(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 109286595 A
(43)申请公布日 2019.01.29

(21)申请号 201710592851.3

(22)申请日 2017.07.19

(71)申请人 比亚迪股份有限公司
地址 518118 广东省深圳市坪山新区比亚迪路3009号

(72)发明人 王坤

(74)专利代理机构 北京清亦华知识产权代理事务所(普通合伙) 11201
代理人 张润

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/40(2006.01)

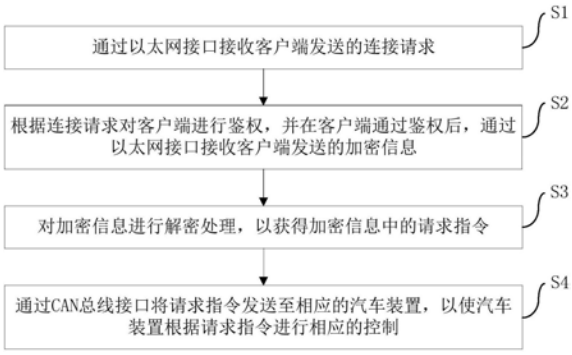
权利要求书2页 说明书11页 附图4页

(54)发明名称

汽车及其控制方法和控制装置及计算机设备

(57)摘要

本发明公开了一种汽车及其控制方法和控制装置及计算机设备，所述控制方法包括以下步骤：通过以太网接口接收客户端发送的连接请求；根据连接请求对客户端进行鉴权，并在客户端通过鉴权后，通过以太网接口接收客户端发送的加密信息；对加密信息进行解密处理，以获得加密信息中的请求指令；以及通过CAN总线接口将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制。本发明实施例的控制方法，能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。



CN 109286595 A

1.一种汽车的控制方法,其特征在于,包括以下步骤:

通过以太网接口接收客户端发送的连接请求;

根据所述连接请求对所述客户端进行鉴权,并在所述客户端通过鉴权后,通过所述以太网接口接收所述客户端发送的加密信息;

对所述加密信息进行解密处理,以获得所述加密信息中的请求指令;以及

通过CAN总线接口将所述请求指令发送至相应的汽车装置,以使所述汽车装置根据所述请求指令进行相应的控制。

2.如权利要求1所述的汽车的控制方法,其特征在于,所述客户端包括手机、平板电脑或台式电脑。

3.如权利要求1所述的汽车的控制方法,其特征在于,在获得所述加密信息中的请求指令之后,还包括:

验证所述请求指令是否在所述客户端行使的权利范围内;

如果是,则通过所述CAN总线接口将所述请求指令发送至相应的汽车装置;

如果否,则断开与所述客户端之间的通信连接,同时生成相应的提醒信息,并将所述提醒信息提供给用户。

4.如权利要求1所述的汽车的控制方法,其特征在于,还包括:

通过所述CAN总线接口接收所述汽车装置发送的反馈信息;

对所述反馈信息进行加密处理;以及

将加密处理后的反馈信息通过所述以太网接口发送至所述客户端。

5.如权利要求1或3所述的汽车的控制方法,其特征在于,所述请求指令包括汽车控制指令、数据查看指令和汽车设置指令中的至少一个。

6.一种计算机设备,其特征在于,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,所述处理器执行所述程序时,实现如权利要求1-5中任一所述的汽车的控制方法。

7.一种汽车的控制装置,其特征在于,包括第一接收模块、鉴权模块、解密模块、第一发送模块、以太网接口和CAN总线接口,其中,

所述第一接收模块用于,通过所述以太网接口接收客户端发送的连接请求;

所述鉴权模块用于,根据所述连接请求对所述客户端进行鉴权,并在所述客户端通过鉴权后,通过所述以太网接口接收所述客户端发送的加密信息;

所述解密模块用于,对所述加密信息进行解密处理,以获得所述加密信息中的请求指令;

所述第一发送模块用于,通过所述CAN总线接口将所述请求指令发送至相应的汽车装置,以使所述汽车装置根据所述请求指令进行相应的控制。

8.如权利要求7所述的汽车的控制装置,其特征在于,所述客户端包括手机、平板电脑或台式电脑。

9.如权利要求7所述的汽车的控制装置,其特征在于,所述第一发送模块,还用于:

在获得所述加密信息中的请求指令之后,验证所述请求指令是否在所述客户端行使的权利范围内;

如果是,则通过所述CAN总线接口将所述请求指令发送至相应的汽车装置;

如果否，则断开与所述客户端之间的通信连接，同时生成相应的提醒信息，并将所述提醒信息提供给用户。

10.如权利要求7所述的汽车的控制装置，其特征在于，还包括：

第二接收模块，所述第二接收模块用于通过所述CAN总线接口接收所述汽车装置发送的反馈信息；

加密模块，所述加密模块用于对所述反馈信息进行加密处理；以及

第二发送模块，所述第二发送模块用于将加密处理后的反馈信息通过所述以太网接口发送至所述客户端。

11.如权利要求7或9所述的汽车的控制装置，其特征在于，所述请求指令包括汽车控制指令、数据查看指令和汽车设置指令中的至少一个。

12.一种汽车，其特征在于，包括如权利要求7-11中任一项所述的汽车的控制装置。

汽车及其控制方法和控制装置及计算机设备

技术领域

[0001] 本发明涉及汽车技术领域，特别涉及一种汽车的控制方法、一种计算机设备、一种汽车的控制装置和一种具有该控制装置的汽车。

背景技术

[0002] 随着汽车行业的发展，汽车上安装的电子设备和传感器越来越多，越来越复杂。其中很多关键的传感器都是通过CAN(Controller Area Network，控制器局域网络)总线来进行数据传输。

[0003] 互联网技术与汽车的融合明显，互联网汽车是汽车技术的一个重要发展方向。汽车联网后用户能够远程控制汽车，使用地图导航和互联网软件，汽车厂商能实时采集汽车运行状态，汽车软件OTA(Over The Air，空中推送升级)。互联网汽车提供了很方便的使用方式，同时也引入了互联网相关的安全问题。尤其是CAN总线只能明文数据传输的情况下，互联网汽车的安全问题尤其突出。

发明内容

[0004] 本发明旨在至少在一定程度上解决上述技术中的技术问题之一。

[0005] 为此，本发明的第一个目的在于提出一种汽车的控制方法，能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0006] 本发明的第二个目的在于提出一种计算机设备。

[0007] 本发明的第三个目的在于提出一种汽车的控制装置。

[0008] 本发明的第三个目的在于提出一种汽车。

[0009] 为达到上述目的，本发明第一方面实施例提出了一种汽车的控制方法，包括以下步骤：通过以太网接口接收客户端发送的连接请求；根据所述连接请求对所述客户端进行鉴权，并在所述客户端通过鉴权后，通过所述以太网接口接收所述客户端发送的加密信息；对所述加密信息进行解密处理，以获得所述加密信息中的请求指令；以及通过CAN总线接口将所述请求指令发送至相应的汽车装置，以使所述汽车装置根据所述请求指令进行相应的控制。

