

(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 2 月 11 日 (11.02.2021)



(10) 国际公布号
WO 2021/023095 A1

(51) 国际专利分类号:
G07C 9/00 (2020.01)

(21) 国际申请号: PCT/CN2020/105912

(22) 国际申请日: 2020 年 7 月 30 日 (30.07.2020)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201910712929.X 2019年8月2日 (02.08.2019) CN

(71) 申请人: 华为技术有限公司 (HUAWEI TECHNOLOGIES CO., LTD.) [CN/CN]; 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(72) 发明人: 王思善 (WANG, Sishan); 中国广东省深圳市龙岗区坂田华为总部办公楼, Guangdong 518129 (CN)。

(74) 代理人: 北京弘权知识产权代理事务所 (普通合伙) (CHINABLE IP); 中国北京市朝阳区安定路35号六层35-10-2内620室, Beijing 100029 (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,

(54) Title: METHOD FOR DETECTING RELAY ATTACK BASED ON COMMUNICATION CHANNELS AND DEVICE

(54) 发明名称: 基于通信通道检测中继攻击的方法及设备

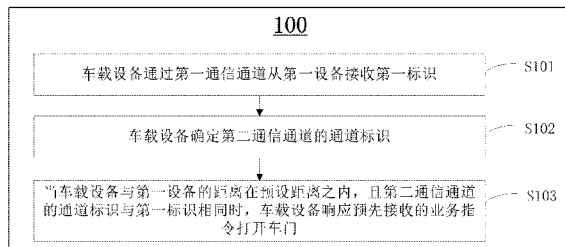


图 3A

S101 A vehicle-mounted device receives a first identifier from a first device by means of a first communication channel
S102 The vehicle-mounted device determines a channel identifier of a second communication channel
S103 When the distance between the vehicle-mounted device and the first device is within a preset distance, and the channel identifier of the second communication channel is the same as the first identifier, the vehicle-mounted device opens a vehicle door in response to a pre-received service instruction

(57) Abstract: A method for detecting a relay attack based on communication channels and a device. A vehicle-mounted device is connected to a first device by means of a first communication channel and a second communication channel, and the first communication channel and the second communication channel are independent to each other. The vehicle-mounted device receives a first identifier from the first device by means of the first communication channel, a communication channel identified by the first identifier being of the same type as the second communication channel. Then, the vehicle-mounted device determines a channel identifier of the second communication channel. Since the communication channel identified by the first identifier is of the same type as the second communication channel, when the channel identifier of the second communication channel is matched with the first identifier, it is indicated that the second communication channel and the communication channel identified by the first identifier are the same communication channel, and furthermore, it is indicated that there is no relay attack. On this basis, when the distance between the vehicle-mounted device and the first device is within a preset distance, the vehicle-mounted device can open a vehicle door in response to a service instruction.

(57) 摘要: 一种基于通信通道检测中继攻击的方法及设备, 其中, 车载设备与第一设备通过第一通信通道和第二通信通道连接, 第一通信通道和第二通信通道相互独立。车载设备通过第一通信通道从第一设备接收第一标识, 第一标识所标识的通信通道与第二通信通道的类型相同。然后, 车载设备确定第二通信通道的通道标识。由于第一标识所标识的通信通道与第二通信通道的类型相同, 所以, 当第二通信通道的通道标识与第一标识匹配, 说明第二通信通道与第一标识所标识的通信通道是同一条通信通道, 进而说明不存在中继攻击。基于此, 车载设备与第一设备的距离在预设距离之内时, 车载设备可以响应业务指令打开车门。

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))。

基于通信通道检测中继攻击的方法及设备

技术领域

本申请涉及通信技术领域，尤其涉及一种基于通信通道检测中继攻击的方法及设备。

5 背景技术

被动无钥匙进入与启动 (passive entry passive start, PEPS) 系统是目前应用在汽车上的常用系统。PEPS 系统包括电子钥匙设备和车载设备，其中，电子钥匙设备可以被用户携带，车载设备可以被内置在汽车中。在实际应用中，车载设备向电子钥匙设备发送业务请求，电子钥匙设备响应该业务请求生成业务指令，该业务指令中携带密钥生成的鉴权数据。车载设备从电子钥匙设备接收到该业务指令以及验证密钥通过，并确定该电子钥匙设备距离该车载设备的距离在预设距离内之后，该车载设备根据密钥控制汽车的门锁打开。

基于 PEPS 系统的工作原理，若在车载设备和电子钥匙设备之间设置中继设备，该中继设备能够将车载设备发送的业务请求指令转发到电子钥匙设备，然后，将电子钥匙设备发送的业务指令转发到车载设备。这样能够在车载设备和电子钥匙设备之间的距离大于预设距离的场景下，使得车载设备被触发打开汽车的门锁。可见，现有 PEPS 系统的安全性较差。

发明内容

本申请提供了一种基于通信通道检测中继攻击的方法及设备，以解决现有 PEPS 系统安全性差的问题。

第一方面，本申请提供了一种基于通信通道检测中继攻击的方法，所述方法应用于车载设备端。其中，车载设备与第一设备通过第一通信通道和第二通信通道连接，第一通信通道和第二通信通道相互独立。本实施例中，车载设备中维护第二通信通道的通道标识确定规则，车载设备可以通过第一通信通道从第一设备接收第一标识，该第一标识用于标识与第二通信通道类型相同的通信通道。然后，车载设备可以确定第二通信通道的通道标识，进而，检测第二通信通道的通道标识与第一标识是否匹配。当车载设备与第一设备的距离在预设距离之内，且第二通信通道的通道标识与第一标识匹配时，车载设备响应预先接收的业务指令打开车门。其中，车载设备预先接收的业务指令的实施例详见下文描述，此处不再详述。

其中，该第一标识根据通道标识确定规则生成，且第一标识用于标识与第二通信通道类型相同的通信通道。进而，车载设备可以通过比对所计算的通道标识和所接收的通道标识是否相同，确定车载设备和电子钥匙设备之间是否被中继攻击。可见，采用本实现方式，该车载设备可以根据通道标识确定车载设备和电子钥匙设备之间是否被中继攻击，并在不存在中继攻击的场景下，响应业务指令打开车门，从而能够提高 PEPS 系统的安全性。

一种可能的实现方式中，第一通信通道可以是业务数据通道，也可以是测距通道，其中，业务数据通道用于传输业务数据，测距通道用于传输测距数据，业务数据通道例如是蓝牙通道，测距通道例如是 UWB 通道。基于此，当第一通信通道是业务数据通道时，车载设备可以通过该业务数据通道从第一设备接收会话密文，该会话密文中包含测距通道标识，测距通道标识用于标识所述测距通道，测距通道标识例如是 UWB 通道标识。相应的，当第一通信通道是测距通道时，车载设备可以通过该测距通道从第一设备接收测距确认字符 ACK 帧，测距 ACK 帧中包含业务数据通道标识，业务数据通道标识用于标识业务数据通道，业务数据通道标识例如是蓝牙通道标识。采用本实现方式，建立两条相互独立的通信通道对应

关系的方式较为灵活，从而能够为车载设备检测是否存在中继攻击提供信息依据。

一种可能的实现方式中，会话密文是将测距通道标识加密得到的。例如，测距通道标识是 UWB 通道标识，业务数据通道例如是蓝牙通道，那么，UWB 通道标识可以以蓝牙会话密文的形式传输。采用本实现方式，能够防止该测距通道标识被仿冒和篡改，从而提高检测的准确性，进而，能够提高 PEPS 系统的安全性。

一种可能的实现方式中，结合上述可能的实现方式，当第二通信通道是业务数据通道时，由于业务数据通道包含该业务数据通道特有的物理通道信息，例如，业务数据通道的传输频段、时域信息、频域信息、多径延迟信息、信号强度、信号相位等，所以，车载设备可以根据第一规则提取该第二通信通道的一项或多项物理特征信息作为该第二通信通道的通道信息，然后，可以根据该第二通信通道的通道信息生成第二通信通道的业务数据通道标识，该业务数据通道标识能够唯一标识第二通信通道。相应的，当第二通信通道是测距通道时，测距通道可以包括测距通道的通用唯一识别码 UUID、测距通道地址、测距通道的会话标识、测距通道会话的前导序列和测距帧返回的时间戳等物理特征信息，基于此，车载设备可以根据第二规则获取第二通信通道的通道信息中的指定信息作为第二通信通道的测距通道标识。其中，第一规则用于指示车载设备确定业务数据通道标识，第二规则用于指示车载设备确定测距通道标识，指定信息是指被指定作为测距通道标识的物理特征信息。

其中，业务数据通道的通道信息是该业务通道的物理特征信息，且不同物理通道具备不同的物理特征，所以，每条业务数据通道对应唯一的业务数据通道标识。相应的，作为测距通道标识的指定信息，是测距通道的唯一信息，所以，每条测距通道也对应唯一的测距通道标识。可见，每条通信通道对应唯一的通道标识，基于此，采用本实现方式，车载设备能够根据通道标识检测是否被中继攻击。

一种可能的实现方式中，车载设备在确定第二通信通道的通道标识之后，在打开车门之前，还需要检测第二通信通道的通道标识和第一标识是否匹配。根据上述描述，一些实施例中，当第二通信通道的通道标识和第一标识是业务数据通道标识时，由于受到天气等因素的影响，业务数据通道的物理特征信息会发生变化，因此，即使业务数据通道未被中继攻击，电子钥匙设备端生成的第一标识与车载设备根据生成标识也可能不同，但是相似度相对较高。所以，本实施例中，车载设备可以检测第二通信通道的通道标识与第一标识的相似度参数是否大于预设阈值，若第二通信通道的通道标识与第一标识的相似度参数大于预设阈值，则确定第二通信通道的通道标识与第一标识相匹配。其中，相似度参数指示第二通信通道的通道标识与第一标识的相似程度，相似度参数越小，说明第二通信通道的通道标识与第一标识的相似程度越小，相似度参数越大，说明第二通信通道的通道标识与第一标识的相似程度越高。所以，采用本实现方式，车载设备可以根据两业务数据通道标识的相似度参数，检测是否被中继攻击。另一些实施例中，当第二通信通道的通道标识和第一标识是测距通道标识时，车载设备检测第二通信通道的通道标识与第一标识相同，则确定第二通信通道的通道标识与所述第一标识相匹配。示例性的，测距通道标识例如是前导序列，由于前导序列可以唯一标识测距通道，基于此，采用本实现方式，车载设备可以根据所接收的前导序列与所提取的本端的前导序列是否相同，确定是否被中继攻击。

一种可能的实现方式中，车载设备可以与第一设备先建立业务数据通道，然后，车载设备可以通过该业务数据通道接收业务指令，然后，车载设备再与第一设备建立与测距通道。采用本实现方式，车载设备能够在确定存在合法业务指令的情况下，对第一设备进行测距，从而能够减少测距产生的资源消耗。

第二方面，本申请提供了一种基于通信通道检测中继攻击的方法，该方法同样应用于车载设备端。本实施例中，车载设备中预置第一规则和第二规则，进而，车载设备可以从第一设备接收业务指令，该业务指令包含第一业务数据通道标识和第一测距通道标识，第一业务数据通道标识用于标识电子钥匙设

备所连接的业务数据通道,第一测距通道标识用于标识电子钥匙设备所连接的测距通道。然后,车载设备可以确定第二业务数据通道标识和第二测距通道标识,第二业务数据通道标识用于标识车载设备所连接的业务数据通道,第二测距通道标识用于标识车载设备所连接的测距通道。进而,车载设备可以检测第一业务数据通道标识与第二业务数据通道标识是否匹配,且第一测距通道标识和第二测距通道标识是否相同。当车载设备与第一设备的距离在预设距离之内,第一业务数据通道标识和第二业务数据通道标识相匹配,且第一测距通道标识和第二测距通道标识相同时,车载设备才响应业务指令打开车门。

本实施例中,车载设备和电子钥匙设备中均预置第一规则和第二规则,进而,车载设备在接收到电子钥匙设备生成的两通道标识之后,可以生成本端对应的两个通道标识,进而,车载设备可以根据两对通道标识的匹配关系,检测是否存在中继攻击,并在不存在中继攻击的场景下,响应业务指令打开车门。可见,采用本实现方式,该车载设备可以根据通道标识确定车载设备和电子钥匙设备之间是否被中继攻击,并在不存在中继攻击的场景下,响应业务指令打开车门,从而能够提高 PEPS 系统的安全性。

第三方面,本申请提供了一种基于通信通道检测中继攻击的方法,所述方法应用于电子钥匙设备端,所述方法与第一方面所述的方法相对应。其中,本实施例中,电子钥匙设备例如与第二设备通过第一通信通道和第二通信通道连接,第一通信通道和第二通信通道相互独立。然后,电子钥匙设备可以生成第一标识,进而,通过所述第一通信通道向所述第二设备发送所述第一标识。进而,触发车载设备执行第一方面的方法。其中,关于第一标识的描述详见第一方面所述,此处不再赘述。

其中,电子钥匙设备使用第二通信通道的通道标识确定规则生成第一标识,并使用第一通信通道传输第二通信通道的通道标识,从而能够建立第一通信通道和第二通信通道的对应关系。采用本实现方式,能够便于车载设备根据通信通道验证对端设备是否是电子钥匙设备,进而,使得车载设备在不存在中继攻击的情况下,响应业务指令打开车门,从而能够提高 PEPS 系统的安全性。

一种可能的实现方式中,电子钥匙设备生成第一标识包括:当第二通信通道是业务数据通道时,业务数据通道包含该业务数据通道特有的物理通道信息,电子钥匙设备可以根据第一规则提取该第二通信通道的一项或多项物理特征信息作为该第二通信通道的通道信息,然后,根据该第二通信通道的通道信息生成第二通信通道的业务数据通道标识。当第二通信通道是测距通道时,电子钥匙设备可以根据第二规则获取第二通信通道的通道信息中的指定信息作为第一标识。其中,电子钥匙设备生成第一标识的方法,与第一方面所述的车载设备生成第二通信通道的通道标识的方法相同。此外,业务数据通道的含义,测距通道的含义,业务数据通道标识的含义,以及测距通道的含义均如第一方面所述,此处不再详述。

一种可能的实现方式中,结合上述可能的实现方式,当第一标识是业务数据通道标识时,电子钥匙设备可以将业务数据通道标识携带在测距确认字符 ACK 帧中,并通过测距通道发送测距 ACK 帧。其中,测距 ACK 帧是电子钥匙设备对第二设备发送的测距帧的应答帧,第二设备可以根据测距帧和每个测距 ACK 帧计算与电子钥匙设备的距离。当第一标识是测距通道标识时,电子钥匙设备可以将测距通道标识加密得到会话密文,然后,通过业务数据通道发送会话密文。例如,测距通道标识是 UWB 通道标识,业务数据通道例如是蓝牙通道,那么,电子钥匙设备可以对 UWB 通道标识加密得到蓝牙会话密文,然后,通过蓝牙通道将该会话密文发送到第二设备。采用本实现方式,建立两条相互独立的通信通道对应关系的方式较为灵活,从而能够为车载设备检测是否存在中继攻击提供信息依据。此外,通过将测距通道标识加密得到会话密文,能够防止该测距通道标识被仿冒和篡改,从而提高检测的准确性,进而,能够提高 PEPS 系统的安全性。

一种可能的实现方式中,若第一通信通道是业务数据通道,电子钥匙设备可以在与第二设备建立第一通信通道之后,通过该业务数据通道向第二设备发送业务指令,以便于车载设备验证业务指令的合法

性，然后，电子钥匙设备再与第二设备建立测距通道。采用本实现方式，使得车载设备在确定存在合法业务指令的情况下进行测距，从而能够减少测距产生的资源消耗。

第四方面，本申请提供了一种基于通信通道检测中继攻击的方法，所述方法同样应用于电子钥匙设备端，所述方法与第三方面所述的方法相对应。本实施例中，电子钥匙设备端预置第一规则和第二规则，进而，在与第二设备建立业务数据通道和测距通道之后，电子钥匙设备可以根据第一规则确定第一业务数据通道标识，并根据第二规则确定第一测距通道标识，第一业务数据通道标识用于标识业务数据通道，第一测距通道标识用于标识测距通道，然后，电子钥匙设备可以生成业务指令，该业务指令包括第一业务数据通道标识和第一测距通道标识，然后，电子钥匙设备通过业务数据通道向第二设备发送业务指令。进而，触发车载设备执行第三方面的方法。

本实施例中，车载设备和电子钥匙设备中均预置第一规则和第二规则，进而，电子钥匙设备可以确定本端所连接的两条通信通道的通道标识，然后，将该两个通道标识携带在业务指令中发送到车载设备端，从而触发车载设备根据该两个通道标识，检测是否存在中继攻击，并在不存在中继攻击的场景下，响应业务指令打开车门。可见，采用本实现方式，该车载设备可以根据通道标识确定车载设备和电子钥匙设备之间是否被中继攻击，并在不存在中继攻击的场景下，响应业务指令打开车门，从而能够提高 PEPS 系统的安全性。

第五方面，本申请还提供了一种车载设备，该车载设备具有实现上述方法中车载设备行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，上述车载设备的结构中包括处理器和收发器，所述处理器被配置为处理该终端设备执行上述方法中相应的功能。所述收发器用于实现上述车载设备与电子钥匙设备之间的通信。所述车载设备还可以包括存储器，所述存储器用于与处理器耦合，其保存该车载设备必要的程序指令和数据。

第六方面，本申请还提供了一种电子钥匙设备，该电子钥匙设备具有实现上述方法中电子钥匙设备行为的功能。所述功能可以通过硬件实现，也可以通过硬件执行相应的软件实现。所述硬件或软件包括一个或多个与上述功能相对应的模块。在一个可能的设计中，上述电子钥匙设备的结构中包括处理器和收发器，所述处理器被配置为处理该电子钥匙设备执行上述方法中相应的功能。所述收发器用于实现上述电子钥匙设备与车载设备之间的通信。所述电子钥匙设备还可以包括存储器，所述存储器用于与处理器耦合，其保存该电子钥匙设备必要的程序指令和数据。

第七方面，本申请还提供了一种芯片，所述芯片包括处理器和接口，所述接口与所述处理器耦合，所述处理器用于执行计算机程序或指令，并实现第一方面、第二方面或第一方面任意可能的设计中的基于通信通道检测中继攻击的方法。

第八方面，本申请还提供了一种芯片，所述芯片包括处理器和接口，所述接口与所述处理器耦合，所述处理器用于执行计算机程序或指令，并实现第三方面、第四方面或第三方面任意可能的设计中的基于通信通道检测中继攻击的方法。

第九方面，本申请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中存储有指令，当其在计算机上运行时，使得计算机执行第一方面、第二方面、第三方面、第四方面、第一方面任意可能的设计中或第三方面任意可能的设计中的方法。

为提高 PEPS 系统的安全性，本申请提供的车载设备和电子钥匙设备中预设通道标识确定规则，进而，在通信过程中，电子钥匙设备使用该通道标识确定规则生成通道标识，并发送到该电子钥匙设备的对端设备。该通道标识是电子钥匙设备当前连接的通信通道的标识。相应的，车载设备从该车载设备的

对端设备接收通道标识之后,根据该通道标识确定规则生成车载设备所接收的通信通道的通道标识,进而,车载设备通过检测所接收的通道标识与车载设备生成的通道标识是否相匹配,来确定该车载设备与该电子钥匙设备之间是否存在中继攻击,进而,确定是否打开车门。

附图说明

5 为了更清楚地说明本申请的技术方案,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,对于本领域普通技术人员而言,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。

图 1A 是本申请提供的一种 PEPS 系统的示例性场景示意图;

图 1B 是本申请提供的一种中继攻击的示例性场景示意图;

10 图 2A 是本申请提供的一种移动交通工具通信系统 10 的示例性系统架构图;

图 2B 是本申请提供的一种车载设备 100 的示例性功能结构图;

图 2C 是本申请提供的一种电子钥匙设备 200 的示例性功能结构图;

图 3A 是本申请提供的基于通信通道检测中继攻击的方法 100 的示例性方法流程图;

图 3B 是本申请提供的基于通信通道检测中继攻击的方法 200 的示例性方法流程图;

15 图 3C 是本申请提供的基于通信通道检测中继攻击的方法 300 的示例性方法流程图;

图 3D 是本申请提供的基于通信通道检测中继攻击的方法 400 的示例性方法流程图;

图 4A 是本申请提供的基于通信通道检测中继攻击的方法 500 的示例性信令交互图;

图 4B 是本申请提供的基于通信通道检测中继攻击的方法 600 的示例性信令交互图;

图 4C 是本申请提供的基于通信通道检测中继攻击的方法 700 的示例性信令交互图;

20 图 4D 是本申请提供的基于通信通道检测中继攻击的方法 800 的示例性信令交互图;

图 4E 是本申请提供的中继攻击场景下的通信信道示意图;

图 5A 是本申请提供的车载设备 50 的示例性结构示意图;

图 5B 是本申请提供的车载设备 51 的示例性结构示意图;

