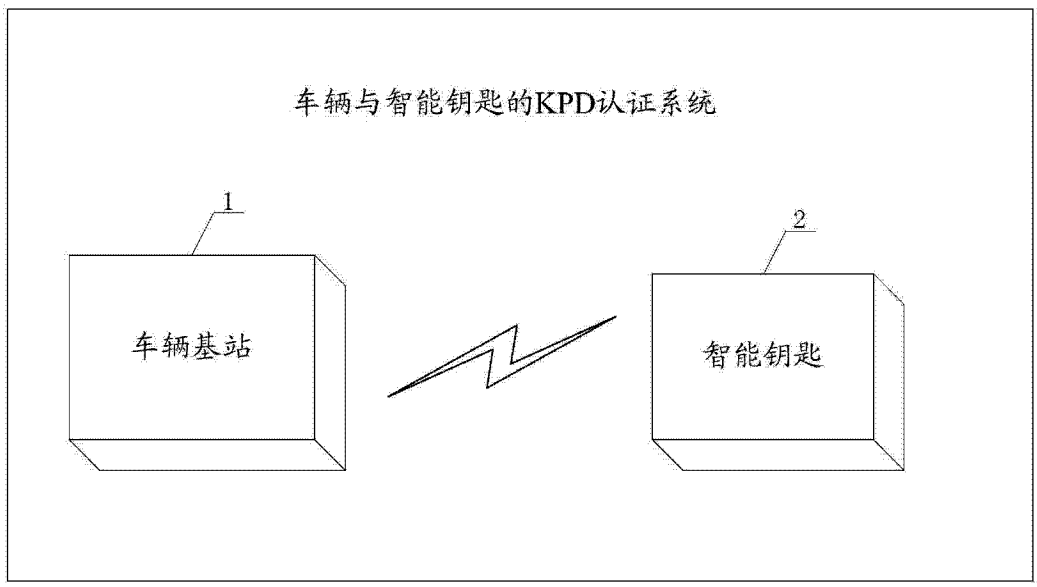


图 5

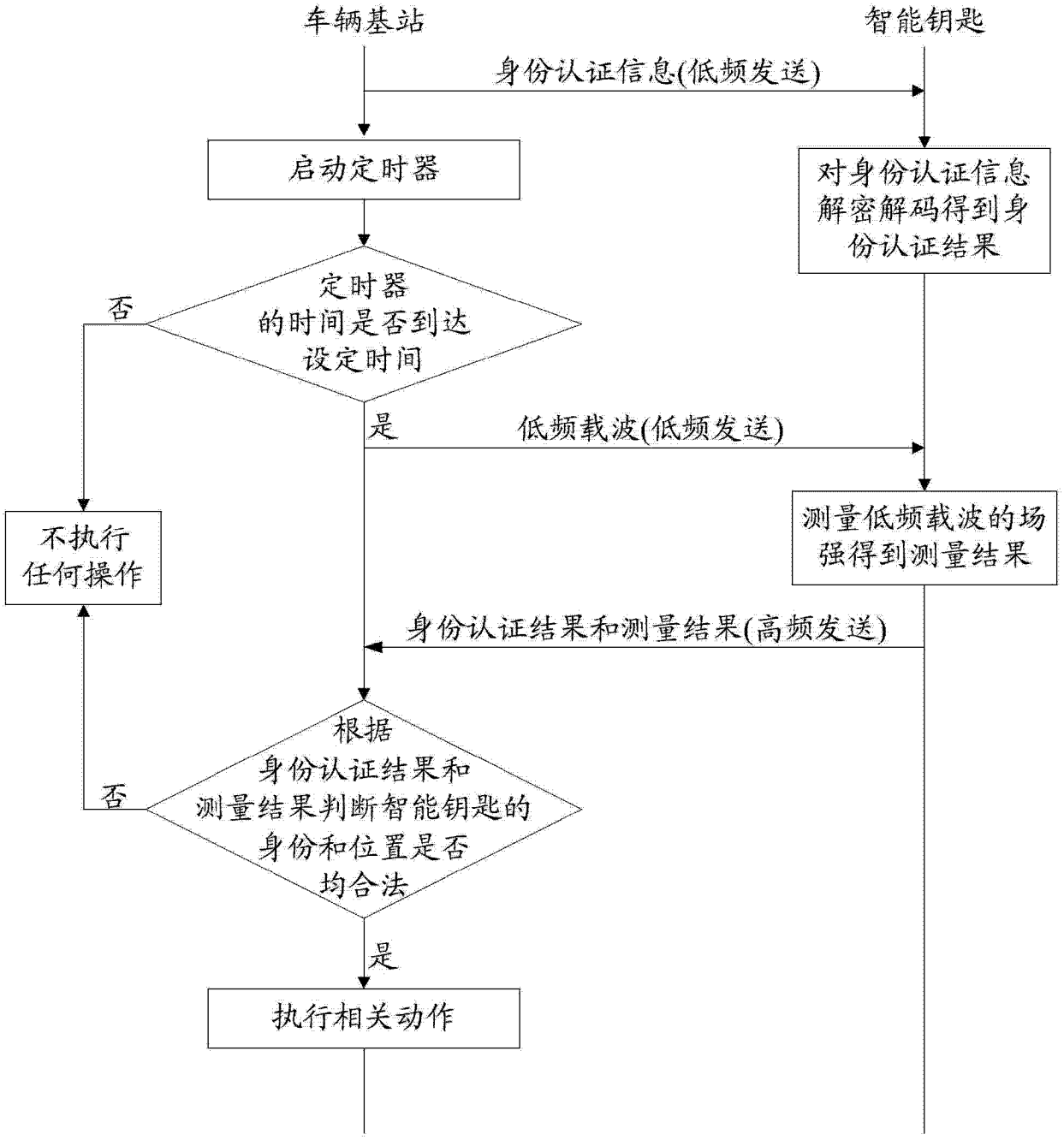

车辆基站
智能钥匙
身份认证信息(低频发送)
启动定时器
对身份认证信息解密解码得到身份认证结果
定时器的时间是否到达设定时间
否
是
低频载波(低频发送)
不执行任何操作
测量低频载波的场强得到测量结果
身份认证结果和测量结果(高频发送)
根据身份认证结果和测量结果判断智能钥匙的身份和位置是否均合法
否
是
执行相关动作

图 6