[0010] 根据本发明实施例的汽车的控制方法，首先通过以太网接口接收客户端发送的连接请求，然后根据连接请求对客户端进行鉴权，并在客户端通过鉴权后，通过以太网接口接收客户端发送的加密信息，再然后对加密信息进行解密处理，以获得加密信息中的请求指令，最后通过CAN总线接口将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制。由此，该控制方法能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0011] 另外，根据本发明上述实施例提出的汽车的控制方法还可以具有如下附加的技术特征：

[0012] 在本发明的一个实施例中，所述客户端包括手机、平板电脑或台式电脑。

[0013] 在本发明的一个实施例中，在获得所述加密信息中的请求指令之后，还包括：验证所述请求指令是否在所述客户端行使的权利范围内；如果是，则通过所述CAN总线接口将所述请求指令发送至相应的汽车装置；如果否，则断开与所述客户端之间的通信连接，同时生成相应的提醒信息，并将所述提醒信息提供给用户。

[0014] 在本发明的一个实施例中，上述汽车的控制方法还包括：通过所述CAN总线接口接收所述汽车装置发送的反馈信息；对所述反馈信息进行加密处理；以及将加密处理后的反馈信息通过所述以太网接口发送至所述客户端。

[0015] 在本发明的一个实施例中，所述请求指令包括汽车控制指令、数据查看指令和汽车设置指令中的至少一个。

[0016] 为达到上述目的，本发明第二方面实施例提出了一种计算机设备，包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序，其特征在于，所述处理器执行所述程序时，实现上述的汽车的控制方法。

[0017] 本发明实施例的计算机设备，首先通过以太网接口接收客户端发送的连接请求，然后根据连接请求对客户端进行鉴权，并在客户端通过鉴权后，通过以太网接口接收客户端发送的加密信息，再然后对加密信息进行解密处理，以获得加密信息中的请求指令，最后通过CAN总线接口将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制。由此，该计算机设备能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0018] 为达到上述目的，本发明第三方面实施例提出了一种汽车的控制装置，包括第一接收模块、鉴权模块、解密模块、第一发送模块、以太网接口和CAN总线接口，其中，所述第一接收模块用于，通过以太网接口接收客户端发送的连接请求；所述鉴权模块用于，根据所述连接请求对所述客户端进行鉴权，并在所述客户端通过鉴权后，通过所述以太网接口接收所述客户端发送的加密信息；所述解密模块用于，对所述加密信息进行解密处理，以获得所述加密信息中的请求指令；所述第一发送模块用于，通过CAN总线接口将所述请求指令发送至相应的汽车装置，以使所述汽车装置根据所述请求指令进行相应的控制。

[0019] 根据本发明实施例的汽车的控制装置，第一接收模块通过以太网接口接收客户端发送的连接请求，鉴权模块根据连接请求对客户端进行鉴权，并在客户端通过鉴权后，通过以太网接口接收客户端发送的加密信息，而后解密模块对加密信息进行解密处理，以获得加密信息中的请求指令，第一发送模块通过CAN总线接口将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制。由此，该控制装置能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0020] 另外，根据本发明上述实施例提出的汽车的控制装置还可以具有如下附加的技术特征：

[0021] 在本发明的一个实施例中，所述客户端包括手机、平板电脑或台式电脑。

[0022] 在本发明的一个实施例中，所述第一发送模块，还用于：在获得所述加密信息中的请求指令之后，验证所述请求指令是否在所述客户端行使的权利范围内；如果是，则通过所述CAN总线接口将所述请求指令发送至相应的汽车装置；如果否，则断开与所述客户端之间的通信连接，同时生成相应的提醒信息，并将所述提醒信息提供给用户。

[0023] 在本发明的一个实施例中，上述汽车的控制装置还包括：第二接收模块，所述第二

接收模块用于通过所述CAN总线接口接收所述汽车装置发送的反馈信息;加密模块,所述加密模块用于对所述反馈信息进行加密处理;以及第二发送模块,所述第二发送模块用于将加密处理后的反馈信息通过所述以太网接口发送至所述客户端。

[0024] 在本发明的一个实施例中,所述请求指令包括汽车控制指令、数据查看指令和汽车设置指令中的至少一个。

[0025] 为了实现上述目的,本发明第四方面实施例提出的一种汽车包括:本发明第二方面实施例的汽车的控制装置。

[0026] 本发明实施例的汽车,通过上述汽车的控制装置,能够通过对客户端的鉴权,来检查客户端是否合法,是否有相应的访问权限等,从而提升了汽车的网络安全性。

[0027] 本发明附加的方面的优点将在下面的描述中部分给出,部分将从下面的描述中变得明显,或通过本发明的实践了解到。

附图说明

[0028] 图1是根据本发明一个实施例的汽车的控制方法的流程图。

[0029] 图2是根据本发明另一个实施例的汽车的控制方法的流程图。

[0030] 图3是根据本发明实施例的CAN总线访问服务的流程图。

[0031] 图4是根据本发明实施例的以太网访问服务的流程图。

[0032] 图5是根据本发明一个实施例的汽车的控制装置的方框示意图。

[0033] 图6是根据本发明实施例的汽车的控制装置的硬件结构示意图。

[0034] 图7是根据本发明另一个实施例的汽车的控制装置的方框示意图。

具体实施方式

[0035] 下面详细描述本发明的实施例,所述实施例的示例在附图中示出,其中自始至终相同或类似的标号表示相同或类似的元件或具有相同或类似功能的元件。下面通过参考附图描述的实施例是示例性的,旨在用于解释本发明,而不能理解为对本发明的限制。

[0036] 下面结合附图来描述本发明实施例的汽车及其控制方法和控制装置及计算机设备。

[0037] 图1是根据本发明一个实施例的汽车的控制方法的流程图。在本发明的实施例中,汽车可包括纯电动汽车、混合动力汽车和燃油汽车等。

[0038] 如图1所示,本发明实施例的汽车的控制方法包括以下步骤:

[0039] S1,通过以太网接口接收客户端发送的连接请求。应说明的是,以太网接口具有高速大带宽的数据传输优势,通过此功能可以大量传输数据到汽车的操作系统(例如,CPU(Central Processing Unit,中央处理器)的嵌入式操作系统,其中,嵌入式操作系统可为Linux操作系统,且该操作系统可实现以太网接口驱动和CAN总线接口驱动,该操作系统具有以太网服务和CAN总线服务)上以进行上网等数据传输工作。其中,该以太网接口可连接到车内局域网关上,与汽车上其他具有以太网接口的模块(例如,无线通信模块)连接在一起,构建车内局域网,该车内局域网中的各个模块可通过以太网进行通信。

[0040] 其中,如图6所示,CPU与RAM(random access memory,随机存取存储器)及其外围电路构成一个上述的汽车的操作系统的基础硬件,固态存储器FLASH可挂接在CPU总线上,