图 6A 是本申请提供的电子钥匙设备 60 的示例性结构示意图;

25 图 6B 是本申请提供的电子钥匙设备 61 的示例性结构示意图。

具体实施方式

下面将结合本申请中的附图,对本申请的技术方案进行清楚地描述。

30 本申请以下实施例中所使用的术语只是为了描述特定实施例的目的,而并非旨在作为对本申请的限制。如在本申请的说明书和所附权利要求书中所使用的那样,单数表达形式“一个”、“一种”、“所述”、“上述”、“该”和“这一”旨在也包括复数表达形式,除非其上下文中明确地有相反指示。还应当理解,尽管在以下实施例中可能采用术语第一、第二等来描述某一类对象,但所述对象不应限于这些术语。这些术语仅用来将该类对象的具体对象进行区分。例如,以下实施例中可能采用术语第一、第二等来描述通道标识,但通道标识不应限于这些术语。这些术语仅用来将指示不同通信通道的标识进行区分。以下实施例中可能采用术语第一、第二等来描述的其他类对象同理,此处不再赘述。

35 以下对本申请的实施场景进行描述。

图 1A 示出了一种被动无钥匙进入与启动(passive entry passive start, PEPS)系统的示例性场景示意图,如图 1A 所示,PEPS 系统中的车载设备与电子钥匙设备例如可以建立业务数据通道,车载设备与电子钥匙设备使用该业务数据通道传输业务数据。车载设备和电子钥匙设备之间例如还可以建立测距通道,车载设备可以通过该测距通道与电子钥匙设备传输测距数据,该测距数据用于车载设备检测与

电子钥匙设备的距离。当车载设备根据测距通道的测距数据确定车载设备与电子钥匙设备的距离在预设距离内时，车载设备中的汽车控制模块根据所接收的业务数据执行开门操作。其中，测距通道和业务数据通道相互独立，并且，车载设备与电子钥匙设备使用业务数据通道传输业务数据的同时，车载设备与电子钥匙设备依然在使用测距通道传输测距数据。

5 本申请所涉及的 PEPS 系统是移动交通工具的通信系统。该通信系统具有无钥匙进入与启动的功能。该通信系统包括通过无线连接的车载设备和电子钥匙设备。

本申请所涉及的车载设备可以被设置在移动交通工具中。该车载设备可以被配置为具备无线通讯功能的一个或者多个服务器，或者一个或者多个天线模组、处理器等。

10 本申请所涉及的电子钥匙设备可以被配置为独立的设备，也可以被配置为搭载电子钥匙相关应用程序的其他电子设备。该电子设备例如包括手机、平板电脑、具备无线通讯功能的可穿戴电子设备（如智能手表）等。便携式电子设备的示例性实施例包括但不限于搭载 iOS®、Android®、Microsoft® 或者其它操作系统的便携式电子设备。上述便携式电子设备也可以是其它便携式电子设备，诸如具有触敏表面或触控面板的膝上型计算机（laptop）等。还应当理解的是，在其他一些实施例中，上述电子设备也可以不是便携式电子设备，而是具有触敏表面或触控面板的台式计算机。

15 示例性的，业务数据通道是用于传输业务数据的通道，业务数据例如可以包括业务请求和业务指令，业务数据通道可以但不限于是蓝牙通道。测距通道是用于传输测距数据的通道，测距数据例如可以包括测距帧和测距确认字符（acknowledgement, ACK）帧，测距通道可以但不限于是使用超宽带（ultra wide band, UWB）模块建立的 UWB 通道。预设距离例如是 2 米到 10 米。

20 本申请涉及的中继攻击是指，中继设备通过攻击手段放大车载设备和电子钥匙设备之间的距离。即，在车载设备和电子钥匙设备之间的距离大于预设距离的场景下，中继设备将业务指令从电子钥匙设备中转发到车载设备，以在车载设备和电子钥匙设备距离较远时，通过攻击手段打开车门的操作。例如，预设距离是 2 米，即车载设备和电子钥匙设备之间的距离小于或者等于 2 米时，车载设备响应业务指令打开车门。但是，一种示例性场景下，车载设备和电子钥匙设备之间的距离是 10 米，中继设备与车载设备之间的距离是 2 米，中继设备可以将业务指令从电子钥匙设备转发到车载设备，进而触发车载设备
25 打开车门。

可以理解的是，业务数据通道和测距通道是相互独立的两条通信通道，所以，只有当图 1A 中示意的蓝牙通道和测距通道所连接均是电子钥匙设备时，车载设备和电子钥匙设备才没有被中继攻击。若图 1A 中示意的蓝牙通道连接电子钥匙设备，但是测距通道所连接的是其他设备时，则蓝牙通道已经被中继攻击。

30 例如，一种中继攻击的场景如图 1B 所示，车载设备和电子钥匙设备之间加入了中继设备，该中继设备例如可以与车载设备建立测距通道和第一业务数据通道，并与电子钥匙设备建立第二业务数据通道。然后，该中继设备通过第一业务数据通道接收车载设备发送的业务请求，并将该业务请求通过第二业务数据通道发送到电子钥匙设备，进而，该中继设备通过第二业务数据通道接收电子钥匙设备发送的业务指令，并将该业务指令通过第一业务数据通道发送到车载设备。基于此，只要该中继设备与车载设备之间的距离在预设距离之内，即可触发车载设备打开车门，导致 PEPS 系统的安全性较差。

35 需要说明的是，虽然图 1B 中的中继设备与车载设备和电子钥匙设备分别通过两条业务数据通道传输业务数据，但是从逻辑层面讲，业务数据依然由车载设备和电子钥匙设备之间以业务数据包的形式交互，中继设备并未与车载设备和电子钥匙设备建立实际的配对关系，中继设备通过转发业务数据包的方式，延长了电子钥匙设备和车载设备之间进行数据交互的作用范围。基于此，图 1B 中示意的“第一业

务数据通道”和“第二业务数据通道”是指中继设备分别与车载设备和电子钥匙设备之间的两条通信通道，且该两条通信通道在本申请实施场景中起到业务数据通道功能。此外，本申请其他实施例中涉及的中继设备所连接的业务数据通道均是该含义，本申请下文相关的实施例对此将不再赘述。

为提高 PEPS 系统的安全性，本申请提供了一种基于通信通道检测中继攻击的方法及设备。本申请
5 中车载设备能够根据通信通道的标识检测当前 PEPS 系统是否安全（即，当前 PEPS 系统是否被中继攻击），进而，在确定 PEPS 系统安全之后，车载设备打开交通工具的门锁，从而能够提高 PEPS 系统的安全性。

以下对本申请的系统框架进行描述。

图 2A 示意了一种移动交通工具通信系统 10 的示例性系统架构图。其中，通信系统 10 包括交通工具 12、一个或多个无线载波系统 14、地面通信网络 16、计算机 18 以及呼叫中心 20。应该理解的是，
10 所公开的方法能够与任何数量的不同系统一起使用，并不特定地限于此处示出的运行环境。同样，系统 10 的架构、构造、设置和运行以及它的单独部件在现有技术中通常是已知的。因此，以下的段落仅仅简单地提供了一个示例通信系统 10 的概述，本文没有示出的其它系统也能够使用所公开的方法。

交通工具 12 可实现在汽车上或可采取汽车的形式。然而，示例系统还可实现在其它车辆上或采取其它车辆的形式，诸如轿车、卡车、摩托车、公交车、船、飞机、直升机、割草机、铲雪车、休旅车、
15 游乐园车辆、农业设备、施工设备、有轨电车、高尔夫球车、火车和电车等其它车辆。此外，机器人装置也可用于执行本文描述的方法和系统。

一些交通工具电子件 28 在图 2A 中示出，包括信息通讯单元 30、麦克风 32、一个或多个按钮 34 或者其它控制输入、音频系统 36、可视显示器 38、以及全球定位系统（global position system, GPS）模块 40 和多个交通工具安全单元（vehicle security module, VSM）42。这些设备中的一些能够直接
20 连接到信息通讯单元，例如麦克风 32 和按钮 34，而其它的使用一个或多个网络连接实现间接连接，例如通信总线 44 或者娱乐总线 46。合适的网络连接的实例包括控制器局域网（controller area network, CAN）、媒体导向系统转移（media oriented systems transport, MOST）、局部互联网络（local interconnect network, LIN）、局域网（local area network, LAN）以及其它合适的连接，例如以太网或者符合已知的国际标准化组织（international organization for standardization, ISO）、美国
25 机动车工程师学会（society of automotive engineers, SAE）和国际电气与电子工程师学会（institute of electrical and electronics engineers, IEEE）标准和规定的其它连接，这仅仅列举一小部分。

信息通讯单元 30 可以是原始设备制造商（original equipment manufacturer, OEM）安装（嵌入）或者配件市场设备，它安装在交通工具中，且能够在无线载波系统 14 上且经无线联网进行无线声音和/
30 或数据通信。这能使交通工具与呼叫中心 20、其它启用信息通讯的交通工具、或者一些其它实体或者设备通信。信息通讯单元优选地使用无线电广播来与无线载波系统 14 建立通信通道（声音信道和/或数据信道），使得声音和/或数据传输能够在信道上被发送和接收。通过提供声音和数据通信，信息通讯单元 30 能使交通工具提供多种不同的服务，包括与导航、电话、紧急救援、诊断、信息娱乐等相关联的那些服务。数据能够经数据连接（例如经数据信道上的分组数据传输，或者经使用现有技术中已知技术的
35 的声音信道）被发送。对于包括声音通信（例如，在呼叫中心 20 处具有现场顾问 live advisor 或者声音响应单元）和数据通信（例如，提供 GPS 位置数据或者车辆诊断数据至呼叫中心 20）两者的组合服务，系统可利用在声音信道上的单个呼叫，并根据需要在声音信道和在声音和数据传输之间切换，这可以使用本领域技术人员已知的技术来完成。此外，可使用短消息服务 SMS 发送和接收数据（例如，分组数据协议（packet data protocol, PDP））；信息通讯单元可被配置为移动终止和/或发起，或者被配置为应

用终止和/或发起。

信息通讯单元 30 根据全球移动通信系统 (global system for mobile communication, GSM) 或者码分多址 (code division multiple access, CDMA) 标准利用蜂窝通信, 因此包括用于声音通信 (例如免提呼叫) 的标准蜂窝芯片集、用于数据传输的无线调制解调器、电子处理设备 52、一个或多个数字存储器设备 54 以及双天线 56。应该明白, 调制解调器能够通过存储在信息通讯单元内的软件实施且由处理器 52 执行, 或者它能够是位于信息通讯单元 30 内部或者外部的分开的硬件部件。调制解调器能够使用任何数量的不同标准或者协议 (例如 EVDO (CDMA20001xEV-D0, EVDO)、CDMA、通用分组无线服务技术 (general packet radio service, GPRS) 和增强型数据速率 GSM 演进技术 (enhanced data rate for GSM evolution, EDGE)) 来运行。交通工具和其它联网设备之间的无线联网也能够使用信息通讯单元 30 来执行。为此目的, 信息通讯单元 30 能够被配置为根据一个或多个无线协议 (例如, IEEE 802.11 协议、全球微波互联接入 (worldwide interoperability for microwave access, WiMAX) 或者蓝牙中的任何一种) 无线通信。当用于例如传输控制协议/因特网互联协议 (transmission control protocol/internet protocol, TCP/IP) 的分组交换数据通信时, 信息通讯单元能够被配置具有静态 IP 地址, 或者能够被设置以从网络上的另一个设备 (例如路由器) 或者从网络地址服务器自动接收所分配的 IP 地址。

处理器 52 可以是能够处理电子指令的任何类型的设备, 包括微处理器、微控制器、主处理器、控制器、交通工具通信处理器、以及专用集成电路 (application specific integrated circuit, ASIC)。它能够是仅用于信息通讯单元 30 的专用处理器或者能够与其它交通工具系统共享。处理器 52 执行各种类型的数字存储指令, 例如存储电子钥匙设备 200 发送的第一标识。处理器 52 还能够执行程序或者处理数据, 例如, 执行本说明书下文所述的基于通信通道检测中继攻击的方法实施例中的检测操作。

信息通讯单元 30 能够被用于提供不同范围的交通工具服务, 包括与来自交通工具其他部分的无线通信。这样的服务包括: 转向指引 (turn-by-turn direct ins) 以及与基于 GPS 的交通工具导航模块 40 结合提供的其它导航相关联的服务; 安全气囊部署通知以及与一个或多个碰撞传感器接口模块 (例如主体控制模块 (未图示)) 结合提供的其它紧急或路边救援相关联的服务。使用一个或多个诊断模块的诊断报告。以及信息娱乐相关联的服务, 其中音乐、网页、电影、电视节目、视频游戏和/或其它信息被信息娱乐模块下载, 并被存储用于当前或稍后回放。以上列出的服务决不是信息通讯单元 30 的所有能力的详尽列表, 而仅仅是信息通讯单元能够提供的一些服务的列举。此外, 应该理解, 至少一些上述模块能够以存储在信息通讯单元 30 内部或外部的软件指令的形式实施, 它们可以是位于信息通讯单元 30 内部或外部的硬件部件, 或者它们可以是彼此集成的和/或共享的, 或者与位于整个交通工具中的其它系统集成和/或共享, 这仅列举几种可能性。位于信息通讯单元 30 外部的 VSM 42 在工作的情况下, 它们可利用交通工具通信总线 44 与信息通讯单元 30 交换数据和命令。

GPS 模块 40 从 GPS 卫星 60 接收无线电信号。从这些信号, GPS 模块 40 能够确定交通工具的位置, 该交通工具的位置被用于给交通工具驾驶者提供导航和其它位置相关联的服务。导航信息能够被呈现在显示器 38 上 (或者交通工具内的其它显示器) 或者能够用语言呈现, 例如当提供转向导航时完成。能够使用专用的交通工具内的导航模块 (可以是 GPS 模块 40 的一部分) 来提供导航服务, 或者一些或全部导航服务可以经信息通讯单元 30 来完成, 其中位置信息被发送到远程位置, 以便于为交通工具提供导航地图、地图标注 (感兴趣的点、餐馆等)、路线计算等等。位置信息能够被提供给呼叫中心 20 或者其它远程计算机系统, 例如计算机 18, 以用于其它的目的, 例如车队管理。并且, 新的或者更新的地图数据能够经信息通讯单元 30 从呼叫中心 20 下载至 GPS 模块 40。

除了音频系统 36 和 GPS 模块 40 之外, 交通工具 12 能够包括电子硬件部件形式的其它交通工具安全模块 VSM 42, 其它交通工具安全模块 VSM42 位于整个交通工具中, 通常从一个或多个传感器接收输入, 并使用所感测到的输入来执行诊断、监测、控制、报告和/或其它功能。VSM 42 中的每一个优选地通过通信总线 44 连接到其它 VSM, 也连接到信息通讯单元 30, 并且能够被编程以运行交通工具系统和

5 子系统诊断测试。例如, 一个 VSM 42 能够是控制发动机运行的各方面(例如, 燃料点火和点火时间)的发动机控制模块(engine control module, ECM), 另一个 VSM 42 能够是调节交通工具的动力传动系的一个或多个部件的运行的动力传动系控制模块, 且另一个 VSM 42 能够是管理位于整个交通工具中的各个电部件(如同交通工具的电动门锁和前灯)的主体控制模块。根据一个实施例, 发动机控制模块装备有车载诊断(on board diagnostics, OBD)特征, 车载诊断特征提供大量实时数据, 例如从各种传感器

10 (包括交通工具排放传感器)接收的数据, 并提供标准化系列的诊断故障代码(DTS), 诊断故障代码允许技术人员快速地识别和维修交通工具内的故障。如本领域的技术人员所明白的, 以上提及的 VSM 仅仅是可以在交通工具 12 内使用的一些模块的实例, 许多其它的模块也是可能的。

交通工具电子件 28 还包括多个交通工具用户接口, 为交通工具司乘人员提供了提供和/或接收信息的装置, 包括麦克风 32、按钮 34、音频系统 36 和可视显示器 38。如在本文所使用的, 术语“交通工具用户接口”广泛地包括任何合适形式的电子设备, 包括硬件和软件部件, 该电子设备位于交通工具上, 且能使交通工具用户与交通工具的部件通信或者通过交通工具的部件通信。麦克风 32 提供了至信息通讯单元的音频输入, 以能使驾驶者或者其他司乘人员提供声音命令, 并执行经无线载波系统 14 的免提保护叫。为此目的, 它能够连接到车载自动化声音处理单元, 车载自动化声音处理单元利用现有技术中已知的人机接口(human machine interface, HMI)技术。按钮 34 允许手动用户输入至信息通讯单元 30,

15 以发起无线电话呼叫和提供其它数据、响应或者控制输入。分开的按钮能够被用于发起紧急呼叫以及常规服务求助呼叫至呼叫中心 20。音频系统 36 提供音频输出至交通工具司乘人员且能够是专用的单机系统或者主交通工具音频系统的一部分。根据此处所示的具体实施例, 音频系统 36 可运行地联接到交通工具总线 44 和娱乐总线 46, 且能够提供调幅(amplitude modulation, AM)、调频(frequency modulation, FM)和卫星广播、数字多功能光盘(digital versatile disc, DVD)和其它多媒体功能。这个功能能够与以上描述的信息娱乐模块结合提供或者独立提供。可视显示器 38 优选地是图形显示器, 例如仪表盘上的触摸屏或者从挡风玻璃反射的抬头显示器, 且能够被用于提供多种输入和输出功能。各种其它交通工具用户接口也能够被利用, 因为图 2A 中的接口仅仅是一种具体实施方案的实例。

20

25

无线载波系统 14 优选地是蜂窝电话系统, 包括多个蜂窝塔 70 (仅示出一个)、一个或多个移动交换中心(mobile switching center, MSC)72 以及将无线载波系统 14 与地面网络 16 连接所要求的任何其它的联网部件。每个蜂窝塔 70 包括发送和接收天线以及基站, 来自不同蜂窝塔的基站直接连接到 MSC 72 或者经中间装置(例如基站控制器)连接到 MSC 72。蜂窝系统可实施任何合适的通信技术, 包括例如模拟技术(例如模拟移动通信系统(advanced mobile phone system, AMPS))或者更新的数字技术(例如 CDMA (例如 CDMA2000)或 GSM/GPRS)。如本领域的技术人员将会明白的, 各种蜂窝塔/基站/MSC 设置都是可能的, 且可与无线载波系统 14 一起使用。例如, 基站和蜂窝塔能够共同位于相同的地点, 或者它们能够彼此定位较远, 每个基站能够响应单个的蜂窝塔或者单个基站能够服务各个蜂窝塔, 各个基站能够联接到单个 MSC, 这仅仅列举一小部分可能的设置。

30

35

除了使用无线载波系统 14 之外, 卫星通信形式的不同无线载波系统能够被用于提供与交通工具的单向或者双向通信。这能够使用一个或多个通信卫星 62 和上行链路发射站 64 来完成。单向通信能够是例如卫星广播服务, 其中节目内容(新闻、音乐等)被发射站 64 接收、打包用于上传、且接下来发送到

卫星 62，卫星 62 将节目广播到用户。双向通信能够是例如使用卫星 62 在交通工具 12 和站 64 之间中继电话通信的卫星电话服务。如果使用，这种卫星电话能够被附加到无线载波系统 14 或者代替无线载波系统 14 使用。

地面网络 16 可以是常规的陆基无线电通信网络，它连接到一个或多个固定电话，并将无线载波系统 14 连接到呼叫中心 20。例如，地面网络 16 可包括公共交换电话网络(public switched telephone network, PSTN)，例如被用于提供有线电话、分组交换数据通信以及互联网基础设施的 PSTN。地面网络 16 的一个或多个部分能够通过使用标准的有线网络、光纤或者其它光学网络、电缆网络、电力线、其它无线网络(例如无线局域网(wireless local area networks, WLAN))、或者提供宽带无线访问(broadband wireless access, BWA)的网络及其任何组合来实施。地面网络 16 还可以包括用于存储、上传、转换和/或在发送者和接收者之间传输短消息(short message service, SMS)的一个或多个短消息服务中心(short message service center, SMSC)。例如，SMSC 可以从呼叫中心 20 或者内容提供商(例如，外部短消息实体或者 ESME)接收 SMS 消息，且 SMSC 可以将 SMS 消息传输给交通工具 12 (例如，移动终端设备)。SMSC 和它们的功能对于技术人员来说是已知的。此外，呼叫中心 20 不必经地面网络 16 连接，但是可以包括无线电话设备，使得它能够直接与无线网络(例如无线载波系统 14)通信。