保存有启动分区和该汽车的操作系统,剩余的划分为配置分区,用来保存配置数据。其中,上述CAN总线接口可接在CPU总线上,是在该汽车的操作系统中进行CAN总线数据读写的硬件外设,上述以太网接口也可接在CPU总线上,是该汽车的操作系统进行网络操作的硬件外设。

[0041] 在本发明的一个实施例中,客户端可包括手机、平板电脑或台式电脑。其中,平板电脑可为设置在后座的车载pad(平板电脑)。

[0042] 例如,冬季较为寒冷,为保障汽车的性能以及减少对汽车的损耗,可先将汽车启动一段时间后再进行驾驶。为了减少热车的等待时间,用户可以在步行去车库取车的过程中,通过手机上的汽车APP(Application,应用程序),发送连接请求至汽车的远程服务器,然后汽车的远程服务器将该连接请求发送至该用户的汽车上。再然后该汽车的操作系统(例如,Linux操作系统)通过以太网接口接收该连接请求。其中,连接请求可包括汽车的唯一编码,以便于汽车的远程服务器根据该唯一编码查找到相应的汽车。

[0043] 需要说明的是,上述汽车的远程服务器可将该连接请求发送至上述汽车的无线通信装置上,而后该无线通信装置将该连接请求转发至车内局域网关,最后,该车内局域网关可对该连接请求进行协议转换以将其转换为符合上述汽车的操作系统的通信协议,并将转换后的连接请求通过以太网线传输至上述的以太网接口。其中,无线通信装置可包括WIFI(Wireless Fidelity,无线局域网)模块和GSM(Global System for Mobile communication,全球移动通信系统)模块。

[0044] 在本发明的其他实施例中,用户还可通过手机上的汽车APP利用汽车的内部局域网将连接请求直接发送到该汽车上,无需通过汽车的远程服务器进行转发。其中,汽车的内部局域网可为上述无线通信装置的广播网络,应说明的是,该实施例中所描述的广播网络具有一定的局限性,无法大面积的广播,其广播的范围可为以汽车为圆心半径为8M、15M或20M形成的圆的范围内。用户可根据实际情况选择发送链接请求的方式,此处不做限定。

[0045] S2,根据连接请求对客户端进行鉴权,并在客户端通过鉴权后,通过以太网接口接收客户端发送的加密信息。

[0046] 具体地,上述汽车的操作系统在接收到客户端发出的连接请求后,可根据该连接请求对客户端进行鉴权,以检查客户端是否合法,是否有汽车状态查询配置权限和远程控制权限等,例如,可通过利用认证授权来验证客户端中的数字签名的正确与否对该客户端进行鉴权。如果该客户端通过鉴权,则该汽车的操作系统可接受该客户端的连接请求,并根据此连接请求建立与该客户端之间的通信连接。而后通过以太网接口接收该客户端通过该通信连接发送的加密信息。

[0047] S3,对加密信息进行解密处理,以获得加密信息中的请求指令。其中,请求指令可包括汽车控制指令、数据查看指令和汽车设置指令中的至少一个。

[0048] 在本发明的实施例中,汽车控制指令可包括汽车启动指令、车门开启/关闭指令、车窗控制指令和车内多媒体控制指令等。数据查看指令可包括汽车状态查询指令、汽车配置查询指令等。汽车设置指令可包括车载空调参数设置指令、汽车相关的配置参数设置指令等。

[0049] S4,通过CAN总线接口将请求指令发送至相应的汽车装置,以使汽车装置根据请求指令进行相应的控制。其中,CAN总线接口可与汽车上的CAN总线连接,与汽车上其他具有

CAN总线接口的模块(例如,发动机启动模块、车窗控制装置和整车控制器等)连接在一起,且CAN总线数据是明文收发。

[0050] 在本发明的实施例中,汽车装置可包括车窗控制装置、汽车启动装置和车载多媒体设置装置等,应说明的是,上述的汽车装置不局限于这些,还可包括各种传感器模块、空调等,此处不做限定。

[0051] 具体地,上述汽车的操作系统在接收到客户端发出的加密信息后,可根据预设的解密算法对该加密信息进行解密处理,以从中获取该客户端发出的请求指令。然后,该汽车的操作系统根据该请求指令确定相应的汽车装置,例如,如果请求指令为汽车启动指令,则汽车装置可为发动机启动模块;如果请求指令为车窗控制指令,则汽车装置可为车窗控制装置;如果请求指令为车辆状态信息查询指令,则汽车装置可为汽车的整车控制器。

[0052] 上述汽车的操作系统在根据该请求指令确定相应的汽车装置后,可通过CAN总线接口将请求指令发送至相应的汽车装置,以使汽车装置根据请求指令进行相应的控制。例如,当请求指令为汽车启动指令时,通过CAN总线接口将该汽车启动指令发送至发动机启动模块,已使该发动机启动模块根据该汽车启动指令启动汽车。应说明的是,该实施例中所描述的预设的解密算法可根据实际情况进行标定。

[0053] 为了使操作客户端的用户能及时知晓发送的请求指令的执行状态,在本发明的一个实施例中,上述汽车的控制方法还可包括通过CAN总线接口接收汽车装置发送的反馈信息,并对反馈信息进行加密处理,以及将加密处理后的反馈信息通过以太网接口发送至客户端。

[0054] 具体的,当汽车装置根据请求指令完成相应的控制时,可生产相应的反馈信息,并将其通过CAN总线接口以明文的形式发送至上述汽车的操作系统。然后,根据预设的加密算法对该反馈信息进行加密,并通过以太网接口将加密后的反馈信息发送至客户端,以使正在使用客户端的用户能够及时知晓发送的请求指令的知晓状态,有利于提升客户端的用户体验。其中,预设的加密算法可根据实际情况进行标定。

[0055] 综上所述,本发明实施例提供的汽车的控制方法,能够通过对客户端的鉴权,来检查客户端是否合法,是否有相应的访问权限等,从而提升了汽车的网络安全性。

[0056] 为了进一步提升汽车的网络安全性,在本发明的一个实施例中,如图2所示,在获得加密信息中的请求指令之后,还可包括以下步骤:

[0057] S101,验证请求指令是否在客户端行使的权利范围内。

[0058] 具体的,上述汽车的操作系统在获得加密信息中的请求指令之后,根据该请求指令确定与该请求指令对应的命令类型及相应的权限级别,例如,如果该请求指令为发动机启动指令,则该请求指令为控制类命令,级别为A级;如果该请求指令为汽车状态查询指令,则该请求指令为查询类命令,级别为B级。然后,汽车的操作系统将依据该请求指令的命令类型及相应的权限级别,对发送该请求指令的客户端进行权限的验证,即,对比对该客户端鉴权时的信息,其中包括客户端行使的权利范围。

[0059] S102,如果是,则通过CAN总线接口将请求指令发送至相应的汽车装置。

[0060] 具体的,上述汽车的操作系统在验证请求指令是在客户端行使的权利范围内之后,才通过CAN总线接口将请求指令发送至相应的汽车装置,从而进一步提升汽车的网络安全性。

[0061] S103,如果否,则断开与客户端之间的通信连接,同时生成相应的提醒信息,并将提醒信息提供给用户。

[0062] 具体的,上述汽车的操作系统在验证请求指令不是在客户端行使的权利范围内之后,为了保证汽车的网络安全将会主动断开与客户端之间的通信连接,同时生成相应的提醒信息,并将该提醒信息提供给用户。

[0063] 例如,如果该请求指令为控制汽车开门指令,而经过验证发现发送该指令的客户端并不具有开启汽车车门的权利,上述汽车的操作系统可认为该客户端可能被非法分子利用,为了保证汽车的安全性,可先主动断开与该客户端之间的通信连接,然后生成该客户端正在发送自身权利范围之外的请求指令的提醒信息,并将其发送至驾驶员的移动终端中,或者将其发送至该汽车的报警服务器中,以最大程度的保证汽车的安全。

[0064] 为使本领域技术人员更清楚地了解本发明,且更清楚本发明中CAN总线服务,图3是根据本发明实施例的CAN总线访问服务的流程图。如图3所示,该CAN访问服务可包括以下步骤:

[0065] S01,汽车的操作系统开机启动。

[0066] S02,侦听CAN驱动上报的事件(即,通过CAN总线接口上传至汽车的操作系统的事件),判断是否有新数据上报,若没有则继续执行本步骤;若有新报文,则执行步骤S03。

[0067] S03,查找与互联网访问服务(即,以太网服务)共享的CAN报文监控表,对比新报文是否是需要监控的报文,若不是则执行步骤S02,若是则执行步骤S04。

[0068] S04,对比新报文与上一次报文是否有变化,若没有变化则执行步骤S02,若有变化则执行步骤S05。

[0069] S05,更新该报文对应的汽车运行状态,继续执行步骤S06。

[0070] S06,调用互联网访问服务的API(Application Programming Interface,应用程序编程接口)密文推送新的汽车运行状态信息给客户端(即,通过以太网接口发送给客户端),跳转执行步骤S02。

[0071] 为使本领域技术人员更清楚地了解本发明,且更清楚本发明中以太网访问服务,图4是根据本发明实施例的以太网访问服务的流程图。如图4所示,该以太网服务可包括以下步骤:

[0072] S001,汽车的操作系统开机启动。

[0073] S002,等待新的客户端连接请求,若没有则继续执行本步骤;若有则执行步骤S003。

[0074] S003,判断是否为合法的客户端请求;若不是则执行步骤S002;若是则执行步骤S004。

[0075] S004,解密客户端发送的加密信息以获得该加密信息中的请求指令。

[0076] S005,若该指令是读取汽车状态接口,则转至步骤S006;若该指令是设置汽车状态则转至步骤S008;若该指令是监控配置接口则转至步骤S010;否则转至步骤S004。

[0077] S006,读取CAN访问服务的汽车状态表;转至步骤S007。

[0078] S007,将执行结果密文发送至客户端;转至步骤S012。

[0079] S008,调用CAN访问服务的API控制汽车状态,执行步骤S009。

[0080] S009,读取CAN访问服务的API的执行结果;转至步骤S07。

[0081] S010,设置与CAN问服务共享的监控报文表,执行步骤S11。

[0082] S011,读取CAN访问服务的监控报文表配置结果;转至步骤S07。

[0083] S012,判断客户端是否已经退出,若是则转至步骤S013;否则转至步骤S004;步骤S013。

[0084] S013,执行客户端退出操作。

[0085] 综上,根据本发明实施例的汽车的控制方法,首先通过以太网接口接收客户端发送的连接请求,然后根据连接请求对客户端进行鉴权,并在客户端通过鉴权后,通过以太网接口接收客户端发送的加密信息,再然后对加密信息进行解密处理,以获得加密信息中的请求指令,最后通过CAN总线接口将请求指令发送至相应的汽车装置,以使汽车装置根据请求指令进行相应的控制。由此,该控制方法能够通过对客户端的鉴权,来检查客户端是否合法,是否有相应的访问权限等,从而提升了汽车的网络安全性。

[0086] 另外,本发明的实施例还提出了一种计算机设备,包括存储器、处理器及存储在存储器上并可在处理器上运行的计算机程序,其特征在于,处理器执行程序时,实现上述的汽车的控制方法。

[0087] 本发明实施例的计算机设备,首先通过以太网接口接收客户端发送的连接请求,然后根据连接请求对客户端进行鉴权,并在客户端通过鉴权后,通过以太网接口接收客户端发送的加密信息,再然后对加密信息进行解密处理,以获得加密信息中的请求指令,最后通过CAN总线接口将请求指令发送至相应的汽车装置,以使汽车装置根据请求指令进行相应的控制。由此,该计算机设备能够通过对客户端的鉴权,来检查客户端是否合法,是否有相应的访问权限等,从而提升了汽车的网络安全性。

[0088] 图5是根据本发明一个实施例的汽车的控制装置的方框示意图。在本发明的实施例中,汽车可包括纯电动汽车、混合动力汽车和燃油汽车等。

[0089] 如图5所示,本发明实施例的汽车的控制装置包括:第一接收模块100、鉴权模块200、解密模块300、第一发送模块400、以太网接口500和CAN总线接口600。

[0090] 其中,第一接收模块100用于通过以太网接口500接收客户端发送的连接请求。应说明的是,以太网接口500具有高速大带宽的数据传输优势,通过此功能可以大量传输数据到汽车的操作系统(例如,CPU的嵌入式操作系统,其中,嵌入式操作系统可为Linux操作系统,且该操作系统可实现以太网接口驱动和CAN总线接口驱动,该操作系统具有以太网服务和CAN总线服务)上以进行上网等数据传输工作。其中,该以太网接口可连接到车内局域网关上,与汽车上其他具有以太网接口的模块(例如,无线通信模块)连接在一起,构建车内局域网,该车内局域网中的各个模块可通过以太网进行通信。其中,上述的汽车的操作系统可包括第一接收模块100、鉴权模块200、解密模块300、第一发送模块400。

[0091] 其中,如图6所示,CPU10与RAM(random access memory,随机存取存储器)20及其外围电路构成一个上述的汽车的操作系统的基础硬件,固态存储器FLASH30可挂接在CPU10总线上,保存有启动分区和该汽车的操作系统,剩余的划分为配置分区,用来保存配置数据。其中,CAN总线接口600可接在CPU10总线上,是在该汽车的操作系统中进行CAN总线数据读写的硬件外设,以太网接口500也可接在CPU10总线上,是该汽车的操作系统进行网络操作的硬件外设。