计算机 18 能够是多个计算机中的一个，这多个计算机可经私人或者公共网络(例如互联网)访问。每个这样的计算机 18 都能够被用于一个或多个目的，例如交通工具可经信息通讯单元 30 和无线载波系统 14 访问网页服务器。其它这样的可访问计算机 18 能够是例如：服务中心计算机，其中诊断信息和其它交通工具数据能够经信息通讯单元 30 从交通工具上传；交通工具所有者或者其他用户为例如如下目的而使用的客户端计算机：访问或者接收交通工具数据，或者设置或配置用户参数，或者控制交通工具的功能；或者第三方库，无论是通过与交通工具 12 还是呼叫中心 20 通信，或者与两者通信，交通工具数据或其它信息被提供至或者来自该第三方库。计算机 18 还能够被用于提供互联网连接，例如域名服务器(domain name server, DNS)服务，或者作为使用动态主机配置协议(dynamic host configuration protocol, DHCP) 或者其它合适的协议来分配 IP 地址给交通工具 12 的网络地址服务器。

呼叫中心 20 被设计以提供多种不同的系统后端功能给交通工具电子件 28，并且根据在此示出的示例性实施例，呼叫中心 20 通常包括一个或多个交换机 80、服务器 82、数据库 84、现场顾问 86、以及自动声音响应系统(automatic voice response system, VRS) 88，它们在现有技术中全部都是已知的。这些各种呼叫中心部件优选地经有线或者无线局域网彼此联接。交换机 80 能够是专用交换分机(private branch exchange, PBX)，路由进入的信号，使得声音传输通常通过普通电话发送到现场顾问 86 或者使用 VoIP 发送到自动声音响应系统 88。现场顾问电话也能够使用网络语音电话业务(voice over internet phone, VoIP)，如图 2A 中的虚线所指示。VoIP 和通过交换机 80 的其它的数据通信经连接在交换机 80 和网络 90 之间的调制解调器(未图示)来实施。数据传输经调制解调器传递到服务器 82 和/或数据库 84。数据库 84 能够存储账户信息，例如用户身份验证信息、交通工具标识符、数据图表(profile)记录、行为模式以及其它有关的用户信息。数据传输也可以由无线系统来执行，例如 802.11x, GPRS 等等。此外，可使用短消息服务(SMS)发送和/或接收数据(例如，PDP)；且呼叫中心 20 可被配置为移动终止和/或发起，或者被配置为应用终止和/或发起。虽然所阐述的实施例已经被描述为它将会与使用现场顾问 86 的有人控制的呼叫中心 20 一起使用，但是将会明白呼叫中心可代替使用 VRS 88 作为自动顾问，或者 VRS 88 和现场顾问 86 的组合可以被使用。

图 2B 示意了本申请提供的一种车载设备 100 的示例性功能结构图。车载设备 100 耦合到图 2A 示意的移动交通工具中，车载设备 100 可包括传感器系统 101、控制系统 102、外围设备 103、电源 104、计

算装置 105 以及用户接口 106。计算装置 105 可包括处理器 1051 和存储器 1052。计算装置 105 可以是车载设备 100 的控制器或控制器的一部分。存储器 1052 可包括处理器 1051 可运行的指令 1053，并且还可存储地图数据 1054。车载设备 100 的组件可被配置为以与彼此互连和/或与耦合到各系统的其它组件互连的方式工作。例如，电源 104 可向车载设备 100 的所有组件提供电力。计算装置 105 可被配置为从传感器系统 101、控制系统 102 和外围设备 103 接收数据并对它们进行控制。例如，计算装置 105 可以从传感器系统 101 接收测距数据，并根据该测距数据计算测距结果，然后，计算装置 105 可以将测距结果发送到控制系统 102，以触发控制系统 102 执行后续操作。计算装置 105 可被配置为在用户接口 106 上生成图像的显示并从用户接口 106 接收输入。

在其它示例中，车载设备 100 可包括更多、更少或不同的系统，并且每个系统可包括更多、更少或不同的组件。此外，示出的系统和组件可以按任意种的方式进行组合或划分。

传感器系统 101 可包括用于感测关于车载设备 100 所位于的环境的信息的若干个传感器。如图所示，传感器系统的传感器包括 GPS 模块 1011、惯性测量单元 (inertial measurement unit, IMU) 1012、无线电检测和雷达测距 (RADAR) 单元 1013、激光测距 (LIDAR) 单元 1014、相机 1015、用于为修改传感器的位置和/或朝向的致动器 1016 以及 (一个或多个) UWB 模块 1017。示例性的，传感器系统 101 用于通过 UWB 模块 1017 向 UWB 模块 2031 发送测距帧，并从 UWB 模块 2031 接收测距 ACK 帧，然后，传感器系统 101 可以将相关的测距数据发送到计算装置 105，以触发计算装置 105 计算测距结果。计算装置 105 可以根据一个或多个 UWB 模块的测距数据和定位算法对车辆进行定位，并生成测距结果。传感器系统 101 也可包括额外的传感器，包括例如监视车辆 100 的内部系统的传感器 (例如，监视器、燃油量表、机油温度，等等)。传感器系统 101 也可以包括其它传感器。

GPS 模块 1011 可以为用于估计交通工具的地理位置的任何传感器。为此，GPS 模块 1011 可能包括收发器，基于卫星定位数据，估计车载设备 100 相对于地球的位置。在示例中，计算装置 105 可用于结合地图数据 1054 使用 GPS 模块 1011 来估计交通工具可在其上行驶的道路上的车道边界的位置。GPS 模块 1011 也可采取其它形式。

IMU 1012 可以是用于基于惯性加速度及其任意组合来感测交通工具的位置和朝向变化。在一些示例中，传感器的组合可包括例如加速度计和陀螺仪。传感器的其它组合也是可能的。

RADAR 单元 1013 可以被看作物体检测系统，其用于使用无线电波来检测物体的特性，诸如物体的距离、高度、方向或速度。RADAR 单元 1013 可被配置为传送无线电波或微波脉冲，其可从波的路线中的任何物体反弹。物体可将波的一部分能量返回至接收器 (例如，碟形天线或天线)，该接收器也可以是 RADAR 单元 1013 的一部分。RADAR 单元 1013 还可被配置为对接收到的信号 (从物体反弹) 执行数字信号处理，并且可被配置为识别物体。

其它类似于 RADAR 的系统已用在电磁波谱的其它部分上。一个示例是 LIDAR (光检测和测距)，其可使用来自激光的可见光，而非无线电波。

LIDAR 单元 1014 包括传感器，该传感器使用光感测或检测交通工具所位于的环境中的物体。通常，LIDAR 是可通过利用光照射目标来测量到目标的距离或目标的其它属性的光学遥感技术。作为示例，LIDAR 单元 1014 可包括被配置为发射激光脉冲的激光源和/或激光扫描仪，和用于为接收激光脉冲的反射的检测器。例如，LIDAR 单元 1014 可包括由转镜反射的激光测距仪，并且以一维或二维围绕数字化场景扫描激光，从而以指定角度间隔采集距离测量值。在示例中，LIDAR 单元 1014 可包括诸如光 (例如，激光) 源、扫描仪和光学系统、光检测器和接收器电子器件之类的组件，以及位置和导航系统。

在示例中，LIDAR 单元 1014 可被配置为使用紫外光 (UV)、可见光或红外光对物体成像，并且可用

于广泛的目标,包括非金属物体。在一个示例中,窄激光波束可用于以高分辨率对物体的物理特征进行地图绘制。

在示例中,从约 10 微米(红外)至约 250 纳米(UV)的范围中的波长可被使用。光通常经由后向散射被反射。不同类型的散射被用于不同的 LIDAR 应用,诸如瑞利散射、米氏散射和拉曼散射以及荧光。基于不同种类的后向散射,作为示例,LIDAR 可因此被称为瑞利激光 RADAR、米氏 LIDAR、拉曼 LIDAR 以及钠/铁/钾荧光 LIDAR。波长的适当组合可允许例如通过寻找反射信号的强度的依赖波长的变化对物体进行远程地图绘制。

使用扫描 LIDAR 系统和非扫描 LIDAR 系统两者可实现三维(3D)成像。“3D 选通观测激光 RADAR(3D gated viewing laser radar)”是非扫描激光测距系统的示例,其应用脉冲激光和快速选通相机。成像 LIDAR 也可使用通常使用互补金属氧化物半导体(complementary metal oxide semiconductor, CMOS)和混合互补金属氧化物半导体/电荷耦合器件(charge coupled device, CCD)制造技术在单个芯片上构建的高速检测器阵列和调制敏感检测器阵列来执行。在这些装置中,每个像素可通过以高速解调或选通来被局部地处理,以使得阵列可被处理成表示来自相机的图像。使用此技术,可同时获取上千个像素以创建表示 LIDAR 单元 1014 检测到的物体或场景的 3D 点云。

点云可包括 3D 坐标系统中的一组顶点。这些顶点例如可由 X、Y、Z 坐标定义,并且可表示物体的外表面。LIDAR 单元 1014 可被配置为通过测量物体的表面上的大量点来创建点云,并可点云作为数据文件输出。作为通过 LIDAR 单元 1014 的对物体的 3D 扫描过程的结果,点云可用于识别并可视化物体。

在一个示例中,点云可被直接渲染以可视化物体。在另一示例中,点云可通过可被称为曲面重建的过程被转换为多边形或三角形网格模型。用于将点云转换为 3D 曲面的示例技术可包括德洛内三角剖分、阿尔法形状和旋转球。这些技术包括在点云的现有顶点上构建三角形的网络。其它示例技术可包括将点云转换为体积距离场,以及通过移动立方体算法重建这样定义的隐式曲面。

相机 1015 可以用于获取交通工具所位于的环境的图像的任何相机(例如,静态相机、视频相机等)。为此,相机可被配置为检测可见光,或可被配置为检测来自光谱的其它部分(诸如红外光或紫外光)的光。其它类型的相机也是可能的。相机 1015 可以是二维检测器,或可具有三维空间范围。在一些示例中,相机 1015 例如可以是距离检测器,其被配置为生成指示从相机 1015 到环境中的若干点的距离的二维图像。为此,相机 1015 可使用一种或多种距离检测技术。例如,相机 1015 可被配置为使用结构光技术,其中车辆 100 利用预定光图案,诸如栅格或棋盘格图案,对环境中的物体进行照射,并且使用相机 1015 检测从物体的预定光图案的反射。基于反射的光图案中的畸变,车载设备 100 可被配置为检测到物体上的点的距离。预定光图案可包括红外光或其它波长的光。

致动器 1016 例如可被配置为修改传感器的位置和/或朝向。传感器系统 101 可额外地或可替换地包括除了所示出的那些以外的组件。

UWB 模块 1017 可以用于向电子钥匙设备 200 中的 UWB 模块 2031(详见图 2C 示意的电子钥匙设备的结构图)发送测距帧,然后,UWB 模块 1017 接收 UWB 模块 2031 发送的应答帧。进而,UWB 模块 1017 根据测距帧中的时间戳和应答帧中的时间戳确定交通工具和电子钥匙设备 200 的距离。

控制系统 102 可被配置为控制车载设备 100 及其组件的操作。为此,控制系统 102 可包括制动单元 1023、传感器融合算法 1024、计算机视觉系统 1025、导航或路线控制(pathing)系统 1026 以及避障系统 1027。控制系统 102 还可以被配置为获取计算装置 105 传输的距离计算结果,进而,在该距离计算结果指示的距离在预设距离之内时,控制交通工具的门打开或启动交通工具的发动机。

制动单元 1023 可以是配置为使车载设备 100 减速的机构的任意组合。例如，制动单元 1023 可使用摩擦来减慢车轮/轮胎 1014。作为另一示例，制动单元 1023 可被配置为再生的(regenerative)并且将车轮/轮胎 1014 的动能转换为电流。制动单元 1023 也可采取其它形式。

传感器融合算法 1024 可以包括例如计算装置 105 可运行的算法(或者存储算法的计算机程序产品)。

5 传感器融合算法 1024 可被配置为接受来自传感器的数据作为输入。所述数据可包括例如表示在传感器系统 101 的传感器处感测到的信息的数据。传感器融合算法 1024 可包括例如卡尔曼滤波器、贝叶斯网络或者另外的算法。传感器融合算法 1024 还可被配置为基于来自传感器系统 101 的数据来提供各种评价，包括例如对交通工具所位于的环境中的个体物体和/或特征的评估、对具体情形的评估和/或基于特定情形的可能影响的评估。其它评价也是可能的。

10 计算机视觉系统 1025 可以是配置为处理和分析由相机 1015 捕捉的图像以便识别交通工具所位于的环境中的物体和/或特征的任何系统，所述物体和 /或特征包括例如车道信息、交通信号和障碍物。为此，计算机视觉系统 1025 可使用物体识别算法、从运动中恢复结构(structure from motion, SFM)算法、视频跟踪或其它计算机视觉技术。在一些示例中，计算机视觉系统 1025 可以额外地被配置为地图绘制环境、跟随物体、估计物体的速度，等等。

15 导航和路线控制系统 1026 可以是配置为确定交通工具的驾驶路线的任何系统。导航和路线控制系统 1026 可以额外地被配置为在交通工具处于操作中的同时动态地更新驾驶路线。在一些示例中，导航和路线控制系统 1026 可被配置为结合来自传感器融合算法 1024、GPS 模块 1011 和一个或多个预定地图的数据以便为交通工具确定驾驶路线。

20 避障系统 1027 可以是配置为识别、评估和避免或者以其它方式越过车载设备 100 所位于的环境中的障碍物的任何系统。

控制系统 102 可以额外地或可替换地包括除了所示出的那些以外的组件。

外围设备 103 可被配置为允许车载设备 100 与外部传感器、其它车辆和/或用户交互。为此，外围设备 103 可包括例如无线通信系统 1031、触摸屏 1032、麦克风 1033 和/或扬声器 1034。

25 无线通信系统 1031 可以是配置为直接地或经由通信网络无线耦合至一个或多个其它车辆、传感器或其它实体的任何系统。为此，无线通信系统 1031 可包括用于直接或通过空中接口与其它车辆、传感器或其它实体通信的天线和芯片集。芯片集或整个无线通信系统 1031 可被布置为根据一个或多个其它类型的无线通信(例如，协议)来通信，所述无线通信诸如蓝牙、IEEE 802.11 (包括任何 IEEE 802.11 修订版)中描述的通信协议、蜂窝技术(诸如 GSM、CDMA、通用移动通信系统(universal mobile telecommunications system, UMTS)、EV-DO、WiMAX 或长期演进(long term evolution, LTE))、
30 紫蜂、专用短程通信(dedicated short range communications, DSRC)以及射频识别(radio frequency identification, RFID)通信，等等。无线通信系统 1031 也可采取其它形式。

触摸屏 1032 可被用户用来向车载设备 100 输入命令。为此，触摸屏 1032 可被配置为经由电容感测、电阻感测或者表面声波过程等等来感测用户的手指的位置和移动中的至少一者。触摸屏 1032 可能够感测在与触摸屏表面平行或与触摸屏表面在同一平面内的方向上、在与触摸屏表面垂直的方向上或者在这
35 两个方向上的手指移动，并且还可能够感测施加到触摸屏表面的压力的水平。触摸屏 1032 可由一个或多个半透明或透明绝缘层和一个或多个半透明或透明导电层形成。触摸屏 1032 也可采取其它形式。

麦克风 1033 可被配置为从车载设备 100 的用户接收音频(例如，声音命令或其它音频输入)。类似地，扬声器 1034 可被配置为向车载设备 100 的用户输出音频。

外围设备 103 可以额外地或可替换地包括除了所示出的那些以外的组件。

电源 104 可被配置为向车载设备 100 的一些或全部组件提供电力。为此，电源 104 可包括例如可再充电锂离子电池或铅酸电池。在一些示例中，一个或多个电池组可被配置为提供电力。其它电源材料和配置也是可能的。在一些示例中，电源 104 和能量源 1012 可一起实现，如一些全电动车中那样。

5 包括在计算装置 105 中的处理器 1051 可包括一个或多个通用处理器和/或一个或多个专用处理器（例如，数字信号处理器等）。就处理器 1051 包括多于一个处理器而言，这种处理器可单独工作或组合工作。计算装置 105 可实现基于通过用户接口 106 接收的输入控制车载设备 100 的功能。

存储器 1052 进而可包括一个或多个易失性存储组件和/或一个或多个非易失性存储组件，诸如光、磁和/或有机存储装置，并且存储器 1052 可全部或部分与处理器 1051 集成。存储器 1052 可包含可由处理器 1051 运行的指令 1053（例如，程序逻辑），以运行各种车辆功能，包括本说明书中描述的基于通信
10 通道检测中继攻击的方法的各实施例。

车载设备 100 的组件可被配置为以与在其各自的系统内部和/或外部的其它组件互连的方式工作。为此，车载设备 100 的组件和系统可通过系统总线、网络 and/ 或其它连接机制通信地链接在一起。

图 2C 示意了本申请提供的一种电子钥匙设备 200 的示例性功能结构图。电子钥匙设备 200 包括处理器 201、安全单元（secure element, SE）202、传感器 203、外围设备 204 和电源 205。

15 可以理解的是，本申请示意的结构并不构成对电子钥匙设备 200 的具体限定。在本申请另一些实施例中，电子钥匙设备 200 可以包括比图示更多或更少的部件，或者组合某些部件，或者拆分某些部件，或者不同的部件布置。图示的部件可以以硬件，软件或软件和硬件的组合实现。

处理器 201 可以被配置为处理发送至车载设备 100 的各种数据的操作。基于此，处理器 201 用于生成各通信通道的通道标识，还用于将所生成的通道标识传输到 SE。处理器 201 可以包括控制器 2011，
20 一些实施例中，控制器 2011 用于执行在第一通信通道传输第二通信通道的通道标识的操作。又一些实施例中，控制器 2011 还用于执行在第二通信通道传输第一通信通道的通道标识的操作。

SE 202 中设置有业务应用（applet）（图中未示出），该 applet 用于生成业务指令，还用于将通信通道的通道标识添加到业务指令中。

25 传感器 203 可以包括用于测量电子钥匙设备 200 与车载设备 100 距离的传感器。传感器 203 例如包括（一个或多个）UWB 模块 2031。UWB 模块 2031 可以用于从车载设备 100 中的 UWB 模块 1017（详见图 2B 示意的电子钥匙设备的结构图）接收测距帧，然后，UWB 模块 2031 向 UWB 模块 1017 发送应答帧，以使计算装置 105 基于 UWB 模块 1017 提供的时间戳计算车载设备 100 和电子钥匙设备 200 之间距离。

30 外围设备 204 可以被配置为允许电子钥匙设备 200 与外部传感器或者车辆交互。为此，外围设备 204 可以包括例如无线通信系统 2041。其中，无线通信系统 2041 可包括用于直接或通过空中接口与车载设备 100、传感器或其它实体通信的天线和芯片集。芯片集或整个无线通信系统 2041 可被布置为根据一个或多个其它类型的无线通信（例如，协议）来通信，所述无线通信诸如蓝牙、IEEE 802.11（包括任何 IEEE 802.11 修订版）中描述的通信协议、蜂窝技术（诸如 GSM、CDMA、UMTS、EV-DO、WiMAX 或 LTE）、紫蜂、DSRC 以及 RFID 通信，等等。无线通信系统 2041 也可采取其它形式。

35 电源 205 可被配置为向电子钥匙设备 200 的一些或全部组件提供电力。为此，电源 205 可以包括例如可再充电锂离子电池或铅酸电池。在一些示例中，一个或多个电池组可被配置为提供电力。其它电源材料和配置也是可能的。

可以理解的是，一些实施例中，图 2C 示意的各功能模块可以被配置在独立的电子钥匙设备中使用。另一些实施例中，图 2C 示意的各功能模块可以与其他电子设备中相应的功能模块耦合，当电子设备的功能模块实现本申请以下基于通信通道检测中继攻击的方法的实施例时，该电子设备被用作电子钥匙设

备 200。

以下对本申请的基于通信通道检测中继攻击的方法进行示例性描述。

一些实施例中，车载设备和电子钥匙设备中均预置第一规则。或者，另一些实施例中，车载设备和电子钥匙设备中均预置第二规则。又一些实施例中，车载设备和电子钥匙设备中均预置第一规则和第二规则。其中，业务数据通道标识用于标识业务数据通道，测距通道标识用于标识测距通道。

其中，第一规则用于指示车载设备和电子钥匙设备确定业务数据通道标识。一些实施例中，第一规则用于指示车载设备和电子钥匙设备提取所连接业务数据通道的业务数据通道信息，然后，使用所提取的业务数据通道信息生成业务数据通道标识。业务数据通道信息例如是该业务数据通道的传输频段、时域信息、频域信息、多径延迟信息、信号强度、信号相位等物理通信特征中的至少一个。另一些实施例中，第一规则用于指示车载设备和电子钥匙设备将所连接业务数据通道的任意通道信息作为业务数据通道标识。例如，第一规则指示车载设备和电子钥匙设备将均将业务数据通道的多径延迟信息作为业务数据通道标识。一些实施例中，业务数据通道标识由业务数据通道的物理特征确定，通常这些物理特征只在建立两条物理业务数据通道的设备间具有匹配关系，不同物理通道具备不同的物理特征。