[0092] 在本发明的一个实施例中,客户端可包括手机、平板电脑或台式电脑。其中,平板

电脑可为设置在后座的车载pad(平板电脑)。

[0093] 例如,冬季较为寒冷,为保障汽车的性能以及减少对汽车的损耗,可先将汽车启动一段时间后再进行驾驶。为了减少热车的等待时间,用户可以在步行去车库取车的过程中,通过手机上的汽车APP(Application,应用程序),发送连接请求至汽车的远程服务器,然后汽车的远程服务器将该连接请求发送至该用户的汽车上。再然后该汽车的操作系统(例如,Linux操作系统)的第一接收模块100通过以太网接口500接收该连接请求。其中,连接请求可包括汽车的唯一编码,以便于汽车的远程服务器根据该唯一编码查找到相应的汽车。

[0094] 需要说明的是,上述汽车的远程服务器可将该连接请求发送至上述汽车的无线通信装置上,而后该无线通信装置将该连接请求转发至车内局域网关,最后,该车内局域网关可对该连接请求进行协议转换以将其转换为符合上述汽车的操作系统的通信协议,并将转换后的连接请求通过以太网线传输至上述的以太网接口500。其中,无线通信装置可包括WIFI(Wireless Fidelity,无线局域网)模块和GSM(Global System for Mobile communication,全球移动通信系统)模块。

[0095] 在本发明的其他实施例中,用户还可通过手机上的汽车APP利用汽车的内部局域网将连接请求直接发送到该汽车上,无需通过汽车的远程服务器进行转发。其中,汽车的内部局域网可为上述无线通信装置的广播网络,应说明的是,该实施例中所描述的广播网络具有一定的局限性,无法大面积的广播,其广播的范围可为以汽车为圆心半径为8M、15M或20M形成的圆的范围内。用户可根据实际情况选择发送链接请求的方式,此处不做限定。

[0096] 鉴权模块200用于根据连接请求对客户端进行鉴权,并在客户端通过鉴权后,通过以太网接口500接收客户端发送的加密信息。

[0097] 具体地,上述汽车的操作系统的鉴权模块200在接收到客户端发出的连接请求后,可根据该连接请求对客户端进行鉴权,以检查客户端是否合法,是否有汽车状态查询配置权限和远程控制权限等,例如,可通过利用认证授权来验证客户端中的数字签名的正确与否对该客户端进行鉴权。如果该客户端通过鉴权,则鉴权模块200可接受该客户端的连接请求,并根据此连接请求建立与该客户端之间的通信连接。而后通过以太网接口500接收该客户端通过该通信连接发送的加密信息。

[0098] 解密模块300用于对加密信息进行解密处理,以获得加密信息中的请求指令。其中,请求指令可包括汽车控制指令、数据查看指令和汽车设置指令中的至少一个。

[0099] 在本发明的实施例中,汽车控制指令可包括汽车启动指令、车门开启/关闭指令、车窗控制指令和车内多媒体控制指令等。数据查看指令可包括汽车状态查询指令、汽车配置查询指令等。汽车设置指令可包括车载空调参数设置指令、汽车相关的配置参数设置指令等。

[0100] 第一发送模块400用于通过CAN总线接口600将请求指令发送至相应的汽车装置,以使汽车装置根据请求指令进行相应的控制。其中,CAN总线接口600可与汽车上的CAN总线连接,与汽车上其他具有CAN总线接口的模块(例如,发动机启动模块、车窗控制装置和整车控制器等)连接在一起,且CAN总线数据是明文收发。

[0101] 在本发明的实施例中,汽车装置可包括车窗控制装置、汽车启动装置和车载多媒体设置装置等,应说明的是,上述的汽车装置不局限于这些,还可包括各种传感器模块、空调等,此处不做限定。

[0102] 具体地，上述汽车的操作系统的解密模块300在接收到鉴权模块200转发的加密信息后，可根据预设的解密算法对该加密信息进行解密处理，以从中获取该客户端发出的请求指令。然后，该汽车的操作系统的第一发送模块400根据该请求指令确定相应的汽车装置，例如，如果请求指令为汽车启动指令，则汽车装置可为发动机启动模块；如果请求指令为车窗控制指令，则汽车装置可为车窗控制装置；如果请求指令为车辆状态信息查询指令，则汽车装置可为汽车的整车控制器。

[0103] 上述汽车的操作系统的第一发送模块400在根据该请求指令确定相应的汽车装置后，可通过CAN总线接口600将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制。例如，当请求指令为汽车启动指令时，通过CAN总线接口600将该汽车启动指令发送至发动机启动模块，已使该发动机启动模块根据该汽车启动指令启动汽车。应说明的是，该实施例中所描述的预设的解密算法可根据实际情况进行标定。

[0104] 为了使操作客户端的用户能及时知晓发送的请求指令的执行状态，在本发明的一个实施例中，如图7所示，上述汽车的控制装置还可包括：第二接收模块700、加密模块800和第二发送模块900。其中，上述汽车的操作系统还可包括第二接收模块700、加密模块800和第二发送模块900。

[0105] 其中，第二接收模块700用于通过CAN总线接口600接收汽车装置发送的反馈信息。

[0106] 加密模块800用于对反馈信息进行加密处理。

[0107] 第二发送模块900用于将加密处理后的反馈信息通过以太网接口500发送至客户端。

[0108] 具体的，当汽车装置根据请求指令完成相应的控制时，可生产相应的反馈信息，并将其通过CAN总线接口600以明文的形式发送至上述汽车的操作系统的第二接收模块700。然后，第二接收模块700将该反馈信息转发至加密模块800，而后加密模块800根据预设的加密算法对该反馈信息进行加密，最后第二发送模块900并通过以太网接口500将加密后的反馈信息发送至客户端，以使正在使用客户端的用户能够及时知晓发送的请求指令的知晓状态，有利于提升客户端的用户体验。其中，预设的加密算法可根据实际情况进行标定。

[0109] 综上所述，本发明实施例提供的汽车的控制装置，能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0110] 为了进一步提升汽车的网络安全性，在本发明的一个实施例中，第一发送模块100还可用于在获得加密信息中的请求指令之后，验证请求指令是否在客户端行使的权利范围内，如果是，则通过CAN总线接口将请求指令发送至相应的汽车装置，如果否，则断开与客户端之间的通信连接，同时生成相应的提醒信息，并将提醒信息提供给用户。

[0111] 具体的，上述汽车的操作系统的第一发送模块100在获得加密信息中的请求指令之后，根据该请求指令确定与该请求指令对应的命令类型及相应的权限级别，例如，如果该请求指令为发动机启动指令，则该请求指令为控制类命令，级别为A级；如果该请求指令为汽车状态查询指令，则该请求指令为查询类命令，级别为B级。然后，第一发送模块100将依据该请求指令的命令类型及相应的权限级别，对发送该请求指令的客户端进行权限的验证，即，对比对该客户端鉴权时的信息，其中包括客户端行使的权利范围。

[0112] 第一发送模块100在验证请求指令是在客户端行使的权利范围内之后，才通过CAN总线接口600将请求指令发送至相应的汽车装置，从而进一步提升汽车的网络安全性。

[0113] 第一发送模块100在验证请求指令不是在客户端行使的权利范围内之后，为了保证汽车的网络安全将会主动断开与客户端之间的通信连接，同时生成相应的提醒信息，并将该提醒信息提供给用户。

[0114] 例如，如果该请求指令为控制汽车开门指令，而经过验证发现发送该指令的客户端并不具有开启汽车车门的权利，第一发送模块100可认为该客户端可能被非法分子利用，为了保证汽车的安全性，可先主动断开与该客户端之间的通信连接，然后生成该客户端正在发送自身权利范围之外的请求指令的提醒信息，并将其发送至驾驶员的移动终端中，或者将其发送至该汽车的报警服务器中，以最大程度的保证汽车的安全。

[0115] 需要说明的是，前述对汽车的控制方法实施例的解释说明也适用于该实施例的汽车的控制装置，此处不再赘述。

[0116] 综上，根据本发明实施例的汽车的控制装置，第一接收模块通过以太网接口接收客户端发送的连接请求，鉴权模块根据连接请求对客户端进行鉴权，并在客户端通过鉴权后，通过以太网接口接收客户端发送的加密信息，而后解密模块对加密信息进行解密处理，以获得加密信息中的请求指令，第一发送模块通过CAN总线接口将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制。由此，该控制装置能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0117] 为了实现上述实施例，本发明还提出一种汽车，其包括上述汽车的控制装置。

[0118] 本发明实施例的汽车，通过上述汽车的控制装置，能够通过对客户端的鉴权，来检查客户端是否合法，是否有相应的访问权限等，从而提升了汽车的网络安全性。

[0119] 在本发明的描述中，需要理解的是，术语“中心”、“纵向”、“横向”、“长度”、“宽度”、“厚度”、“上”、“下”、“前”、“后”、“左”、“右”、“竖直”、“水平”、“顶”、“底”、“内”、“外”、“顺时针”、“逆时针”、“轴向”、“径向”、“周向”等指示的方位或位置关系为基于附图所示的方位或位置关系，仅是为了便于描述本发明和简化描述，而不是指示或暗示所指的装置或元件必须具有特定的方位、以特定的方位构造和操作，因此不能理解为对本发明的限制。

[0120] 此外，术语“第一”、“第二”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”的特征可以明示或者隐含地包括一个或者更多个该特征。在本发明的描述中，“多个”的含义是两个或两个以上，除非另有明确具体的限定。

[0121] 在本发明中，除非另有明确的规定和限定，术语“安装”、“相连”、“连接”、“固定”等术语应做广义理解，例如，可以是固定连接，也可以是可拆卸连接，或成一体；可以是机械连接，也可以是电连接；可以是直接相连，也可以通过中间媒介间接相连，可以是两个元件内部的连通或两个元件的相互作用关系。对于本领域的普通技术人员而言，可以根据具体情况理解上述术语在本发明中的具体含义。

[0122] 在本发明中，除非另有明确的规定和限定，第一特征在第二特征“上”或“下”可以是第一和第二特征直接接触，或第一和第二特征通过中间媒介间接接触。而且，第一特征在第二特征“之上”、“上方”和“上面”可是第一特征在第二特征正上方或斜上方，或仅仅表示第一特征水平高度高于第二特征。第一特征在第二特征“之下”、“下方”和“下面”可以是第一特征在第二特征正下方或斜下方，或仅仅表示第一特征水平高度小于第二特征。

[0123] 在本说明书的描述中，参考术语“一个实施例”、“一些实施例”、“示例”、“具体示例”、或“一些示例”等的描述意指结合该实施例或示例描述的具体特征、结构、材料或者特点包含于本发明的至少一个实施例或示例中。在本说明书中，对上述术语的示意性表述不必须针对的是相同的实施例或示例。而且，描述的具体特征、结构、材料或者特点可以在任一个或多个实施例或示例中以合适的方式结合。此外，在不相互矛盾的情况下，本领域的技术人员可以将本说明书中描述的不同实施例或示例以及不同实施例或示例的特征进行结合和组合。

[0124] 尽管上面已经示出和描述了本发明的实施例，可以理解的是，上述实施例是示例性的，不能理解为对本发明的限制，本领域的普通技术人员在本发明的范围内可以对上述实施例进行变化、修改、替换和变型。

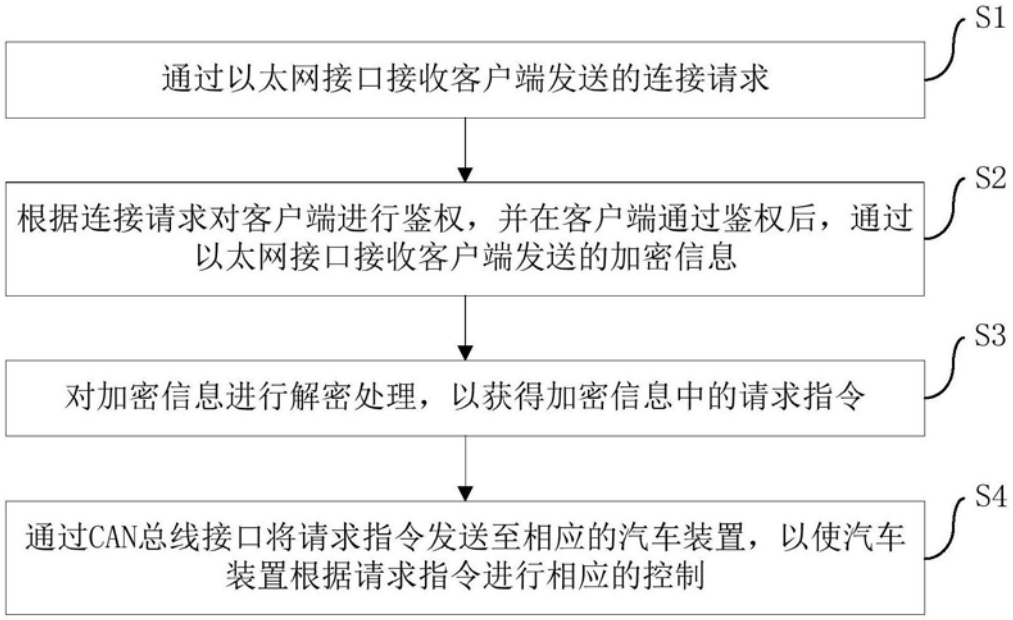

S1
通过以太网接口接收客户端发送的连接请求
S2
根据连接请求对客户端进行鉴权，并在客户端通过鉴权后，通过以太网接口接收客户端发送的加密信息
S3
对加密信息进行解密处理，以获得加密信息中的请求指令
S4
通过CAN总线接口将请求指令发送至相应的汽车装置，以使汽车装置根据请求指令进行相应的控制