第二规则用于指示车载设备和电子钥匙设备确定测距通道标识。一些实施例中，第二规则可以指示将测距通道的通用唯一识别码（universally unique identifier, UUID）、测距通道地址、测距通道的会话标识、测距通道会话的前导序列和测距帧返回的时间戳中的一个，指定为测距通道标识。本申请中，将作为测距通道标识的信息称为指定信息。例如，第二规则指示车载设备 100 和电子钥匙设备 200 均将 UWB 地址作为测距通道标识。另一些实施例中，第二规则可以指示根据测距通道的会话密钥生成的密文或者消息鉴别码生成测距通道标识，例如，车载设备 100 和电子钥匙设备 200 可以均根据 UWB 会话密钥基于预设算法生成的密文作为测距通道标识；再如，车载设备 100 和电子钥匙设备 200 可以均根据消息鉴别码生成测距通道标识。

基于此，参见图 3A，图 3A 是基于通信通道检测中继攻击的方法 100 的一种示例性方法流程图。基于通信通道检测中继攻击的方法 100（以下简称方法 100）包括以下步骤：

步骤 S101，车载设备通过第一通信通道从第一设备接收第一标识。

其中，第一设备是车载设备所连接的设备。第一标识用于标识与第二通信通道类型相同的通信通道。第一通信通道和第二通信通道相互独立，且第一通信通道和第二通信通道均用于连接车载设备与第一设备。

一些实施例中，第一通信通道是业务数据通道，那么，第二通信通道就是测距通道，相应的，第一标识是测距通道标识。例如，如图 4A 示意的实施例，第一通信通道是蓝牙通道，那么，第二通信通道就是 UWB 通道，相应的，第一标识是 UWB 通道标识。另一些实施例中，第一通信通道是测距通道，那么，第二通信通道是业务数据通道，相应的，第一标识是业务数据通道标识。例如，如图 4B 示意的实施例，第一通信通道是 UWB 通道，那么，第二通信通道就是蓝牙通道，相应的，第一标识是蓝牙通道标识。

示例性的，一些实施例中，第一通信通道是业务数据通道，第一标识是测距通道标识，该测距通道标识可以以会话密文的形式在第一通信通道中传输。其中，该测距通道标识例如可以由电子钥匙设备添加到业务数据通道中。例如，UWB 通道标识可以以蓝牙会话密文的形式，通过蓝牙通道传输。详见图 4B 示意的实施例所述，此处不再详述。另一些实施例中，第一通信通道是测距通道，第一标识是业务数据通道标识，该业务数据通道标识可以包含于该测距通道所传输的测距确认字符（acknowledgement, ACK）帧中传输。例如，蓝牙通道标识可以被携带在测距 ACK 帧中，通过 UWB 通道传输。详见图 4A 示意的实施例所述，此处不再详述。

步骤 S102, 车载设备确定第二通信通道的通道标识。

其中, 车载设备可以根据第二通信通道对应的通道标识确定规则确定第二通信通道的通道标识。

可以理解的是, 步骤 S101 中涉及的第一标识所标识的通信信道的类型, 与第二通信通道的类型相同, 并且, 车载设备和电子钥匙设备生成通道标识的规则相同, 所以, 车载设备可以通过检测两标识的关系确定当前是否存在中继攻击。示例性的, 第一标识例如 UWB 通道标识, 那么, 第一标识所标识的是电子钥匙设备连接的 UWB 通道。车载设备可以确定车载设备所连接的 UWB 通道的标识, 进而, 车载设备可以通过检测该两 UWB 通道标识是否相同, 确定是否被中继攻击。若两 UWB 通道标识相同, 则车载设备可以确定没有遭受到中继攻击, 若两 UWB 通道标识不相同, 则车载设备可以确定遭受到中继攻击。

一些实施例中, 第一标识例如是业务数据通道标识, 第二通信通道是业务数据通道, 车载设备可以根据第一规则提取第二通信通道的通道信息中的至少一个信息, 然后, 根据所提取的通道信息中的至少一个信息生成第二通信通道的业务数据通道标识。如图 4A 示意的实施例, 第二通信通道例如是蓝牙通道, 车载设备可以提取该蓝牙通道的传输频段和多径延迟信息, 然后, 根据传输频段和多径延迟信息生成蓝牙通道标识。另一些实施例中, 第一标识例如是测距通道标识, 第二通信通道则是测距通道, 车载设备根据第二规则获取第二通信通道的通道信息中的指定信息作为第二通信通道的测距通道标识。如图 4B 示意的实施例, 第二通信通道例如是 UWB 通道, 车载设备可以提取该 UWB 通道的前导序列 UWB 通道标识。

进一步的, 若第二通信通道的通道标识与第一标识匹配, 说明第二通信通道是车载设备与电子钥匙设备之间通信通道, 第一设备即为电子钥匙设备, 也即车载设备与电子钥匙设备之间未被中继攻击。若第二通信通道的通道标识与第一标识不匹配, 说明第二通信通道不是车载设备与电子钥匙设备之间通信通道, 第一设备即为中继设备, 也即车载设备与电子钥匙设备之间存在中继攻击。

一些实施例中, 第二通信通道的通道标识和第一标识是业务数据通道标识, 车载设备可以使用计算相似度和计算二者梯度中至少一种方式, 计算第二通信通道的通道标识与第一标识的相似度参数, 然后, 确定相似度参数是否大于预设阈值。相似度参数指示第二通信通道的通道标识与第一标识的相似程度, 相似度参数越小, 说明第二通信通道的通道标识与第一标识的相似程度越小, 相似度参数越大, 说明第二通信通道的通道标识与第一标识的相似程度越高。基于此, 若第二通信通道的通道标识与第一标识的相似度参数大于预设阈值, 车载设备确定第二通信通道的通道标识与第一标识相匹配。其中, 第二通信通道的通道标识与第一标识的相似度参数大于预设阈值, 说明第二通信通道的通道标识与第一标识所对应的业务数据通道信息基本相同, 进而, 说明业务数据通道未被中继攻击。反之, 若第二通信通道的通道标识与第一标识的相似度参数大于预设阈值, 说明第二通信通道的通道标识与第一标识所对应的业务数据通道信息不同, 进而证明车载设备和电子钥匙设备之间业务数据通道受到中继攻击。

例如, 受到天气等因素的影响, 蓝牙通道的多径延迟信息等物理通道信息会发生变化, 因此, 即使该蓝牙通道未被中继攻击, 电子钥匙设备端根据该蓝牙通道的信息生成的第一标识, 与车载设备根据生成的该蓝牙通道的信息生成的标识也可能不同, 但是相似度相对较高。所以, 本实施例中, 车载设备可以根据两蓝牙通道标识的相似度参数, 检测是否被中继攻击。

另一些实施例中, 第二通信通道的通道标识和第一标识是测距通道标识, 车载设备可以检测第二通信通道的通道标识与第一标识是否相同, 若第二通信通道的通道标识与第一标识相同, 车载设备确定第二通信通道的通道标识与第一标识相匹配。其中, 第二通信通道的通道标识与第一标识相同, 说明第二通信信道与第一标识所标识的测距信道是同一条测距通道, 进而说明第一设备是电子钥匙设备, 也即车载设备和电子钥匙设备之间未被中继攻击。反之, 若第二通信通道的通道标识与第一标识不同, 说明第

二通信信道与第一标识所标识的测距信道不是一条测距通道，进而说明第一设备是中继设备。

示例性的，第二通信通道是UWB通道，且UWB通道标识是前导序列的场景下，车载设备与第一设备建立UWB通道时，可以确定该UWB通道的前导序列，前导序列可以唯一标识UWB通道。基于此，车载设备可以根据所接收的前导序列与所提取的本端的前导序列是否相同，确定是否被中继攻击。

- 5 步骤S103，当车载设备与第一设备的距离在预设距离之内，且第二通信通道的通道标识与第一标识匹配时，车载设备响应预先接收的业务指令打开车门。

其中，车载设备在与第一设备建立的测距通道之后，传感器系统101一直通过该测距通道按照一定频率向第一设备发送测距帧，然后，从第一设备接收每个测距帧的测距ACK帧，进而，传感器系统101将每组测距帧和测距ACK帧发送到计算装置105。计算装置105根据每组测距帧和测距ACK帧计算车载设备与第一设备的当前距离。然后，计算装置105将所得到的当前距离发给控制系统102。控制系统102判断当前距离是否在预设距离之内，若车载设备与第一设备的当前距离在预设距离之内，且第二通信通道的通道标识与第一标识相匹配时，控制系统102控制交通工具的门打开。

示例性的，车载设备所发送的测距帧中可以包括该车载设备生成的识别标识，进而，车载设备接收到测距ACK帧之后，可以检测该测距ACK帧中是否包含该识别标识，若该测距ACK帧中包含该识别标识，车载设备根据相应测距帧和该测距ACK帧计算车载设备与第一设备的距离。该识别标识例如是nonce随机数。该随机数可以是车载设备随机生成，并携带在第一个测距帧中的。

此外，该业务指令由电子钥匙设备生成，并在电子钥匙设备建立业务数据通道之后的任意时刻传输到车载设备。相应的，车载设备可以在打开车门之前的任意时刻接收到该业务指令。

一些实施例中，车载设备可以在检测到该车载设备与第一设备的距离在预设距离之内之后，向第一设备发送业务请求，进而，车载设备从第一设备接收到该业务指令。另一些实施例中，车载设备连接业务数据通道之后，即可通过该业务数据通道接收业务指令。

可见，采用本实现方式，车载设备和电子钥匙设备中维护业务数据通道或者测距通道的通道标识确定规则，然后，该车载设备可以根据相应的通道标识确定规则以及该车载设备所连接的通道的信息确定通道标识，进而，该车载设备可以在接收到同类型通信通道的标识之后，通过比对所计算的通道标识和所接收的通道标识是否相同，确定车载设备和电子钥匙设备之间是否被中继攻击，并在不存在中继攻击的场景下，响应业务指令打开车门，从而能够提高PEPS系统的安全性。

此外，在一种可能的实现方式中，在执行步骤S101之前，车载设备在建立业务数据通道连接之后，可以通过该业务数据通道接收业务指令，在接收到该业务指令之后，该车载设备与第一设备建立测距通道，并通过该测距通道向第一设备发送测距帧。进而，执行上述方法100。

30 采用本实现方式，车载设备能够在确定存在合法业务指令的情况下，对第一设备进行测距，从而能够减少测距产生的资源消耗。

参见图3B，图3B是基于通信通道检测中继攻击的方法200的一种示例性方法流程图。基于通信通道检测中继攻击的方法200（以下简称方法200）是电子钥匙设备200端的实施例，方法200与方法100相对应。方法200包括以下步骤：

- 35 步骤S201，电子钥匙设备与第二设备建立第一通信通道。

其中，第一通信通道是电子钥匙设备与第二设备之间的通信通道。与方法100相对应的，第一通信通道可以是业务数据通道或者测距通道。

步骤S202，电子钥匙设备生成第一标识。

其中，第一标识用于标识与第二通信通道类型相同的通信通道。第二通信通道是电子钥匙设备与第

二设备之间的通信通道。第二通信通道与第一通信信道相互独立。若第一通信通道是业务数据通道，第一标识则是测距通道标识，若第一通信通道是测距通道，第一标识则是业务数据通道标识。

一些实施例中，第一通信通道是业务数据通道，第一标识则是测距通道标识。电子钥匙设备可以根据第二规则确定测距通道标识。与方法 100 相对应的，第一通信通道例如是蓝牙通道，那么，第二通信通道就是 UWB 通道，相应的，第一标识是 UWB 通道标识。另一些实施例中，第一通信通道是测距通道，第一标识则是业务数据通道标识。电子钥匙设备可以根据第一规则确定该业务数据通道标识。例如，第一通信通道是 UWB 通道，那么，第二通信通道就是蓝牙通道，相应的，第一标识是蓝牙通道标识。示例性的，电子钥匙设备在生成该业务数据通道标识时，可以将业务会话密钥作为参数，从而能够防止该业务数据通道标识被仿冒和篡改。其中，电子钥匙设备生成通道标识的操作过程，与车载设备生成通道标识的操作过程相似，本申请此处不再详述。

步骤 S203，电子钥匙设备通过第一通信通道向第二设备发送第一标识。

一些实施例中，第一标识是测距通道标识，电子钥匙设备可以将该测距通道标识加密得到会话密文，然后，在业务数据通道上传输该会话密文。例如，电子钥匙设备可以将 UWB 通道标识加密生成蓝牙会话密文，然后，通过蓝牙通道向第二设备传输该蓝牙会话密文。另一些实施例中，第一标识是业务数据通道标识。电子钥匙设备可以将该业务数据通道标识添加到测距 ACK 帧，并通过第一通信通道传输该测距 ACK 帧。示例性的，第一标识例如是 UWB 通道标识，电子钥匙设备可以不断的接收第二设备发送的测距帧，然后，向第二设备发送测距帧的测距 ACK 帧。其中，每个测距 ACK 帧中均可以包含 UWB 通道标识，或者在指定测距 ACK 帧中包含 UWB 通道标识。此外，每个测距 ACK 帧中还可以包含识别标识，该识别标识由车载设备生成，并包含在测距帧中。

根据本实施例的描述，电子钥匙设备通过第一通信通道发送第二通信通道对应的通道标识，从而建立第一通信通道和第二通信通道的对应关系，进而便于确定第一通信通道和第二通信通道连接的是同一设备。

此外，电子钥匙设备还通过业务数据通道向第二设备发送业务指令。一些实施例中，电子钥匙设备可以从第二设备接收业务请求，然后，通过业务数据通道向第二设备发送业务指令。另一些实施例中，第一通信通道是业务数据通道，电子钥匙设备在建立业务数据通道之后，可以立即向第二设备发送业务指令，以触发车载设备检测业务指令，然后，再与第二设备建立测距通道。例如，电子钥匙设备向第二设备发送业务指令之后唤醒 UWB 模块 1017。若第二设备是车载设备，在车载设备唤醒 UWB 模块 1017 之后，电子钥匙设备与第二设备建立 UWB 通道。

可以理解的是，车载设备接收到通道标识和业务指令之后，根据通道标识执行一系列的验证，在确定该车载设备与电子钥匙设备之间不存在中继攻击，且该车载设备与该电子钥匙设备的距离在预设距离之内之后，响应业务指令打开车门。车载设备执行的操作详见方法 100 的描述，本申请此处不再详述。

可见，采用本实现方式，电子钥匙设备使用第一通信通道传输第二通信通道的通道标识，能够建立第一通信通道和第二通信通道的对应关系，从而向车载设备提供通道的对应关系，以便于车载设备根据通信通道验证对端设备是否是电子钥匙设备，进而，使得车载设备在不存在中继攻击的情况下，响应业务指令打开车门，从而能够提高 PEPS 系统的安全性。

参见图 3C，图 3C 是基于通信通道检测中继攻击的方法 300 的一种示例性方法流程图。基于通信通道检测中继攻击的方法 300（以下简称方法 300）的实施场景例如是车载设备 100 和电子钥匙设备 200 中均预置第一规则和第二规则。方法 300 包括以下步骤：

步骤 S301，车载设备从第一设备接收业务指令。

其中,该业务指令中包含第一业务数据通道标识和第一测距通道标识,该第一业务数据通道标识用于标识电子钥匙设备所连接的业务数据通道,该第一测距通道标识用于标识电子钥匙设备所连接的测距通道。业务指令包含电子钥匙设备中的数字密钥生成,用于车载设备验证电子钥匙设备持有合法的数字密钥。

- 5 示例性的,参考图 4C 和图 4D,第一业务数据通道标识例如是第一蓝牙通道标识,第一测距通道标识例如是第一 UWB 通道,第一蓝牙通道标识用于标识电子钥匙设备所连接的蓝牙通道,第一 UWB 通道用于标识电子钥匙设备所连接的 UWB 通道。

步骤 S302,车载设备确定第二业务数据通道标识和第二测距通道标识。

- 10 其中,该第二业务数据通道标识用于标识车载设备所连接的业务数据通道,该第二测距通道标识用于标识车载设备所连接的测距通道。本实施例中,车载设备确定第二业务数据通道标识和第二测距通道标识的操作,详见方法 100 中的相关描述,本申请此处不再详述。

示例性的,参考图 4C 和图 4D,第二业务数据通道标识例如是第二蓝牙通道标识,第二测距通道标识例如是第二 UWB 通道,第二蓝牙通道标识用于标识车载设备所连接的蓝牙通道,第二 UWB 通道用于标识车载设备所连接的 UWB 通道。

- 15 进一步的,若第一业务数据通道标识和第二业务数据通道标识相匹配,且第一测距通道标识和第二测距通道标识相同,说明第一设备是电子钥匙设备,否则,说明第一设备是中继设备。

步骤 S303,当车载设备与第一设备的距离在预设距离之内,第一业务数据通道标识和第二业务数据通道标识相匹配,且第一测距通道标识和第二测距通道标识相同时,车载设备响应业务指令打开车门。

- 20 其中,方法 300 与方法 100 中相同的部分,可以参照方法 100 的操作及实施场景,例如,车载设备向第一设备发送业务请求,在对第一设备的业务指令验证通过后,车载设备继续进行距离判断,当车载设备与第一设备的距离在预设距离之内时,执行 S105。本申请此处不再赘述。

参见图 3D,图 3D 是基于通信通道检测中继攻击的方法 400 的一种示例性方法流程图。基于通信通道检测中继攻击的方法 400(以下简称方法 400)是电子钥匙设备 200 端的实施例,方法 400 与方法 300 相对应。方法 400 包括以下步骤:

- 25 步骤 S401,电子钥匙设备与第二设备建立业务数据通道和测距通道。

步骤 S402,电子钥匙设备确定第一业务数据通道标识和第一测距通道标识。

步骤 S403,电子钥匙设备生成业务指令。

- 30 示例性的,结合图 2C,本实施例中,处理器 201 可以确定第一业务数据通道标识和第一测距通道标识,然后,处理器 201 将第一业务数据通道标识和第一测距通道标识传输到 SE 2011 中的 applet 中,该 applet 生成包含第一业务数据通道标识和第一测距通道标识的业务指令。

步骤 S404,电子钥匙设备通过业务数据通道向第二设备发送业务指令。

其中,结合图 2C,控制器 2012 可以执行在业务数据通道传输业务指令的操作。

其中,方法 400 与方法 200 中相同的部分,可以参照方法 200 的操作及实施场景,例如,电子钥匙设备可以在接收到业务请求之后,执行步骤 S401。本申请此处不再赘述。

- 35 可以理解的是,车载设备接收到业务指令之后,执行方法 300 所述的操作,本申请此处不再详述。

综上,本申请提供的车载设备和电子钥匙设备中预设通道标识确定规则,进而,在通信过程中,电子钥匙设备使用该通道标识确定规则生成通道标识,并发送到该电子钥匙设备的对端设备。该通道标识是电子钥匙设备当前连接的通信通道的标识。相应的,车载设备从该车载设备的对端设备接收通道标识之后,根据该通道标识确定规则生成车载设备所接收的通信通道的通道标识,进而,车载设备通过检测

所接收的通道标识与车载设备生成的通道标识是否相同,来确定该车载设备与该电子钥匙设备之间是否存在中继攻击,进而,确定是否打开车门。

以下结合图 2A 至图 2C 示意的设备,通过实例对本申请所述的基于通信通道检测中继攻击的方法进行描述。

- 5 其中,车载设备例如是图 2B 所述的车载设备 100,电子钥匙设备可以是图 2C 所述的电子钥匙设备 200。示例性的,车载设备 100 和电子钥匙设备 200 中均设置第一规则和第二规则。本实施例中,业务数据通道例如是蓝牙通道,测距通道例如是 UWB 通道。基于此,车载设备 100 和电子钥匙设备 200 的初始状态如下:车载设备 100 的蓝牙模块与电子钥匙设备 200 的蓝牙模块预先配对,然后,在车载设备 100 与电子钥匙设备 200 建立蓝牙通道之前,UWB 模块 1017 和 UWB 模块 2031 均处于睡眠模式,即 UWB 模块 1017 和 UWB 模块 2031 未建立 UWB 通道且不进行 UWB 数据交互。在车载设备 100 与电子钥匙设备 200 建立蓝牙通道之后,UWB 模块 1017 和 UWB 模块 2031 被唤醒,建立 UWB 通道且通过 UWB 数据交互进行测距。

进一步的,以下以车载设备和电子钥匙设备未被中继攻击的实施场景为例,对车载设备 100 和电子钥匙设备 200 之间通信过程进行介绍。

- 15 如图 4A 所示,图 4A 示意了基于通信通道检测中继攻击的方法 500 的信令交互图,基于通信通道检测中继攻击的方法 500 (以下简称方法 500) 包括如下步骤:

步骤 S501,车载设备 100 与电子钥匙设备 200 建立蓝牙通道 A。

其中,车载设备 100 与电子钥匙设备 200 的距离在一定距离内时,车载设备 100 的蓝牙模块与电子钥匙设备 200 的蓝牙模块建立连接,形成蓝牙通道 A。该一定距离大于本申请所述的预设距离。