图1

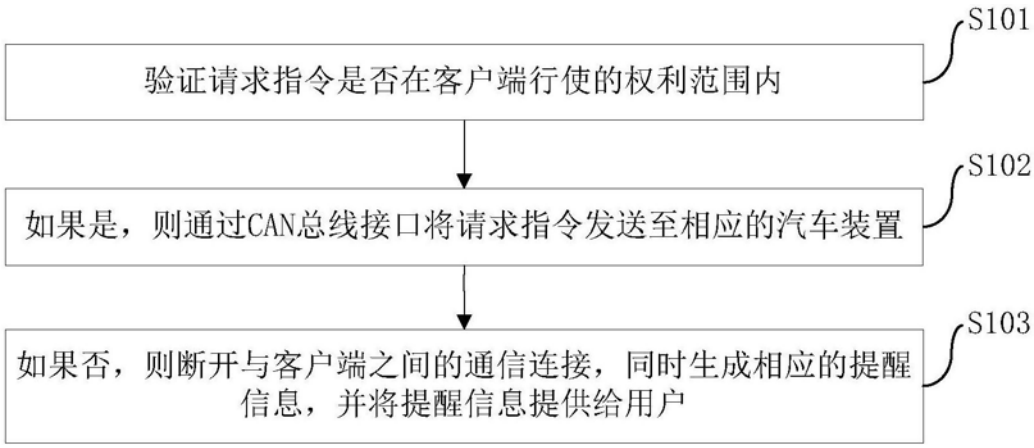

S101
验证请求指令是否在客户端行使的权利范围内
S102
如果是，则通过CAN总线接口将请求指令发送至相应的汽车装置
S103
如果否，则断开与客户端之间的通信连接，同时生成相应的提醒信息，并将提醒信息提供给用户

图2

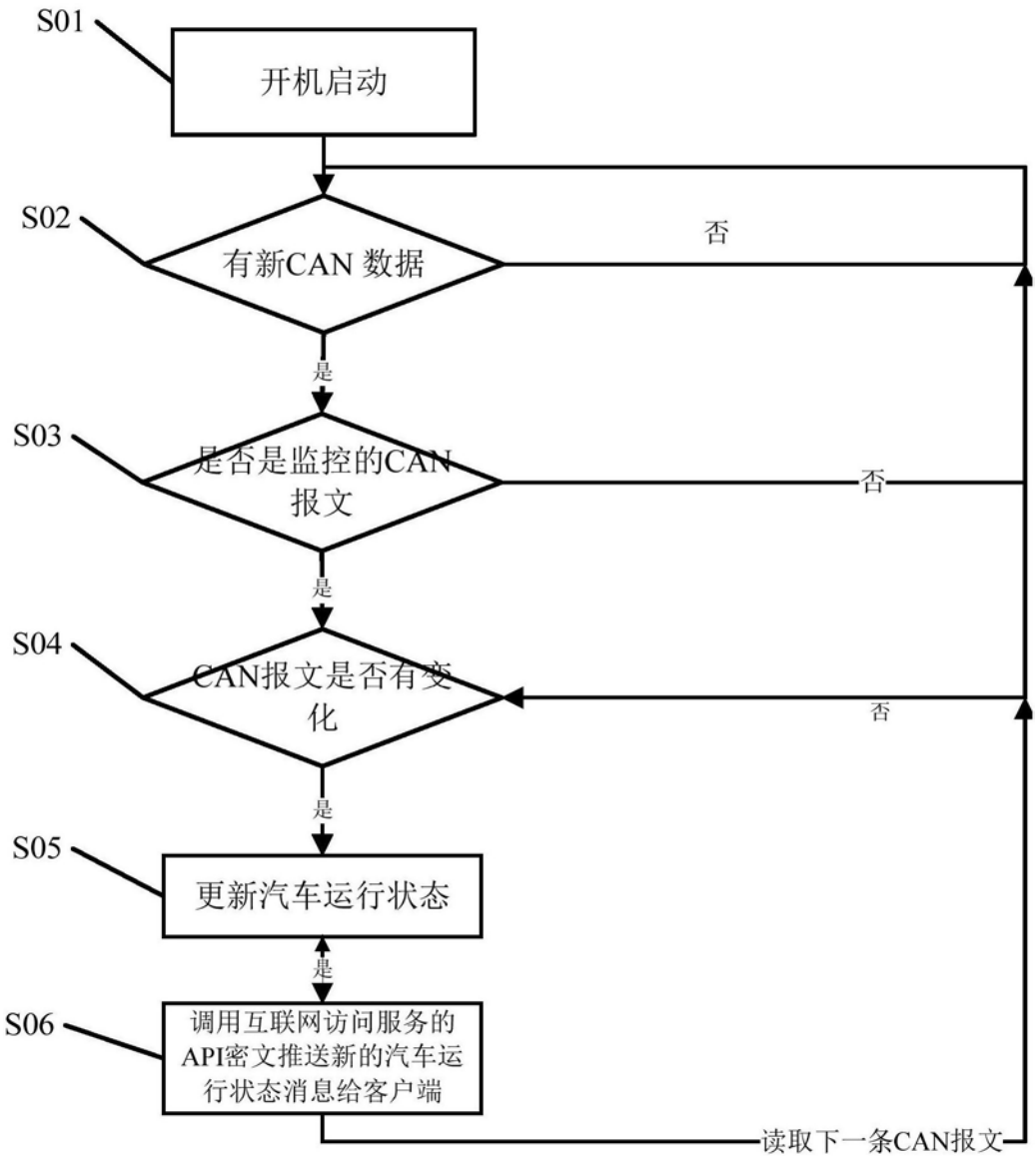

S01
开机启动
S02
有新CAN 数据
否
是
S03
是否是监控的CAN报文
否
是
S04
CAN报文是否有变化
否
是
S05
更新汽车运行状态
是
S06
调用互联网访问服务的API密文推送新的汽车运行状态消息给客户端
读取下一条CAN报文