- 20 示例性的,在建立蓝牙通道 A 之后,电子钥匙设备 200 中的处理器 201 可以唤醒 UWB 模块 2031,以接收测距帧。此外,电子钥匙设备 200 例如还根据第一规则提取蓝牙通道 A 的传输频段、多径延迟信息和信号强度信息,然后,根据蓝牙通道 A 的传输频段、多径延迟信息和信号强度信息生成蓝牙通道标识 BT01。示例性的,电子钥匙设备 200 还可以使用蓝牙会话密钥参与计算得到 BT01,以使 BT01 无法被伪造或者篡改。

- 25 步骤 S502,电子钥匙设备 200 生成业务指令。

结合图 2C,SE 202 生成业务指令。

步骤 S503,电子钥匙设备 200 通过蓝牙通道 A 向车载设备 100 发送业务指令。

步骤 S504,车载设备 100 唤醒 UWB 模块 1017,并与电子钥匙设备 200 建立 UWB 通道 A。

- 30 其中,车载设备 100 接收业务指令之后,可以利用业务密钥对业务指令进行鉴权,通过后认为电子钥匙设备 200 是合法的电子钥匙设备,进而,车载设备 100 唤醒 UWB 模块 1017,使得 UWB 模块 1017 与 UWB 模块 2031 连接,得到 UWB 通道 A。

步骤 S505,车载设备 100 通过 UWB 通道 A 向电子钥匙设备 200 发送测距帧。

其中,UWB 模块 1017 向 UWB 模块 2031 发送测距帧。

步骤 S506,电子钥匙设备 200 向车载设备 100 发送测距 ACK 帧。

- 35 其中,UWB 模块 2031 向 UWB 模块 1017 发送测距 ACK 帧。测距 ACK 帧是响应测距帧的数据帧,测距 ACK 帧中包含蓝牙通道标识 BT01。

结合图 2C,处理器 201 可以将蓝牙通道标识 BT01 携带在测距 ACK 帧中,然后,控制器 2011 调用 UWB 通道 A 传输测距 ACK 帧。

需要指出的是,在步骤 S504 之后,UWB 模块 1017 持续按照预设频率向 UWB 模块 2031 发送测距帧,

相应的，UWB 模块 2031 同样按照该预设频率持续的向 UWB 模块 1017 回复测距 ACK 帧。进而，车载设备根据每组测距帧和测距 ACK 帧测量车载设备 100 与电子钥匙设备 200 的距离。

步骤 S507，车载设备 100 根据蓝牙通道标识 BT01 检测是否被中继攻击。

5 车载设备 100 在接收到测距 ACK 帧之后，可以根据第一规则提取车载设备 100 所连接的蓝牙通道的传输频段、多径延迟信息和信号强度信息，然后，根据所提取的传输频段、多径延迟信息和信号强度信息生成蓝牙通道标识。示例性的，车载设备 100 同样可以使用蓝牙会话密钥计算蓝牙通道标识。

由于本实施例中，车载设备 100 所连接的蓝牙通道是蓝牙通道 A，所以，车载设备 100 得到的蓝牙通道标识是 BT01。进而，车载设备 100 可以确定车载设备 100 与电子钥匙设备 200 之间未被中继攻击。

10 步骤 S508，在车载设备 100 与电子钥匙设备 200 的距离在预设距离之内时，车载设备 100 响应业务指令打开车门。

示例性的，预设距离例如是 2 米，当车载设备 100 与电子钥匙设备 200 的距离小于或者等于 2 米时，车载设备 100 响应业务指令打开车门。

15 采用本实现方式，车载设备 100 在确定电子钥匙设备 200 具备合法业务指令时，再执行测距操作，从而能够节省资源。另外，电子钥匙设备 200 通过使用 UWB 通道传输蓝牙通道标识的方式，将蓝牙通道和 UWB 通道绑定。车载设备 100 通过蓝牙通道标识检测是否被中继。

如图 4B 所示，图 4B 示意了基于通信通道检测中继攻击的方法 600 的信令交互图，基于通信通道检测中继攻击的方法 600（以下简称方法 600）包括如下步骤：

步骤 S601，车载设备 100 与电子钥匙设备 200 建立蓝牙通道 A 和 UWB 通道 A，并确定 UWB 通道标识 UWB01。

20 其中，蓝牙通道 A 和 UWB 通道 A 的建立过程可以如上述任一实施例所述，此处不再赘述。

本实施例中，在建立 UWB 通道 A 之后，电子钥匙设备 200 根据第二规则确定 UWB 通道标识 UWB01。示例性的，第二规则例如指示将 UWB 通道 A 的前导序列作为 UWB 通道标识 UWB01。此外，在建立 UWB 通道 A 之后，车载设备 100 一直在测量车载设备 100 与电子钥匙设备 200 的距离。车载设备 100 测距的操作过程，本申请此处不再详述。

25 此外，本实施例中，在建立蓝牙通道 A 之后，电子钥匙设备 200 可以随时通过蓝牙通道 A 向车载设备 100 发送业务指令。

步骤 S602，电子钥匙设备 200 通过蓝牙通道 A 向车载设备 100 发送 UWB 通道标识 UWB01。

其中，处理器 201 可以将 UWB01 加密得到蓝牙会话密文，然后，处理器 201 调用蓝牙通道 A 传输蓝牙会话密文。

30 步骤 S603，车载设备 100 根据 UWB 通道标识 UWB01 检测是否被中继攻击。

示例性的，车载设备 100 接收 UWB01 之后，处理器 1051 根据第二规则获取本端（车载设备 100 端）连接的 UWB 通道的前导序列作为本端的 UWB 通道标识，然后，处理器 1051 可以判断本端的 UWB 通道标识是否是 UWB01。应理解，本实施例中处理器 1051 得到的本端的 UWB 通道标识是 UWB01，进而，车载设备 100 可以确定车载设备 100 与电子钥匙设备 200 之间未被中继攻击。

35 步骤 S604，在车载设备 100 与电子钥匙设备 200 的距离在预设距离之内时，车载设备 100 响应业务指令打开车门。

其中，步骤 S604 的具体执行过程与方法 500 的步骤 S508 相似，详细过程可参见步骤 S508 的描述，此处不再赘述。

采用本实现方式，电子钥匙设备 200 通过使用蓝牙通道传输 UWB 通道标识的方式，将蓝牙通道和

UWB 通道绑定。车载设备 100 通过 UWB 通道标识检测是否被中继。

如图 4C 所示，图 4C 示意了基于通信通道检测中继攻击的方法 700 的信令交互图，基于通信通道检测中继攻击的方法 700（以下简称方法 700）包括如下步骤：

5 步骤 S701，车载设备 100 与电子钥匙设备 200 建立蓝牙通道 A 和 UWB 通道 A，并确定蓝牙通道标识 BT01 和 UWB 通道标识 UWB01。

步骤 S702，电子钥匙设备 200 生成业务指令。

其中，该业务指令中包含蓝牙通道标识 BT01 和 UWB 通道标识 UWB01。示例性的，处理器 201 可以确定 BT01 和 UWB01，然后，处理器 201 将 BT01 和 UWB01 传输到 SE 2011 中的 applet 中，该 applet 生成包含 BT01 和 UWB01 的业务指令。

10 一种可选的实现方式中，电子钥匙设备 200 可以接收车载设备 100 发送的业务请求，然后，电子钥匙设备 200 执行步骤 S702。

步骤 S703，电子钥匙设备 200 通过蓝牙通道 A 向车载设备 100 发送业务指令。

步骤 S704，车载设备 100 根据 BT01 验证车载设备 100 连接的蓝牙通道，并根据 UWB01 验证车载设备 100 连接的 UWB 通道。

15 其中，本实施例的验证过程详见方法 500 和方法 600 的相关描述，本申请此处不再赘述。

步骤 S705，在车载设备 100 与电子钥匙设备 200 的距离在预设距离之内时，车载设备 100 响应业务指令打开车门。

其中，本实施例中，车载设备 100 持续测量车载设备 100 与电子钥匙设备 200 的距离。车载设备 100 测距的操作过程详见上述实施例的描述，本申请此处不再详述。

20 方法 500 至方法 700 均是车载设备和电子钥匙设备未被中继攻击的实施场景下的实施例，以下以车载设备和电子钥匙设备被中继攻击的实施场景为例，对本申请的技术方案进行描述。

如图 4D 所示，图 4D 示意了基于通信通道检测中继攻击的方法 800 的信令交互图。示例性的，如图 4E 示意的场景图，本实施例中车载设备 100 与电子钥匙设备 200 逻辑上的蓝牙通道 A 是至少一个中继设备转发车载设备 100 和电子钥匙 200 的蓝牙交互数据包的方式被中继的。相应的，蓝牙通道 A 可以等效为蓝牙通道 A1 和蓝牙通道 A2 两条蓝牙通道，其中，蓝牙通道 A1 是电子钥匙设备 200 与中继设备之间的蓝牙通道，蓝牙通道 A2 是中继设备与车载设备 100 之间的蓝牙通道。此外，本实施例中，当中继设备攻击车载设备 100 与电子钥匙设备 200 时，中继设备接收车载设备 100 发送的测距帧，并向车载设备 100 回复测距 ACK 帧。一些实施例中，中继设备还可以向电子钥匙设备 200 发送测距帧。基于此，电子钥匙设备 200 与中继设备之间建立 UWB 通道 B1，车载设备 100 与中继设备的之间建立 UWB 通道 B2。

30 基于通信通道检测中继攻击的方法 800（以下简称方法 800）包括如下步骤：

步骤 S801，电子钥匙设备 200 通过蓝牙通道 A 向车载设备 100 发送第一业务指令。

其中，本步骤发生在车载设备 100 与电子钥匙设备 200 被中继设备通过中继建立蓝牙通道 A 之后。第一业务指令包含车载设备 100 打开车门的密文。

35 进而，车载设备 100 验证第一业务指令是合法指令之后，唤醒 UWB 模块 1017，然后，车载设备 100 接入 UWB 通道。车载设备 100 例如接入 UWB 通道 B。

然后，车载设备 100 持续向中继设备发送测距帧，并接收中继设备发送的测距 ACK 帧，以测量车载设备 100 与中继设备的距离。一些实施例中，中继设备还可以向电子钥匙设备 200 发送测距帧，相应的，电子钥匙设备 200 向中继设备发送测距 ACK 帧。车载设备 100 测距的操作过程，本申请此处不再详述。

进一步的，当车载设备 100 检测到该车载设备 100 与中继设备的距离例如小于或者等于 2 米时，车

载设备 100 执行步骤 S802。

步骤 S802，车载设备 100 通过蓝牙通道 A2 向中继设备发送业务请求。

步骤 S803，中继设备通过蓝牙通道 A1 向电子钥匙设备 200 发送业务请求。

5 步骤 S804，电子钥匙设备 200 确定蓝牙通道 A1 对应的通道标识 BT02，以及 UWB 通道 B1 的通道标识 UWB02。

其中，电子钥匙设备 200 根据第一规则确定 BT02，并根据第二规则确定 UWB02。UWB02 例如是 UWB 通道 B1 的前导序列。

步骤 S805，电子钥匙设备 200 生成第二业务指令。

示例性的，该第二业务指令中不仅包含打开车门的密钥计算出的密文，还包含 BT02 和 UWB02。

10 步骤 S806，电子钥匙设备 200 通过蓝牙通道 A1 向中继设备发送第二业务指令。

步骤 S807，中继设备通过蓝牙通道 A2 向车载设备 100 发送第二业务指令。

步骤 S808，车载设备 100 确定蓝牙通道标识 BT03 和 UWB 通道标识 UWB03。

其中，BT03 指示蓝牙通道 A2，UWB03 指示 UWB 通道 B2。车载设备 100 根据第一规则确定 BT03，并根据第二规则确定 UWB03。UWB03 例如是 UWB 通道 B2 的前导序列。

15 步骤 S809，车载设备 100 确定 BT03 与 BT02 不匹配，且 UWB02 与 UWB03 不同。

其中，蓝牙通道 A2 的通道信息与蓝牙通道 A1 的通道信息不同，因此，使用相同的种类的通道信息生成的蓝牙通道标识也不匹配，即，蓝牙通道 A1 的通道标识是 BT02，蓝牙通道 A2 的通道标识是 BT03，且 BT02 和 BT03 的相似度参数小于预设阈值。

BT03 与 BT02 不同，说明蓝牙通道 A 已经被中继攻击。同理，UWB02 与 UWB01 不同，说明车载设备 20 100 所连接的 UWB 通道与电子钥匙设备 200 所连接的 UWB 通道不是同一条 UWB 通道，进而，说明存在中继攻击。

步骤 S810，车载设备 100 输出报警信息。

可以理解的是，图 4E 示意的中继场景仅仅是一种示意性描述，对本申请所涉及的中继场景不构成限制。在另一些实施例中，车载设备 100 和电子钥匙设备 200 之间可以存在多台中继设备，并且，车载 25 设备 100 和电子钥匙设备 200 可以分别连接不同的中继设备，中继设备之间也可以进行通信，以将电子钥匙设备 200 生成的数据传输给车载设备 100。相应的，对应图 4E 示意的中继场景，本申请还可以采用方法 500 或者方法 600 示意的基于通信通道检测中继攻击的方法执行通信，具体的，本申请此处不再详述。

此外，方法 500 至方法 800 均是示意性描述，对本申请所涉及的基于通信通道检测中继攻击的方法 30 不构成限制。在其他一些实施例中，在本申请技术思想的基础上，还可以包括其他操作步骤。在另一些实施例中，在本申请技术思想的基础上，上述各方法的操作步骤可以调换。本申请此处不再详述。

综上，为提高 PEPS 系统的安全性，本申请提供的车载设备和电子钥匙设备中预设通道标识确定规则，进而，在通信过程中，电子钥匙设备使用该通道标识确定规则生成通道标识，并发送到该电子钥匙 35 设备的对端设备。该通道标识是电子钥匙设备当前连接的通信通道的标识。相应的，车载设备从该车载设备的对端设备接收通道标识之后，根据该通道标识确定规则生成车载设备所接收的通信通道的通道标识，进而，车载设备通过检测所接收的通道标识与车载设备生成的通道标识是否相同，来确定该车载设备与该电子钥匙设备之间是否存在中继攻击，进而，确定是否打开车门。

上述本申请提供的实施例中，分别从各个设备本身、以及从各个设备之间交互的角度对本申请实施例提供的基于通信通道检测中继攻击的方法的各方案进行了介绍。例如上述车载设备、电子钥匙设备等

为实现上述功能，包含了执行各个功能相应的硬件结构和软件模块中的最少一种。本领域技术人员应该很容易意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，本申请能够以硬件或硬件和计算机软件的结合形式来实现。某个功能究竟以硬件还是计算机软件驱动硬件的方式来执行，取决于技术方案的特定应用和设计约束条件。专业技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

例如，一些实施例中，车载设备可以包括处理模块和收发模块。所述收发模块可以用于执行方法 100、方法 300、方法 500 至方法 800 中车载设备与电子钥匙设备之间信息的收发。所述处理模块可以用于执行方法 100、方法 300、方法 500 至方法 800 中车载设备除信息收发之外的操作。

可以理解的是，以上各个模块的划分仅仅是一种逻辑功能的划分，实际实现时，所述收发模块的功能可以集成到收发器，所述处理模块的功能可以集成到处理器实现。如图 5A 所示，车载设备 50 包括处理器 501 和收发器 502。所述收发器 502 可以执行方法 100 至方法 800 中车载设备与电子钥匙设备之间信息的收发。所述处理器 501 可以执行方法 100 至方法 800 中车载设备除信息收发之外的操作。

例如，一些实施例中，该收发器 502 可以用于通过第一通信通道从第一设备接收第一标识，第一标识用于标识与第二通信通道类型相同的通信通道，第一通信通道和第二通信通道相互独立，且均用于连接车载设备和第一设备。该处理器 501 可以用于确定第二通信通道的通道标识。该处理器 501 还可以用于当车载设备与第一设备的距离在预设距离之内，且第二通信通道的通道标识与第一标识匹配时，响应预先接收的业务指令打开车门。

再如，另一些实施例中，该收发器 502 可以用于从第一设备接收业务指令，业务指令包含第一业务数据通道标识和第一测距通道标识，第一业务数据通道标识用于标识电子钥匙设备所连接的业务数据通道，第一测距通道标识用于标识电子钥匙设备所连接的测距通道。该处理器 501 可以用于确定第二业务数据通道标识和第二测距通道标识，第二业务数据通道标识用于标识车载设备所连接的业务数据通道，第二测距通道标识用于标识车载设备所连接的测距通道。该处理器 501 还可以用于当车载设备与第一设备的距离在预设距离之内，第一业务数据通道标识和第二业务数据通道标识相匹配，且第一测距通道标识和第二测距通道标识相同时，响应业务指令打开车门。

具体内容可以参考方法 100、方法 300、方法 500 至方法 800 对应的实施例中车载设备相关的描述，此处不再赘述。

图 5A 是从独立功能实体的角度对本申请的车载设备进行描述。在另一种实施场景中，各独立运行的功能实体可以集成在一个硬件实体中，相应的，如图 5B 所示，本实施场景中，车载设备 51 可以包括处理器 511、收发器 512 和存储器 513。其中，存储器 513 可以用于存储车载设备 51 预装的程序/代码，也可以存储用于处理器 511 执行时的代码等。

应理解，本申请的车载设备 51 可对应于本申请的方法 100、方法 300、方法 500 至方法 800 对应的实施例中的车载设备，其中收发器 512 用于执行收发器 512 对应的实施例中车载设备执行的信息的收发，处理器 511 用于执行上述方法 100、方法 300、方法 500 至方法 800 对应的实施例中车载设备除了信息收发之外的其它处理。在此不再赘述。

具体内容可以参考方法 100、方法 300、方法 500 至方法 800 对应的实施例中车载设备相关的描述，此处不再赘述。

同理，一些实施例中，电子钥匙设备可以包括处理模块和收发模块。所述收发模块可以用于执行方法 200、方法 400 至方法 800 中电子钥匙设备与车载设备之间信息的收发。所述处理模块可以用于执行方法 200、方法 400 至方法 800 中电子钥匙设备除信息收发之外的操作。

可以理解的是，以上各个模块的划分仅仅是一种逻辑功能的划分，实际实现时，所述收发模块的功能可以集成到收发器，所述处理模块的功能可以集成到处理器实现。如图 6A 所示，电子钥匙设备 60 包括处理器 601 和收发器 602。所述收发器 602 可以执行方法 200、方法 400 至方法 800 对应的实施例中电子钥匙设备所执行的信息的收发。所述处理器 601 可以执行方法 200、方法 400 至方法 800 对应的

5 实施例中电子钥匙设备除信息收发之外的操作。

例如，一些实施例中，该处理器 601 可以用于与第二设备建立第一通信通道。该处理器 601 还可以用于生成第一标识，第一标识用于标识与第二通信通道类型相同的通信通道，第二通信通道用于连接电子钥匙设备和第二设备，第一通信通道和第二通信通道相互独立。该收发器 602 可以用于通过第一通信通道向第二设备发送所述第一标识。

10 再如，另一些实施例中，该处理器 601 可以用于与第二设备建立业务数据通道和测距通道。该处理器 601 还可以用于确定第一业务数据通道标识和第一测距通道标识，第一业务数据通道标识用于标识业务数据通道，第一测距通道标识用于标识所述测距通道。该处理器 601 还可以用于生成业务指令，业务指令包括第一业务数据通道标识和第一测距通道标识。该收发器 602 可以用于通过业务数据通道向第二设备发送业务指令。

15 具体内容可以参考方法 200、方法 400 至方法 800 对应的实施例中电子钥匙设备相关的描述，此处不再赘述。

图 6A 是从独立功能实体的角度对本申请的电子钥匙设备进行描述。在另一种实施场景中，各独立运行的功能实体可以集成在一个硬件实体中，相应的，如图 6B 所示，本实施场景中，电子钥匙设备 61 可以包括处理器 611、收发器 612 和存储器 613。其中，存储器 613 可以用于存储电子钥匙设备 61 预装

20 的程序/代码，也可以存储用于处理器 611 执行时的代码等。

应理解，本申请的电子钥匙设备 61 可对应于本申请的方法 200、方法 400 至方法 800 对应的实施例中的电子钥匙设备，其中收发器 612 用于执行收发器 612 对应的实施例中电子钥匙设备执行的信息的收发，处理器 611 用于执行上述方法 200、方法 400 至方法 800 对应的实施例中电子钥匙设备除了信息收发之外的其它处理。在此不再赘述。

25 具体内容可以参考方法 200、方法 400 至方法 800 对应的实施例中电子钥匙设备相关的描述，此处不再赘述。

具体实现中，对应车载设备和电子钥匙设备，本申请还分别提供一种计算机存储介质，其中，设置在任意设备中的计算机存储介质可存储有程序，该程序执行时，可实施包括图 3A 至图 4E 提供的基于通信通道检测中继攻击的方法的各实施例中的部分或全部步骤。任意设备中的存储介质均可为磁碟、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。

30

本申请中，收发器可以是有线收发器，无线收发器或其组合。有线收发器例如可以为以太网接口。以太网接口可以是光接口，电接口或其组合。无线收发器例如可以为无线局域网收发器，蜂窝网络收发器或其组合。处理器可以是中央处理器 (central processing unit, CPU)，网络处理器 (network processor, NP) 或者 CPU 和 NP 的组合。处理器还可以进一步包括硬件芯片。上述硬件芯片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。上述 PLD 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)，通用阵列逻辑 (generic array logic, GAL) 或其任意组合。存储器可以包括易失性存储器 (volatile memory)，例如随机存取存储器 (random-access memory, RAM)；存储器也可以包括非易失性存储器 (non-volatile memory)，

35

例如只读存储器 (read-only memory, ROM), 快闪存储器 (flash memory), 硬盘 (hard disk drive, HDD) 或固态硬盘 (solid-state drive, SSD); 存储器还可以包括上述种类的存储器的组合。

图 5B 和图 6B 中还可以包括总线接口, 总线接口可以包括任意数量的互联的总线和桥, 具体由处理器代表的一个或多个处理器和存储器代表的存储器的各种电路链接在一起。总线接口还可以将诸如外围设备、稳压器和功率管理电路等之类的各种其他电路链接在一起, 这些都是本领域所公知的, 因此, 本文不再对其进行进一步描述。总线接口提供接口。收发器提供用于在传输介质上与各种其他设备通信的单元。处理器负责管理总线架构和通常的处理, 存储器可以存储处理器在执行操作时所使用的报文。

本领域技术任何还可以了解到本申请实施例列出的各种说明性逻辑块 (illustrative logical block) 和步骤 (step) 可以通过电子硬件、电脑软件, 或两者的结合进行实现。这样的功能是通过硬件还是软件来实现取决于特定的应用和整个系统的设计要求。本领域技术人员可以对于每种特定的应用, 可以使用各种方法实现所述的功能, 但这种实现不应被理解为超出本申请实施例保护的范围。

本申请实施例中所描述的各种说明性的逻辑单元和电路可以通过通用处理器, 数字信号处理器, 专用集成电路 (ASIC), 现场可编程门阵列 (FPGA) 或其它可编程逻辑装置, 离散门或晶体管逻辑, 离散硬件部件, 或上述任何组合的设计来实现或操作所描述的功能。通用处理器可以为微处理器, 可选地, 该通用处理器也可以为任何传统的处理器、控制器、微控制器或状态机。处理器也可以通过计算装置的组合来实现, 例如数字信号处理器和微处理器, 多个微处理器, 一个或多个微处理器联合一个数字信号处理器核, 或任何其它类似的配置来实现。

本申请实施例中所描述的方法或算法的步骤可以直接嵌入硬件、处理器执行的软件单元、或者这两者的结合。软件单元可以存储于 RAM 存储器、闪存、ROM 存储器、EPROM 存储器、EEPROM 存储器、寄存器、硬盘、可移动磁盘、CD-ROM 或本领域中其它任意形式的存储媒介中。示例性地, 存储媒介可以与处理器连接, 以使得处理器可以从存储媒介中读取信息, 并可以向存储媒介存写信息。可选地, 存储媒介还可以集成到处理器中。处理器和存储媒介可以设置于 ASIC 中, ASIC 可以设置于 UE 中。可选地, 处理器和存储媒介也可以设置于 UE 中的不同的部件中。

应理解, 在本申请的各种实施例中, 各过程的序号的大小并不意味着执行顺序的先后, 各过程的执行顺序应以其功能和内在逻辑确定, 而不对实施例的实施过程构成任何限定。

在上述实施例中, 可以全部或部分地通过软件、硬件、固件或者其任意组合来实现。当使用软件实现时, 可以全部或部分地以计算机程序产品的形式实现。所述计算机程序产品包括一个或多个计算机指令。在计算机上加载和执行所述计算机程序指令时, 全部或部分地产生按照本申请所述的流程或功能。所述计算机可以是通用计算机、专用计算机、计算机网络、或者其他可编程装置。所述计算机指令可以存储在计算机可读存储介质中, 或者从一个计算机可读存储介质向另一个计算机可读存储介质传输, 例如, 所述计算机指令可以从一个网站站点、计算机、服务器或报文中心通过有线 (例如同轴电缆、光纤、数字用户线 (DSL)) 或无线 (例如红外、无线、微波等) 方式向另一个网站站点、计算机、服务器或报文中心进行传输。所述计算机可读存储介质可以是计算机能够存取的任何可用介质或者是包含一个或多个可用介质集成的服务器、报文中心等报文存储设备。所述可用介质可以是磁性介质, (例如, 软盘、硬盘、磁带)、光介质 (例如, DVD)、或者半导体介质 (例如固态硬盘 (solid state disk, SSD)) 等。

本说明书的各个部分均采用递进的方式进行描述, 各个实施例之间相同相似的部分互相参见即可, 每个实施例重点介绍的都是与其他实施例不同之处。尤其, 对于装置和系统实施例而言, 由于其基本相似于方法实施例, 所以描述的比较简单, 相关之处参见方法实施例部分的说明即可。

另外, 本申请提及的“第一”以及“第二”等序数词, 用于对多个相同属性但包含不同内容的对象

进行区分。

尽管已描述了本申请的优选实施例，但本领域内的技术人员一旦得知了基本创造性概念，则可对这些实施例作出另外的变更和修改。所以，所附权利要求意欲解释为包括优选实施例以及落入本申请范围的所有变更和修改。

- 5 显然，本领域的技术人员可以对本申请进行各种改动和变型而不脱离本申请的精神和范围。这样，倘若本申请的这些修改和变型属于本申请权利要求及其等同技术的范围之内，则本申请也意图包含这些改动和变型在内。

权 利 要 求 书

1、一种基于通信通道检测中继攻击的方法，其特征在于，所述方法包括：

车载设备通过第一通信通道从第一设备接收第一标识，所述第一标识用于标识与第二通信通道类型相同的通信通道，所述第一通信通道和所述第二通信通道相互独立，且均用于连接所述车
5 载设备和所述第一设备；

所述车载设备确定所述第二通信通道的通道标识；

当所述车载设备与所述第一设备的距离在预设距离之内，且所述第二通信通道的通道标识与所述第一标识匹配时，所述车载设备响应预先接收的业务指令打开车门。

2、如权利要求 1 所述的方法，其特征在于，所述车载设备通过第一通信通道从第一设备接收
10 第一标识，包括：

当所述第一通信通道是业务数据通道时，所述车载设备通过所述业务数据通道从所述第一设备接收会话密文，所述业务数据通道用于传输业务数据，测距通道标识用于标识所述测距通道；
或者，

当所述第一通信通道是测距通道时，所述车载设备通过所述测距通道从所述第一设备接收测
15 距确认字符 ACK 帧，所述测距 ACK 帧中包含业务数据通道标识，所述测距通道用于传输测距数据。

3、如权利要求 2 所述的方法，其特征在于，所述会话密文是将测距通道标识加密得到的。

4、如权利要求 1 所述的方法，其特征在于，所述车载设备确定所述第二通信通道的通道标识，
包括：

当所述第二通信通道是业务数据通道时，所述车载设备根据第一规则提取所述第二通信通道的通道信息中的至少一个信息，所述第二通信通道的通道信息包括以下一项或多项：业务数据通道的传输频段、时域信息、频域信息、多径延迟信息、信号强度、信号相位，所述第一规则用于指示所述车载设备确定业务数据通道标识；
20

所述车载设备根据所述通道信息中的至少一个信息生成所述第二通信通道的业务数据通道标识；或者，

当所述第二通信通道是测距通道时，所述车载设备根据第二规则获取所述第二通信通道的通道信息中的指定信息作为所述第二通信通道的测距通道标识，所述第二通信通道的通道信息包括测距通道的通用唯一识别码 UUID、测距通道地址、测距通道的会话标识、测距通道会话的前导序列和测距帧返回的时间戳，所述第二规则用于指示所述车载设备确定测距通道标识。
25

5、如权利要求 1 至 4 中任一项所述的方法，其特征在于，在所述车载设备确定所述第二通信通道的通道标识之后，在所述车载设备响应预先接收的业务指令打开车门之前，还包括：
30

当所述第二通信通道的通道标识和所述第一标识是业务数据通道标识时，所述车载设备检测所述第二通信通道的通道标识与所述第一标识的相似度参数大于预设阈值，则确定所述第二通信通道的通道标识与所述第一标识相匹配；或者，

当所述第二通信通道的通道标识和所述第一标识是测距通道标识时，所述车载设备检测所述
35 第二通信通道的通道标识与所述第一标识相同，则确定所述第二通信通道的通道标识与所述第一标识相匹配。

6、如权利要求 1 至 5 中任一项所述的方法，其特征在于，所述车载设备通过第一通信通道从第一设备接收第一标识之前，还包括：

所述车载设备通过与所述第一设备相连接的业务数据通道接收业务指令；

所述车载设备建立与所述第一设备相连接的测距通道。

7、一种基于通信通道检测中继攻击的方法，其特征在于，所述方法包括：

车载设备从第一设备接收业务指令，所述业务指令包含第一业务数据通道标识和第一测距通道标识，所述第一业务数据通道标识用于标识电子钥匙设备所连接的业务数据通道，所述第一测距通道标识用于标识所述电子钥匙设备所连接的测距通道；

所述车载设备确定第二业务数据通道标识和第二测距通道标识，所述第二业务数据通道标识用于标识所述车载设备所连接的业务数据通道，所述第二测距通道标识用于标识所述车载设备所连接的测距通道；

当所述车载设备与所述第一设备的距离在预设距离之内，所述第一业务数据通道标识和所述第二业务数据通道标识相匹配，且所述第一测距通道标识和所述第二测距通道标识相同时，所述车载设备响应所述业务指令打开车门。

8、一种基于通信通道检测中继攻击的方法，其特征在于，所述方法包括：

电子钥匙设备与第二设备建立第一通信通道；

所述电子钥匙设备生成第一标识，所述第一标识用于标识与第二通信通道类型相同的通信通道，所述第二通信通道用于连接所述电子钥匙设备和所述第二设备，所述第一通信通道和所述第二通信通道相互独立；

所述电子钥匙设备通过所述第一通信通道向所述第二设备发送所述第一标识。

9、如权利要求 8 所述的方法，其特征在于，所述电子钥匙设备生成第一标识包括：

当所述第二通信通道是业务数据通道时，所述电子钥匙设备根据第一规则提取所述第二通信通道的通道信息中的至少一个信息，所述第二通信通道的通道信息包括以下一项或多项：业务数据通道的传输频段、时域信息、频域信息、多径延迟信息、信号强度、信号相位，所述第一规则用于指示车载设备确定业务数据通道标识；

所述电子钥匙设备根据所述通道信息中的至少一个信息生成所述第二通信通道的业务数据通道标识，得到所述第一标识；

或者，

当所述第二通信通道是测距通道时，所述电子钥匙设备根据第二规则获取所述第二通信通道的通道信息中的指定信息作为所述第二通信通道的测距通道标识，得到所述第一标识，所述第二通信通道的通道信息包括测距通道的通用唯一识别码 UUID、测距通道地址、测距通道的会话标识、测距通道会话的前导序列和测距帧返回的时间戳，所述第二规则用于指示所述车载设备确定测距通道标识。

10、如权利要求 9 所述的方法，其特征在于，所述电子钥匙设备通过所述第一通信通道向所述第二设备发送所述第一标识，包括：

当所述第一标识是业务数据通道标识时，所述电子钥匙设备将所述业务数据通道标识携带在测距确认字符 ACK 帧中，并通过所述测距通道发送所述测距 ACK 帧；或者，

当所述第一标识是测距通道标识时，所述电子钥匙设备将所述测距通道标识加密得到会话密文，并通过所述业务数据通道测距通道发送所述会话密文。

11、如权利要求 9 或 10 所述的方法，其特征在于，当所述第一通信通道是所述业务数据通道时，电子钥匙设备与第二设备建立第一通信通道之后，生成第一标识之前，还包括：

所述电子钥匙设备通过所述业务数据通道向所述第二设备发送业务指令；

所述电子钥匙设备与所述第二设备建立所述测距通道。

12、一种基于通信通道检测中继攻击的方法，其特征在于，所述方法包括：

电子钥匙设备与第二设备建立业务数据通道和测距通道；

5 所述电子钥匙设备确定第一业务数据通道标识和第一测距通道标识，所述第一业务数据通道标识用于标识所述业务数据通道，所述第一测距通道标识用于标识所述测距通道；

所述电子钥匙设备生成业务指令，所述业务指令包括所述第一业务数据通道标识和所述第一测距通道标识；

所述电子钥匙设备通过所述业务数据通道向所述第二设备发送所述业务指令。

13、一种车载设备，其特征在于，所述车载设备包括处理器和收发器，其中，

10 所述收发器，用于通过第一通信通道从第一设备接收第一标识，所述第一标识用于标识与第二通信通道类型相同的通信通道，所述第一通信通道和所述第二通信通道相互独立，且均用于连接所述车载设备和所述第一设备；

所述处理器，用于确定所述第二通信通道的通道标识；

15 所述处理器，还用于当所述车载设备与所述第一设备的距离在预设距离之内，且所述第二通信通道的通道标识与所述第一标识匹配时，响应预先接收的业务指令打开车门。

14、如权利要求 13 所述的车载设备，其特征在于，

所述收发器，还用于当所述第一通信通道是业务数据通道时，通过所述业务数据通道从所述第一设备接收会话密文，所述业务数据通道用于传输业务数据，测距通道标识用于标识所述测距通道；

20 所述收发器，还用于当所述第一通信通道是测距通道时，通过所述测距通道从所述第一设备接收测距确认字符 ACK 帧，所述测距 ACK 帧中包含业务数据通道标识，所述测距通道用于传输测距数据，所述业务数据通道标识用于标识所述业务数据通道。

15、如权利要求 14 所述的车载设备，其特征在于，所述会话密文是将测距通道标识加密得到的。

25 16、如权利要求 13 所述的车载设备，其特征在于，

所述处理器，还用于当所述第二通信通道是业务数据通道时，根据第一规则提取所述第二通信通道的通道信息中的至少一个信息，所述第二通信通道的通道信息包括以下一项或多项：业务数据通道的传输频段、时域信息、频域信息、多径延迟信息、信号强度、信号相位，所述第一规则用于指示所述车载设备确定业务数据通道标识；

30 所述处理器，还用于根据所述通道信息中的至少一个信息生成所述第二通信通道的业务数据通道标识；

所述处理器，还用于当所述第二通信通道是测距通道时，根据第二规则获取所述第二通信通道的通道信息中的指定信息作为所述第二通信通道的测距通道标识，所述第二通信通道的通道信息包括测距通道的通用唯一识别码 UUID、测距通道地址、测距通道的会话标识、测距通道会话的前导序列和测距帧返回的时间戳，所述第二规则用于指示所述车载设备确定测距通道标识。

17、如权利要求 13 至 16 中任一项所述的车载设备，其特征在于，

所述处理器，还用于当所述第二通信通道的通道标识和所述第一标识是业务数据通道标识时，检测所述第二通信通道的通道标识与所述第一标识的相似度参数大于预设阈值，则确定所述第二通信通道的通道标识与所述第一标识相匹配；

所述处理器，还用于当所述第二通信通道的通道标识和所述第一标识是测距通道标识时，检测所述第二通信通道的通道标识与所述第一标识相同，则确定所述第二通信通道的通道标识与所述第一标识相匹配。

18、如权利要求 13 至 17 中任一项所述的车载设备，其特征在于，

5 所述收发器，还用于通过与所述第一设备相连接的业务数据通道接收业务指令；

所述处理器，还用于建立与所述第一设备相连接的测距通道。

19、一种车载设备，其特征在于，所述车载设备包括处理器和收发器，其中，

所述收发器，用于从第一设备接收业务指令，所述业务指令包含第一业务数据通道标识和第一测距通道标识，所述第一业务数据通道标识用于标识电子钥匙设备所连接的业务数据通道，所述
10 所述第一测距通道标识用于标识所述电子钥匙设备所连接的测距通道；

所述处理器，用于确定第二业务数据通道标识和第二测距通道标识，所述第二业务数据通道标识用于标识所述车载设备所连接的业务数据通道，所述第二测距通道标识用于标识所述车载设备所连接的测距通道；

所述处理器，还用于当所述车载设备与所述第一设备的距离在预设距离之内，所述第一业务
15 数据通道标识和所述第二业务数据通道标识相匹配，且所述第一测距通道标识和所述第二测距通道标识相同时，响应所述业务指令打开车门。

20、一种电子钥匙设备，其特征在于，所述电子钥匙设备包括处理器和收发器，其中，

所述处理器，用于与第二设备建立第一通信通道；

所述处理器，还用于生成第一标识，所述第一标识用于标识与第二通信通道类型相同的通信
20 通道，所述第二通信通道用于连接所述电子钥匙设备和所述第二设备，所述第一通信通道和所述第二通信通道相互独立；

所述收发器，用于通过所述第一通信通道向所述第二设备发送所述第一标识。

21、如权利要求 20 所述的电子钥匙设备，其特征在于，

所述处理器，还用于当所述第二通信通道是业务数据通道时，根据第一规则提取所述第二通信
25 通道的通道信息中的至少一个信息，所述第二通信通道的通道信息包括以下一项或多项：业务数据通道的传输频段、时域信息、频域信息、多径延迟信息、信号强度、信号相位，所述第一规则用于指示车载设备确定业务数据通道标识；

所述处理器，还用于根据所述通道信息中的至少一个信息生成所述第二通信通道的业务数据通道标识，得到所述第一标识；

30 所述处理器，还用于当所述第二通信通道是测距通道时，根据第二规则获取所述第二通信通道的通道信息中的指定信息作为所述第二通信通道的测距通道标识，得到所述第一标识，所述第二通信通道的通道信息包括测距通道的通用唯一识别码 UUID、测距通道地址、测距通道的会话标识、测距通道会话的前导序列和测距帧返回的时间戳，所述第二规则用于指示所述车载设备确定测距通道标识。

35 22、如权利要求 21 所述的电子钥匙设备，其特征在于，

所述处理器，还用于当所述第一标识是业务数据通道标识时，将所述业务数据通道标识携带在测距确认字符 ACK 帧中，并通过所述测距通道发送所述测距 ACK 帧；

所述处理器，还用于当所述第一标识是测距通道标识时，将所述测距通道标识加密得到会话密文，并通过所述业务数据通道测距通道发送所述会话密文。

23、如权利要求 21 或 22 所述的电子钥匙设备，其特征在于，

所述收发器，还用于通过所述业务数据通道向所述第二设备发送业务指令；

所述处理器，还用于与所述第二设备建立所述测距通道。

24、一种电子钥匙设备，其特征在于，所述电子钥匙设备包括处理器和收发器，其中，

5 所述处理器，用于与第二设备建立业务数据通道和测距通道；

所述处理器，还用于确定第一业务数据通道标识和第一测距通道标识，所述第一业务数据通道标识用于标识所述业务数据通道，所述第一测距通道标识用于标识所述测距通道；

所述处理器，还用于生成业务指令，所述业务指令包括所述第一业务数据通道标识和所述第一测距通道标识；

10 所述收发器，用于通过所述业务数据通道向所述第二设备发送所述业务指令。

25、一种计算机可读存储介质，其特征在于，包括指令，当其在计算机上运行时，使得计算机执行如权利要求 1 至 6 中任一项所述的方法，或执行如权利要求 7 所述的方法，或执行如权利要求 8 至 11 中任一项所述的方法，或执行如权利要求 12 所述的方法。

26、一种计算机程序产品，其特征在于，当其在计算机上运行时，使得计算机执行如权利要求 1 至 6 中任一项所述的方法，或使得计算机执行如权利要求 7 所述的方法，或使得计算机执行如权利要求 8 至 11 中任一项所述的方法，或使得计算机执行如权利要求 12 所述的方法。

27、一种芯片，其特征在于，与存储器相连或者包括存储器，用于读取并执行所述存储器中存储的软件程序，以实现如权利要求 1 至 6 中任一项所述的方法，或以实现如权利要求 7 所述的方法，或以实现如权利要求 8 至 11 中任一项所述的方法，或以实现如权利要求 12 所述的方法。