图3

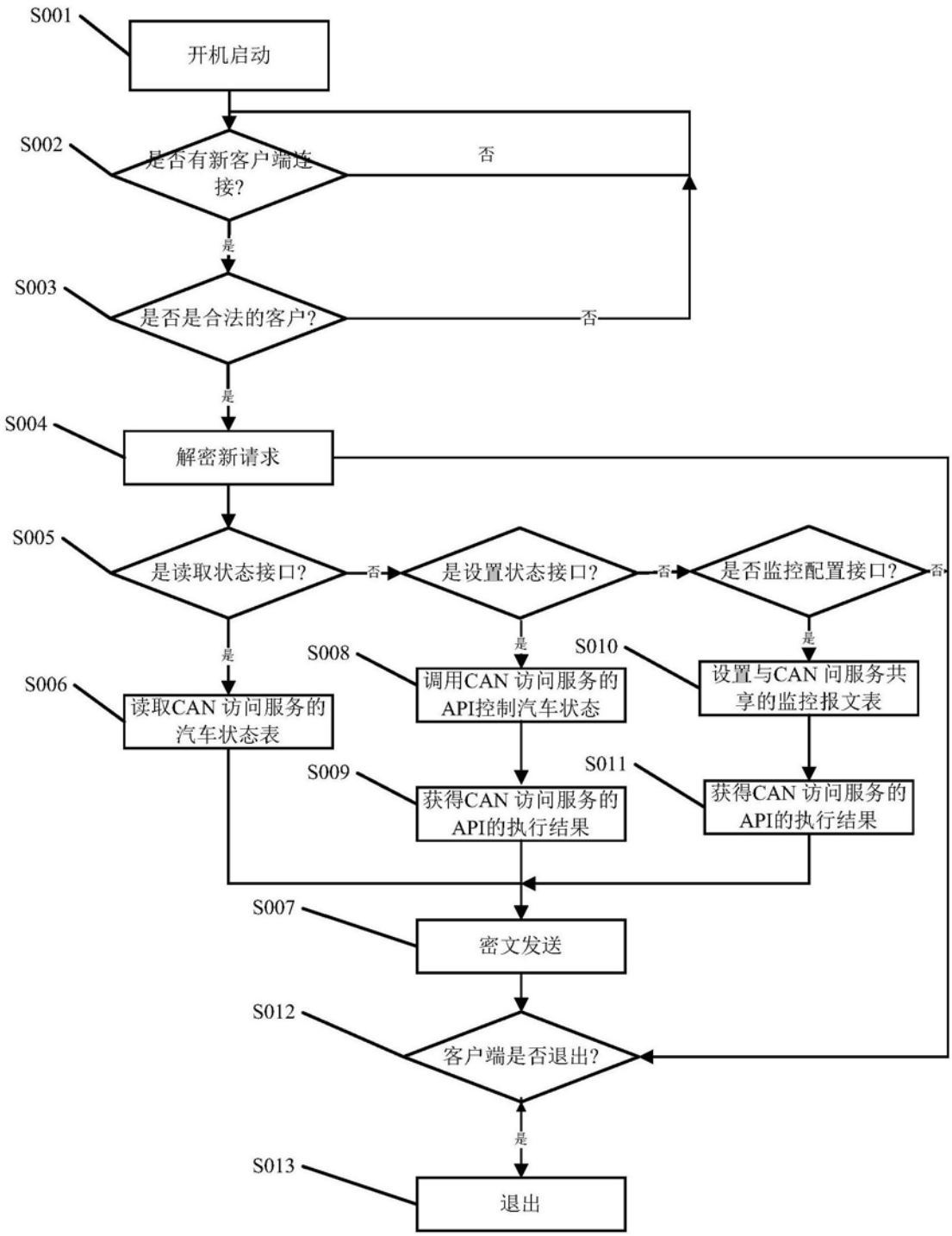

S001
开机启动
S002
是否有新客户端连接?
否
是
S003
是否是合法的客户?
否
是
S004
解密新请求
S005
是读取状态接口?
否
是设置状态接口?
否
是否监控配置接口?
否
是
是
是
S006
读取CAN 访问服务的汽车状态表
S008
调用CAN 访问服务的API控制汽车状态
S010
设置与CAN 问服务共享的监控报文表
S009
获得CAN 访问服务的API的执行结果
S011
获得CAN 访问服务的API的执行结果
S007
密文发送
S012
客户端是否退出?
是
S013
退出

图4

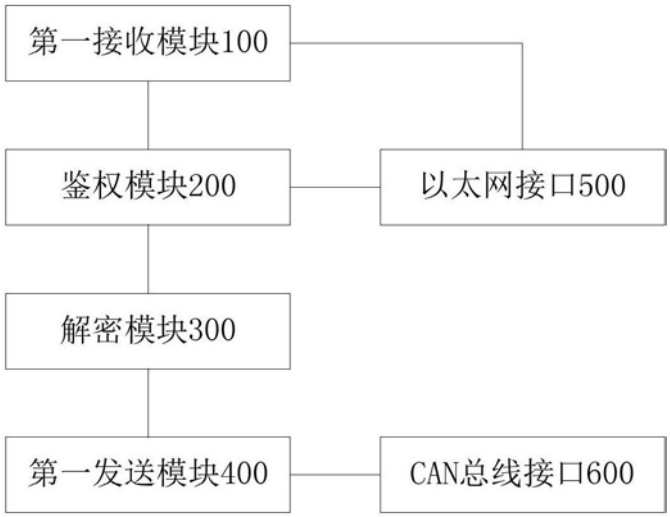

第一接收模块100
鉴权模块200
以太网接口500
解密模块300
第一发送模块400
CAN总线接口600

图5


RAM20
CPU10
FLASH30
以太网接口500
CAN总结接口600

图6

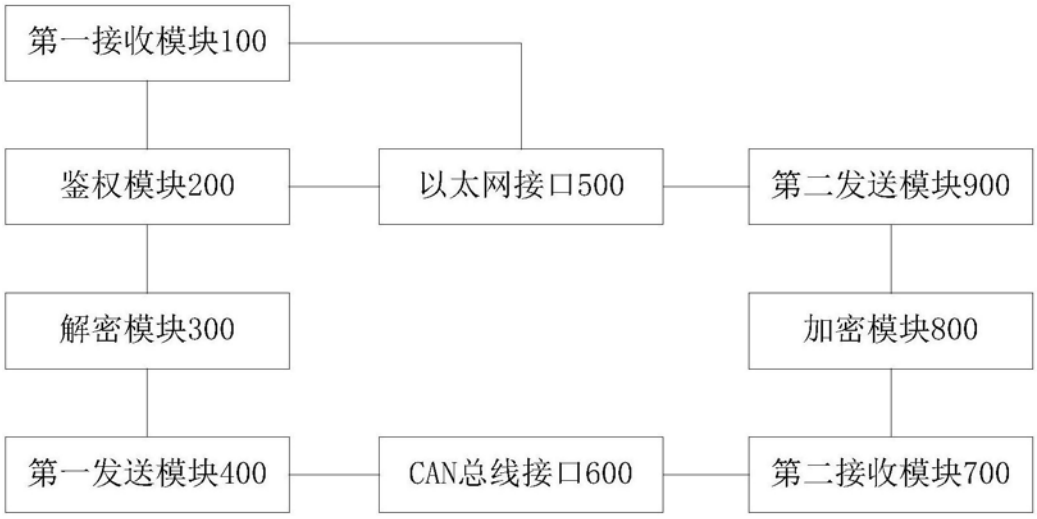

第一接收模块100
鉴权模块200
以太网接口500
第二发送模块900
解密模块300
加密模块800
第一发送模块400
CAN总线接口600
第二接收模块700

图7