20 28、一种通信系统，其特征在于，包括：车载设备与电子钥匙设备；

所述车载设备，用于执行如权利要求 1 至 6 中任一项所述的方法；

所述电子钥匙设备，用于执行如权利要求 8 至 11 中任一项所述的方法。

29、一种通信系统，其特征在于，包括：车载设备与电子钥匙设备；

所述车载设备，用于执行如权利要求 7 项所述的方法；

25 所述电子钥匙设备，用于执行如权利要求 12 所述的方法。

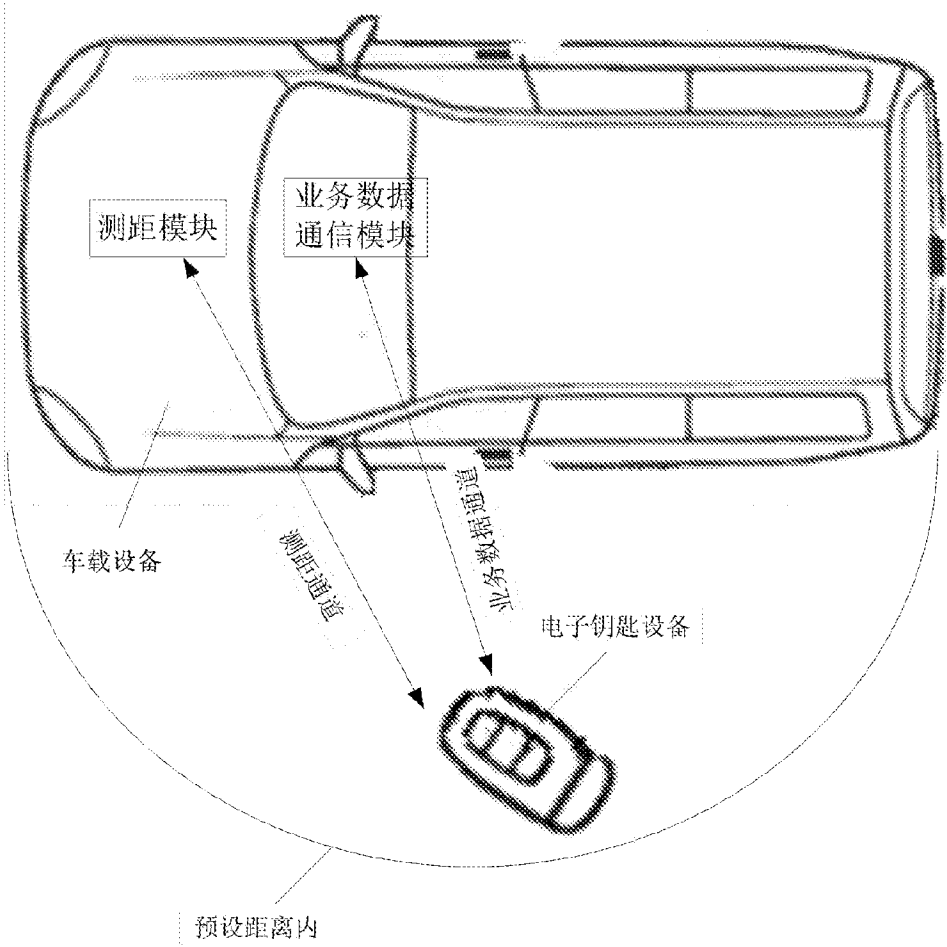


图 1A

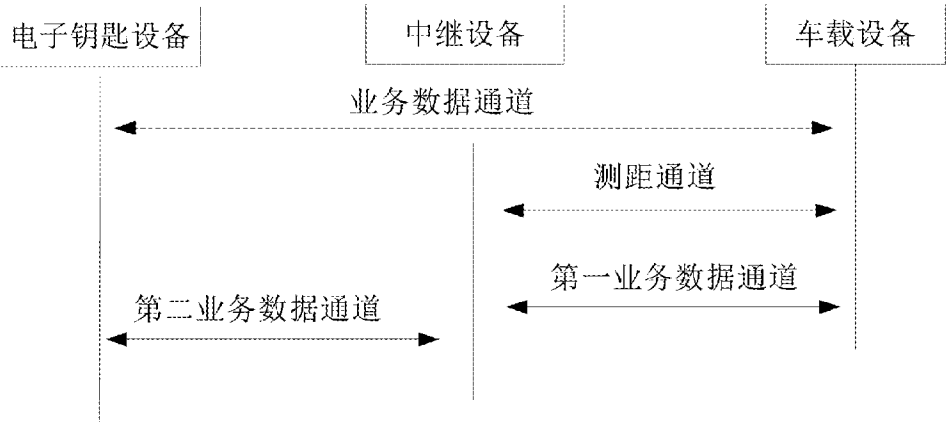


图 1B

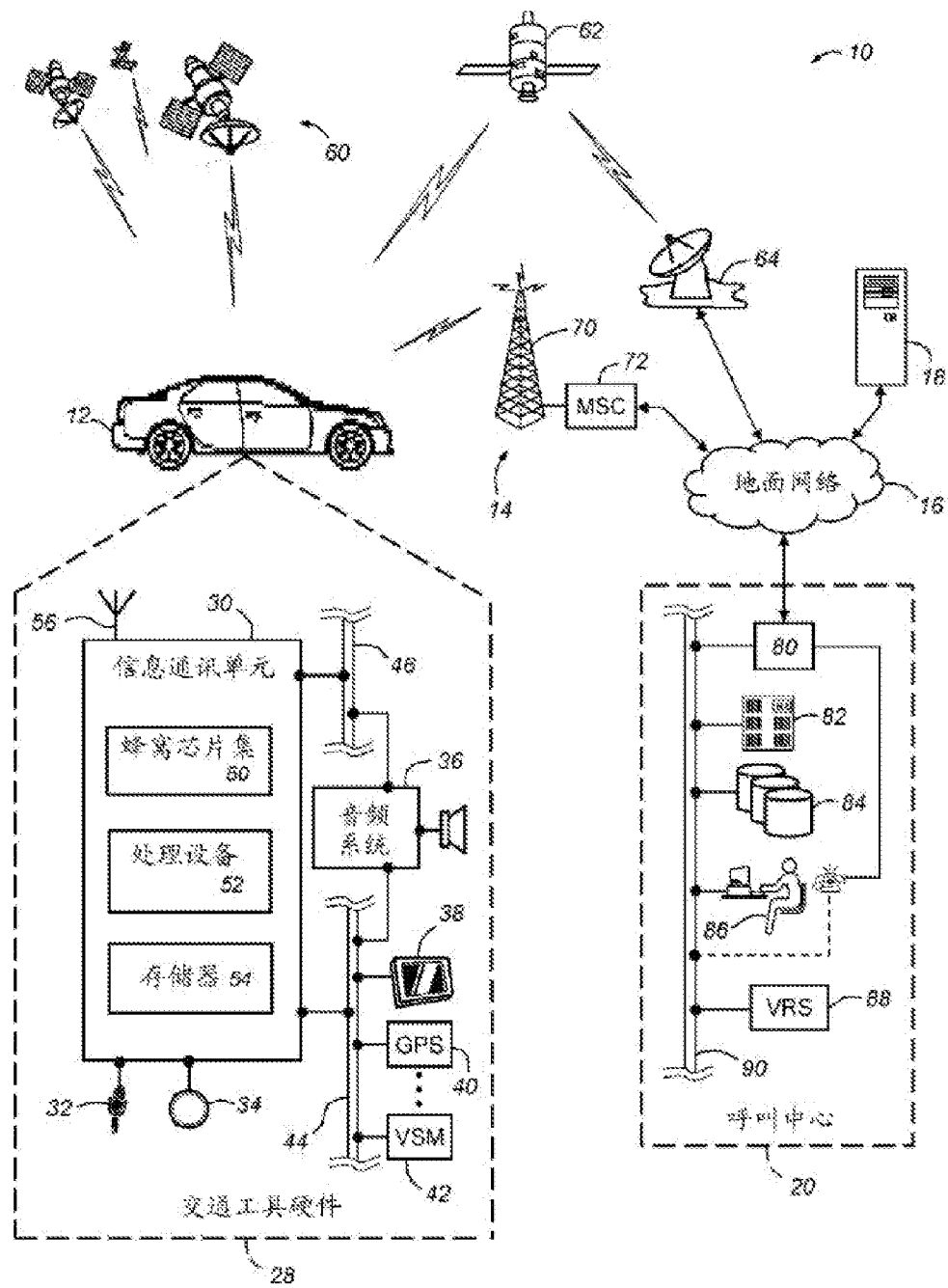


图 2A

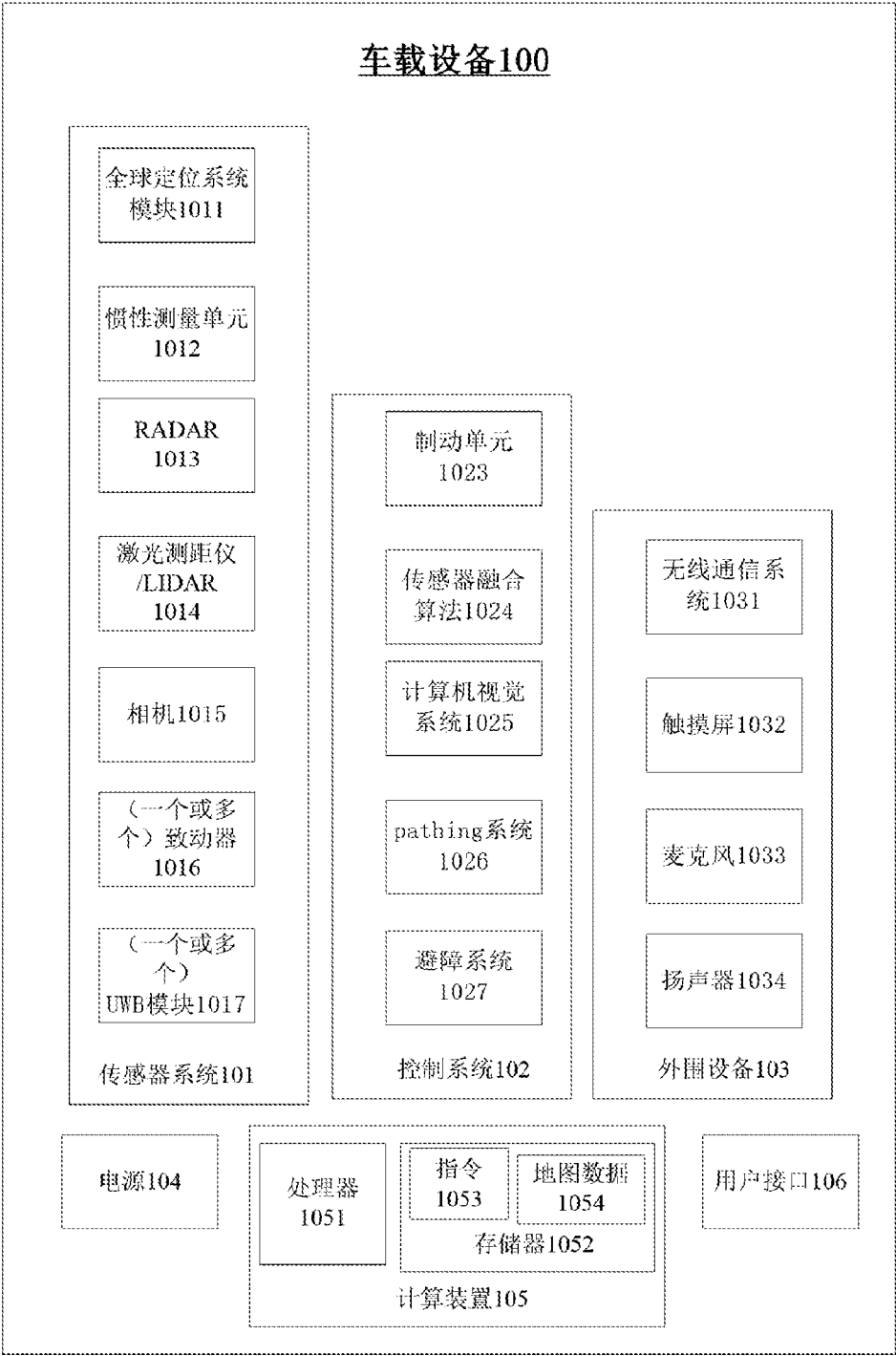


图 2B

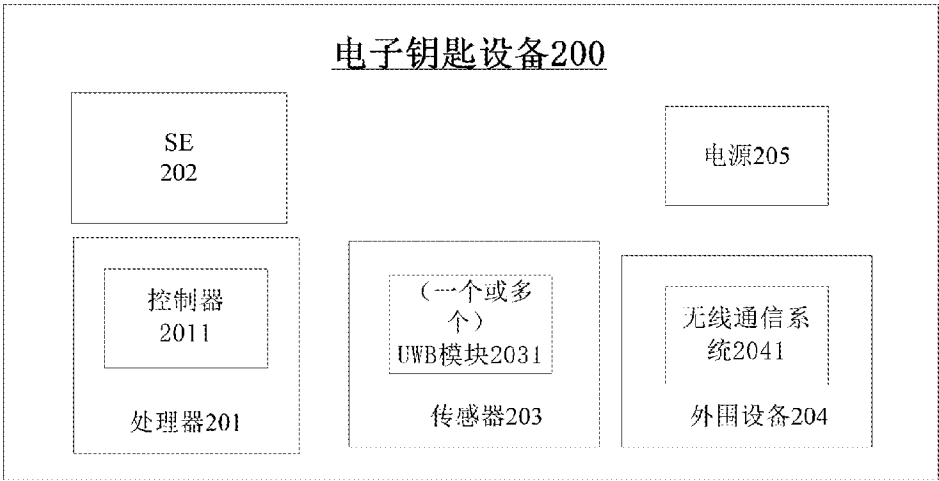


图 2C

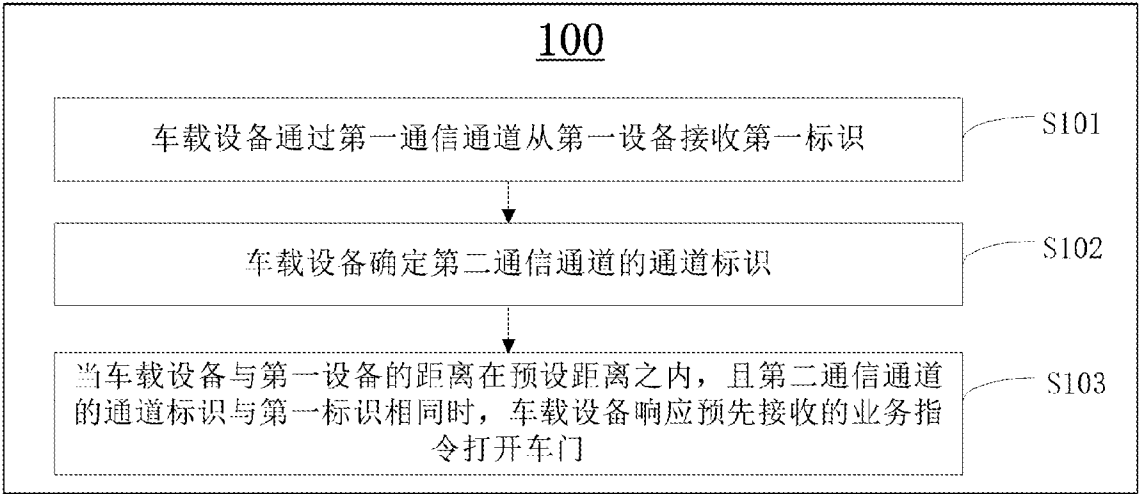


图 3A

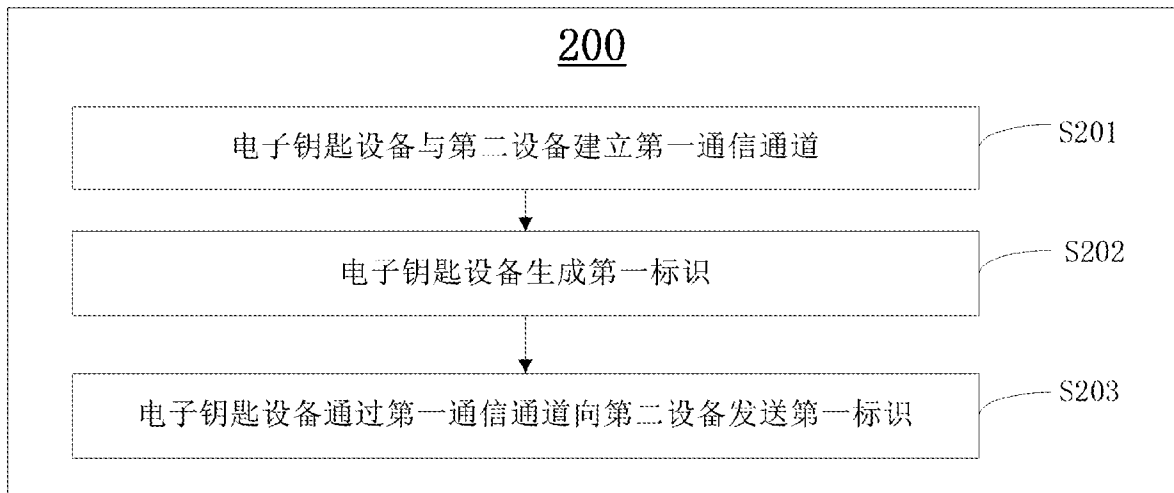


图 3B

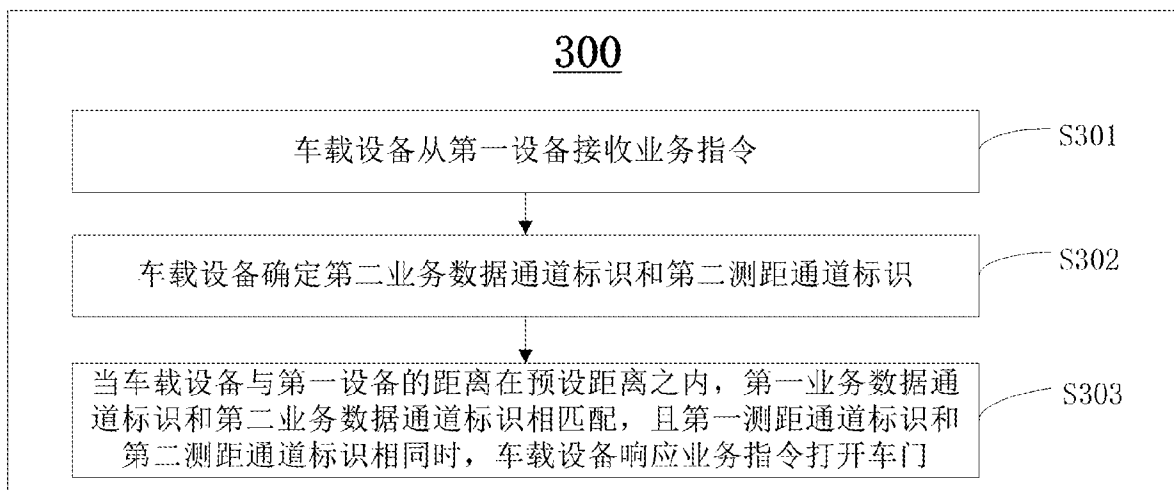


图 3C

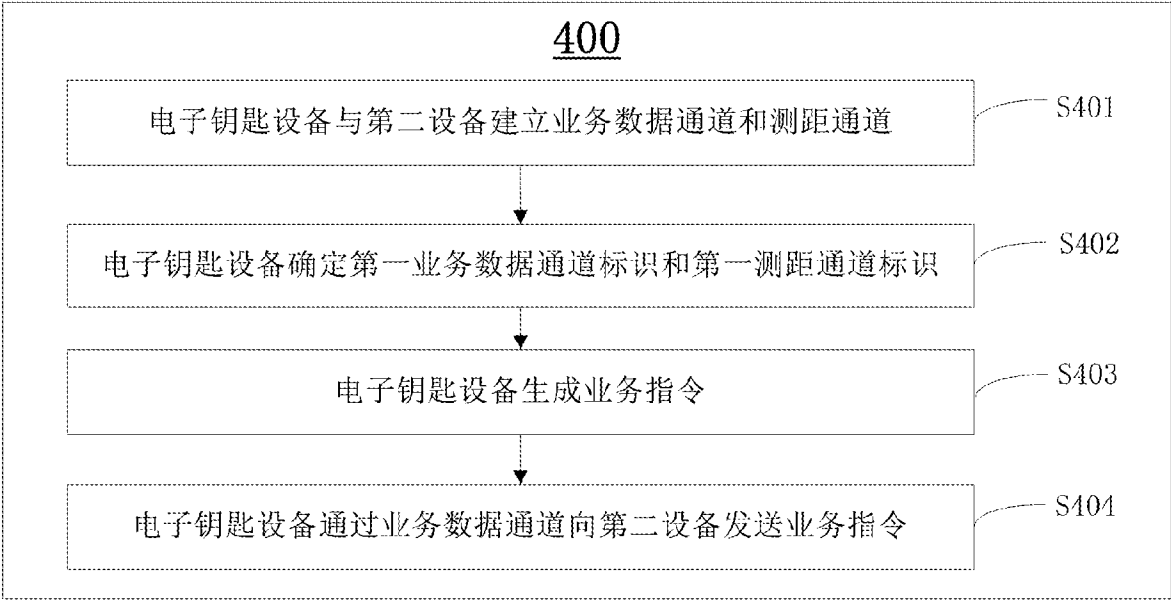


图 3D

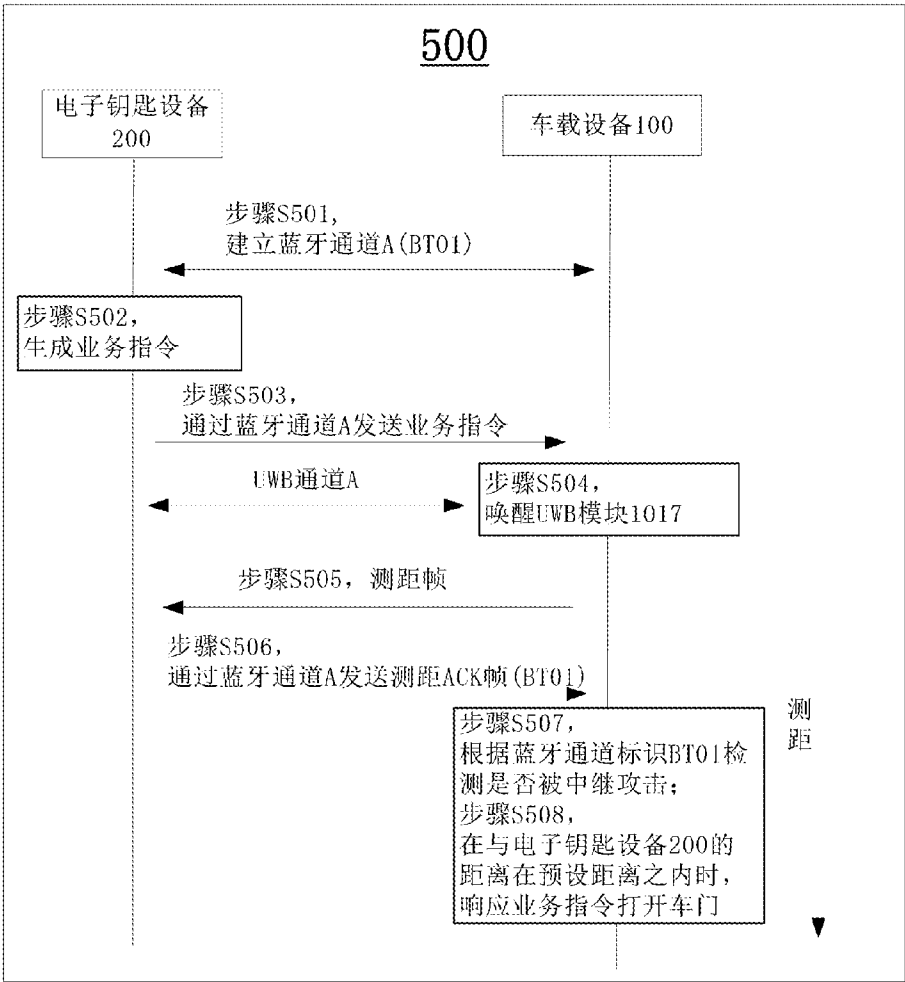


图 4A

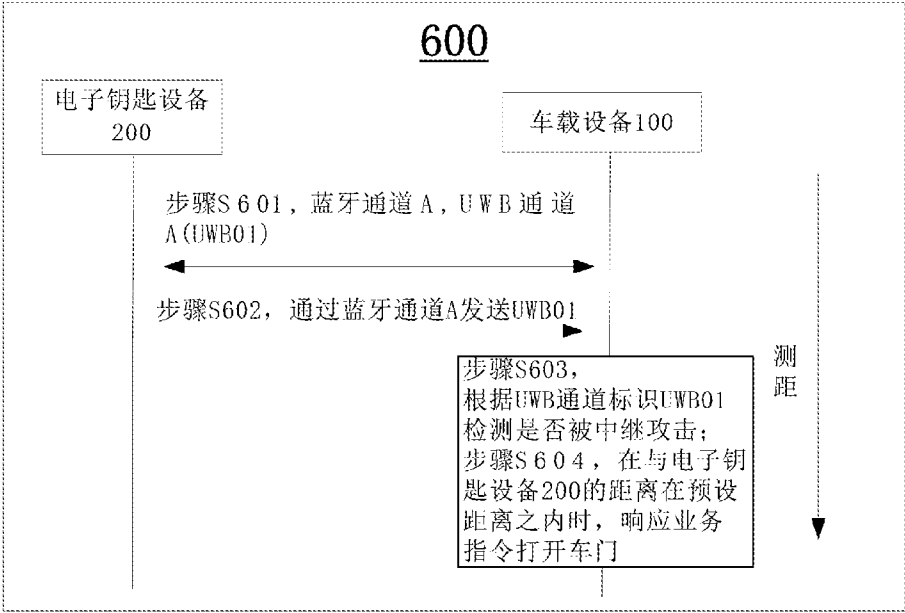


图 4B

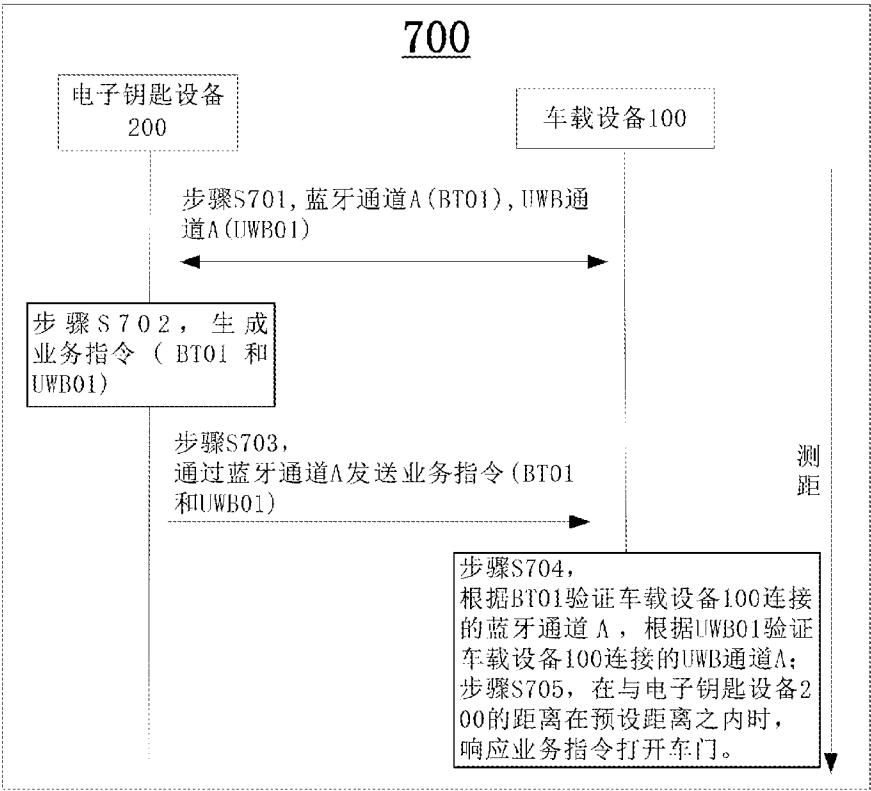


图 4C

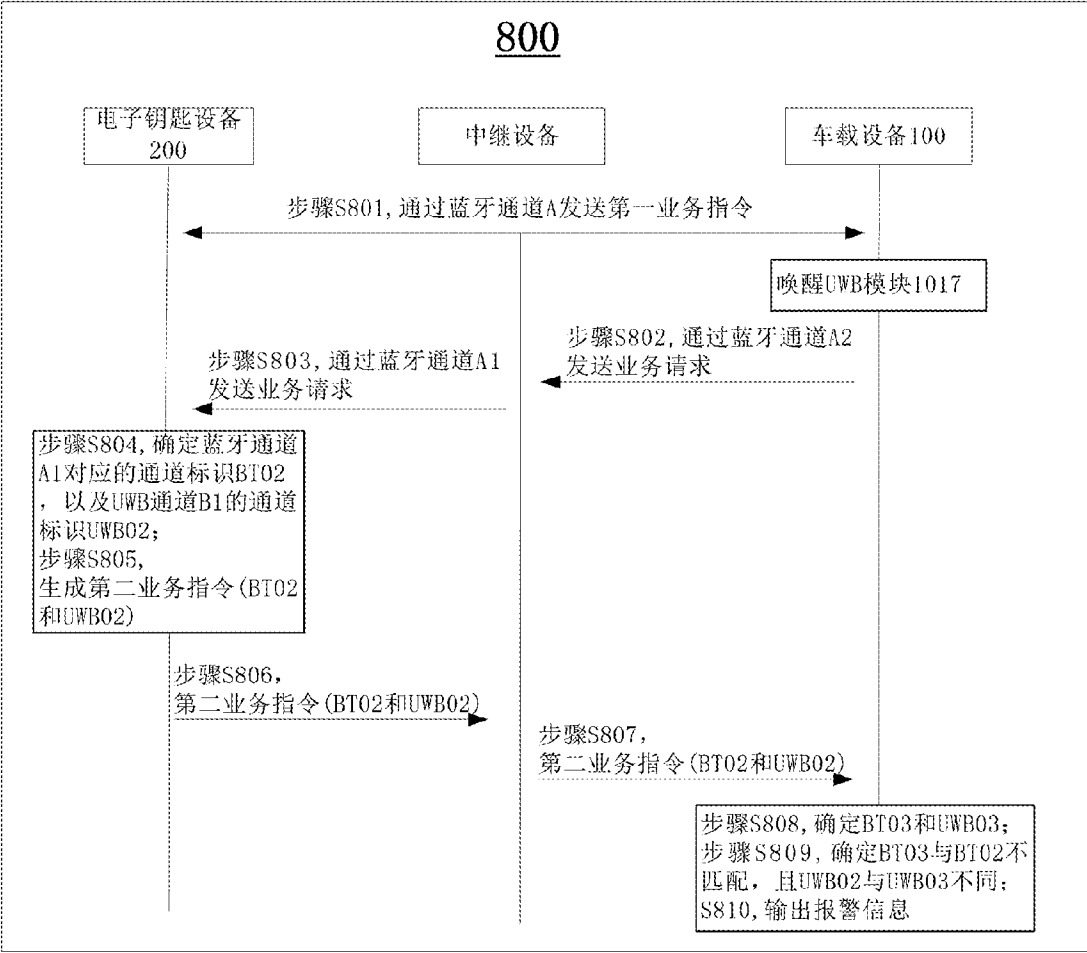


图 4D

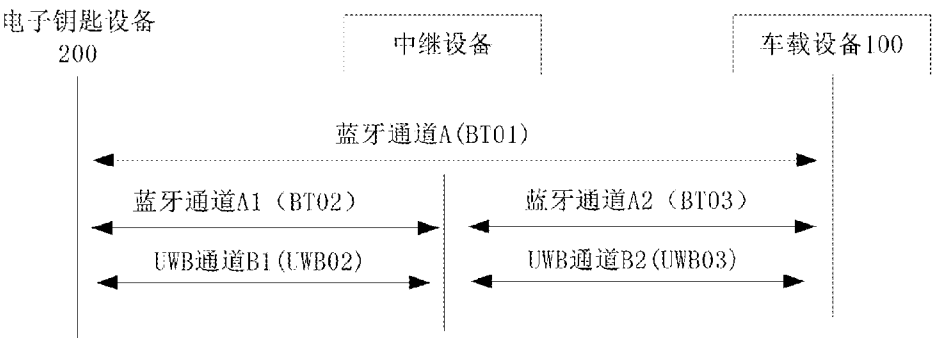


图 4E

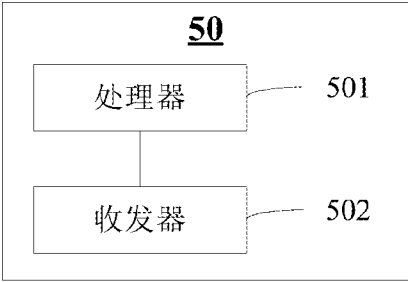


图 5A

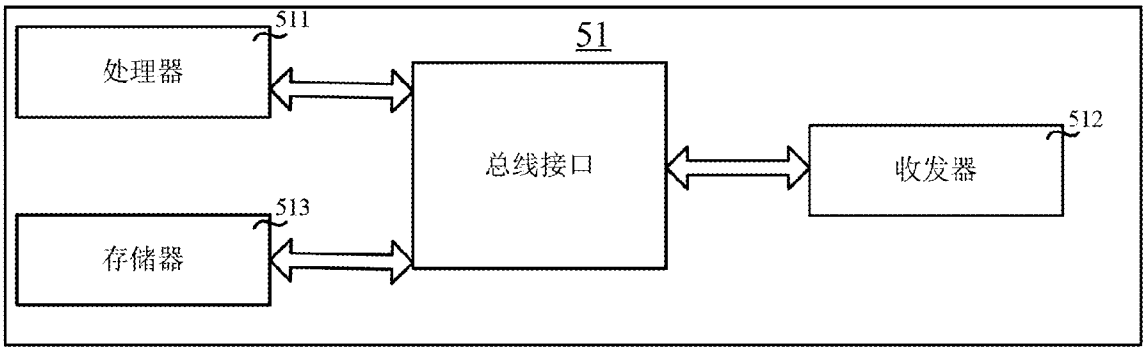


图 5B

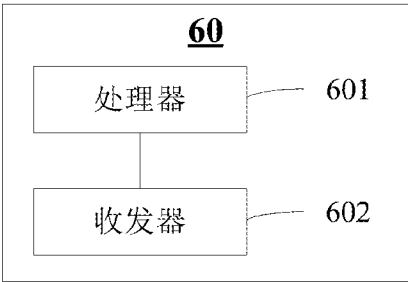


图 6A

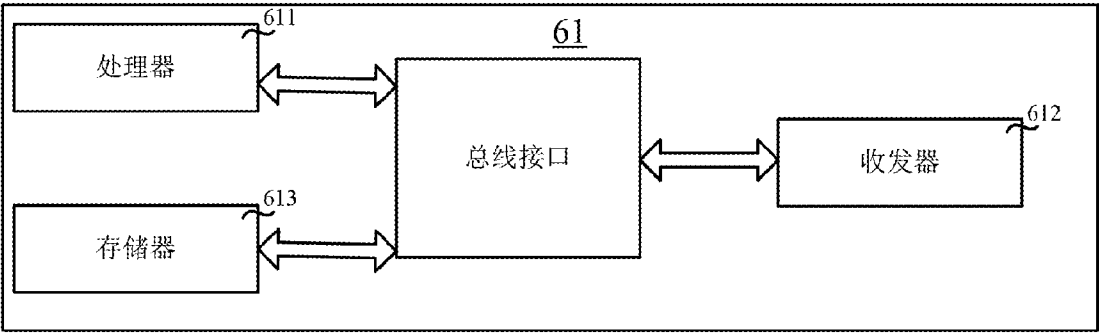


图 6B

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/105912

A. CLASSIFICATION OF SUBJECT MATTER

G07C 9/00(2020.01)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)

G07C9, H04W12, H04L29, B60R25

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)

CNABS; VEN; CNTXT: 中继, 攻击, 检测, 标识, 匹配, 距离, 强度, 相位, 延迟, relay, attack, detect, channel, identification, match, distance, intensity, phase, delay

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 110363899 A (HUAWEI TECHNOLOGIES CO., LTD.) 22 October 2019 (2019-10-22) entire document	1-29
X	CN 107968766 A (RESEARCH INSTITUTE OF CHINA MOBILE COMMUNICATIONS CORPORATION et al.) 27 April 2018 (2018-04-27) description, paragraphs 85-100, and figures 1-11	1, 7, 8, 12-13, 19-20, 24-29
A	CN 106612130 A (HYUNDAI MOTOR COMPANY) 03 May 2017 (2017-05-03) entire document	1-29
A	CN 105899413 A (HUF NORTH AMERICA AUTOMOTIVE PARTS MFG. CORP. et al.) 24 August 2016 (2016-08-24) entire document	1-29
A	CN 108632745 A (NXP B.V.) 09 October 2018 (2018-10-09) entire document	1-29
A	CN 109318856 A (GM GLOBAL TECHNOLOGY OPERATIONS LLC.) 12 February 2019 (2019-02-12) entire document	1-29
A	US 2015135268 A1 (MULTINNOVATION INC.) 14 May 2015 (2015-05-14) entire document	1-29



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

29 October 2020

Date of mailing of the international search report

05 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

Facsimile No. (86-10)62019451

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2020/105912

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2017190420 A1 (NAMSUNG CO., LTD.) 06 July 2017 (2017-07-06) entire document	1-29

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/CN2020/105912

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	110363899	A	22 October 2019	None			
CN	107968766	A	27 April 2018	None			
CN	106612130	A	03 May 2017	US	2019037374	A1	31 January 2019
				DE	102016105977	A1	27 April 2017
				KR	20170048023	A	08 May 2017
				US	10091630	B2	02 October 2018
				US	2017118573	A1	27 April 2017
				KR	101768138	B1	30 August 2017
				US	10694351	B2	23 June 2020
CN	105899413	A	24 August 2016	EP	3077254	B1	25 September 2019
				US	2017158169	A1	08 June 2017
				KR	20160096127	A	12 August 2016
				JP	2017501321	A	12 January 2017
				US	9963109	B2	08 May 2018
				JP	6609557	B2	20 November 2019
				EP	3077254	A1	12 October 2016
				KR	101771376	B1	24 August 2017
				CN	105899413	B	10 April 2018
				WO	2015084852	A1	11 June 2015
CN	108632745	A	09 October 2018	US	2018265040	A1	20 September 2018
				EP	3376475	A1	19 September 2018
CN	109318856	A	12 February 2019	US	10207677	B1	19 February 2019
				US	2019031141	A1	31 January 2019
				DE	102018118424	A1	31 January 2019
US	2015135268	A1	14 May 2015	None			
US	2017190420	A1	06 July 2017	KR	20170079673	A	10 July 2017
				US	10173772	B2	08 January 2019

国际检索报告

国际申请号

PCT/CN2020/105912

A. 主题的分类

G07C 9/00(2020.01)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)

G07C9, H04W12, H04L29, B60R25

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))

CNABS;VEN;CNTXT: 中继, 攻击, 检测, 标识, 匹配, 距离, 强度, 相位, 延迟, relay, attack, detect, channel, identification, match, distance, intensity, phase, delay

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 110363899 A (华为技术有限公司) 2019年 10月 22日 (2019 - 10 - 22) 全文	1-29
X	CN 107968766 A (中国移动通信有限公司研究院等) 2018年 4月 27日 (2018 - 04 - 27) 说明书85-100段, 附图1-11	1, 7, 8, 12-13, 19-20, 24-29
A	CN 106612130 A (现代自动车株式会社) 2017年 5月 3日 (2017 - 05 - 03) 全文	1-29
A	CN 105899413 A (胡夫北美汽车零件制造股份有限公司等) 2016年 8月 24日 (2016 - 08 - 24) 全文	1-29
A	CN 108632745 A (恩智浦有限公司) 2018年 10月 9日 (2018 - 10 - 09) 全文	1-29
A	CN 109318856 A (通用汽车环球科技运作有限责任公司) 2019年 2月 12日 (2019 - 02 - 12) 全文	1-29
A	US 2015135268 A1 (MULTINNOVATION INC) 2015年 5月 14日 (2015 - 05 - 14) 全文	1-29

☒ 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

2020年 10月 29日

国际检索报告邮寄日期

2020年 11月 5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

授权官员

李原

电话号码 86-(010)-62085846

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	US 2017190420 A1 (NAMSUNG CO LTD) 2017年 7月 6日 (2017 - 07 - 06) 全文	1-29

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2020/105912

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	110363899	A	2019年 10月 22日	无			
CN	107968766	A	2018年 4月 27日	无			
CN	106612130	A	2017年 5月 3日	US	2019037374	A1	2019年 1月 31日
				DE	102016105977	A1	2017年 4月 27日
				KR	20170048023	A	2017年 5月 8日
				US	10091630	B2	2018年 10月 2日
				US	2017118573	A1	2017年 4月 27日
				KR	101768138	B1	2017年 8月 30日
				US	10694351	B2	2020年 6月 23日
CN	105899413	A	2016年 8月 24日	EP	3077254	B1	2019年 9月 25日
				US	2017158169	A1	2017年 6月 8日
				KR	20160096127	A	2016年 8月 12日
				JP	2017501321	A	2017年 1月 12日
				US	9963109	B2	2018年 5月 8日
				JP	6609557	B2	2019年 11月 20日
				EP	3077254	A1	2016年 10月 12日
				KR	101771376	B1	2017年 8月 24日
				CN	105899413	B	2018年 4月 10日
				WO	2015084852	A1	2015年 6月 11日
CN	108632745	A	2018年 10月 9日	US	2018265040	A1	2018年 9月 20日
				EP	3376475	A1	2018年 9月 19日
CN	109318856	A	2019年 2月 12日	US	10207677	B1	2019年 2月 19日
				US	2019031141	A1	2019年 1月 31日
				DE	102018118424	A1	2019年 1月 31日
US	2015135268	A1	2015年 5月 14日	无			
US	2017190420	A1	2017年 7月 6日	KR	20170079673	A	2017年 7月 10日
				US	10173772	B2	2019年 1月 8日