(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 110191021 A
(43)申请公布日 2019.08.30

(21)申请号 201910458736.6

(22)申请日 2019.05.29

(71)申请人 北京百度网讯科技有限公司
地址 100085 北京市海淀区上地十街10号百度大厦2层

(72)发明人 曹伟

(74)专利代理机构 北京品源专利代理有限公司 11332
代理人 孟金喆

(51)Int.Cl.
H04L 12/26(2006.01)

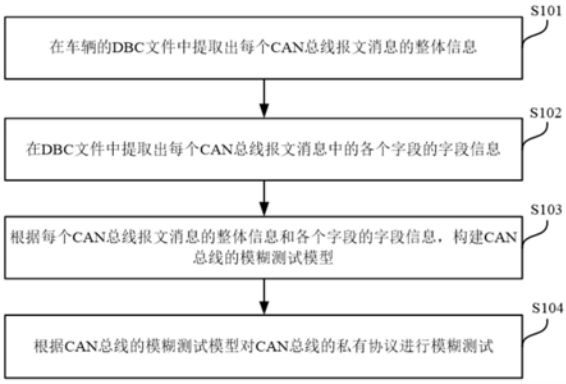
权利要求书2页 说明书13页 附图4页

(54)发明名称

一种协议测试方法、装置、电子设备及存储介质

(57)摘要

本发明实施例公开了一种协议测试方法、装置、电子设备及存储介质。所述方法包括：在车辆的控制器局域网络CAN总线消息描述文件DBC中提取出每个CAN总线报文消息的整体信息；在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；根据所述CAN总线的模糊测试模型对所述CAN总线的私有协议进行模糊测试。在本发明的实施例中，可以自动地构建出CAN总线的模糊测试模型，从而可以实现对CAN总线的私有协议的智能模糊测试。



CN 110191021 A

1.一种协议测试方法,其特征在于,所述方法包括:

在车辆的控制器局域网络CAN总线消息描述文件DBC中提取出每个CAN总线报文消息的整体信息;

在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息;

根据每个CAN总线报文消息的整体信息和各个字段的字段信息,构建CAN总线的模糊测试模型;

根据所述CAN总线的模糊测试模型对所述CAN总线的私有协议进行模糊测试。

2.根据权利要求1所述的方法,其特征在于,所述在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息,包括:

将所述DBC文件的当前行与预先设置的第一正则表达式进行匹配;

若所述当前行与所述第一正则表达式匹配成功,将所述当前行确定为当前CAN总线报文消息的起始行;并在所述当前CAN总线报文消息的起始行中提取出所述当前CAN总线报文消息的整体信息。

3.根据权利要求2所述的方法,其特征在于,所述在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息,包括:

将所述当前行的下一行作为所述当前行;将所述当前行与预先设置的第二正则表达式进行匹配;

若所述当前行与所述第二正则表达式匹配成功,将所述当前行确定为所述当前CAN总线报文消息的当前目标字段;并在所述当前目标字段中提取出所述当前目标字段的字段信息;重复执行上述操作,直到所述当前行与所述第二正则表达式匹配失败。

4.根据权利要求3所述的方法,其特征在于,在所述根据每个CAN总线报文消息的整体信息和各个字段的字段信息,构建CAN总线的模糊测试模型之前,所述方法还包括:

采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理,并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置;

根据各个字段在每个CAN总线报文消息中的偏移位置,在每个CAN总线报文消息中将全部字段进行排序,并填充每个CAN总线报文消息中的保留字段。

5.根据权利要求1所述的方法,其特征在于,所述根据每个CAN总线报文消息的整体信息和各个字段的字段信息,构建CAN总线的模糊测试模型,包括:

根据每个CAN总线报文消息中的各个字段的字段信息,将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中;

根据每个CAN总线报文消息中的各个字段对应的字段类别,构建所述CAN总线的模糊测试模型。

6.一种协议测试装置,其特征在于,所述装置包括:提取模块、构建模块和测试模块;其中,

所述提取模块,用于在车辆的控制器局域网络CAN总线消息描述文件DBC中提取出每个CAN总线报文消息的整体信息;在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息;

所述构建模块,用于根据每个CAN总线报文消息的整体信息和各个字段的字段信息,构建CAN总线的模糊测试模型;

所述测试模块，用于根据所述CAN总线的模糊测试模型对所述CAN总线的私有协议进行模糊测试。

7.根据权利要求6所述的装置，其特征在于，所述提取模块包括：匹配子模块和提取子模块；其中，

所述匹配子模块，用于将所述DBC文件的当前行与预先设置的第一正则表达式进行匹配；

所述提取子模块，用于若所述当前行与所述第一正则表达式匹配成功，将所述当前行确定为当前CAN总线报文消息的起始行；并在所述当前CAN总线报文消息的起始行中提取出所述当前CAN总线报文消息的整体信息。

8.根据权利要求7所述的装置，其特征在于：

所述匹配子模块，还用于若所述当前行与所述第一正则表达式匹配成功，将所述当前行的下一行作为所述当前行；将所述当前行与预先设置的第二正则表达式进行匹配；

所述提取子模块，还用于若所述当前行与所述第二正则表达式匹配成功，将所述当前行确定为所述当前CAN总线报文消息的当前目标字段；并在所述当前目标字段中提取出所述当前目标字段的字段信息；重复执行上述操作，直到所述当前行与所述第二正则表达式匹配失败。

9.根据权利要求8所述的装置，其特征在于，所述提取模块还包括：处理子模块，用于采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理，并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置；根据各个字段在每个CAN总线报文消息中的偏移位置，在每个CAN总线报文消息中将全部字段进行排序，并填充每个CAN总线报文消息中的保留字段。

10.根据权利要求6所述的装置，其特征在于，所述构建模块包括：划分子模块和构建子模块；其中，

所述划分子模块，用于根据每个CAN总线报文消息中的各个字段的字段信息，将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中；

所述构建子模块，用于根据每个CAN总线报文消息中的各个字段对应的字段类别，构建所述CAN总线的模糊测试模型。

11.一种电子设备，其特征在于，包括：

一个或多个处理器；

存储器，用于存储一个或多个程序，

当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现如权利要求1至5中任一项所述的协议测试方法。

12.一种存储介质，其上存储有计算机程序，其特征在于，该程序被处理器执行时实现如权利要求1至5中任一项所述的协议测试方法。

一种协议测试方法、装置、电子设备及存储介质

技术领域

[0001] 本发明实施例涉及互联网技术领域，尤其涉及一种协议测试方法、装置、电子设备及存储介质。

背景技术

[0002] 模糊测试(Fuzz Testing)是一种被广泛使用的软件安全性测试技术，用于发现软件(例如应用程序、协议实现体等)中的隐患，其基本原理是：向待测目标(例如运行有相关软件的服务器、PC等)发送大量的无效输入或错误输入，使得待测目标以非预期的方式运行，从而发现故障。例如，向待测目标发送无效输入，导致待测目标出现内存冲突、程序崩溃、资源用尽等状况。

[0003] 随着车联网的安全问题日益突出，控制器局域网络CAN总线的模糊测试逐渐被安全研究人员提起和应用。对于CAN总线上公开使用的通信协议(该类协议被称为CAN总线的公开协议)，例如UDS、KWP2000、XCP等通信协议，可以使用公开的协议定义文档构建CAN总线的模糊测试模型，然后通过该模糊测试模型对CAN总线的公开协议进行智能模糊测试；然而对于厂家自定义的CAN总线的通信协议(该类协议被称为CAN总线的私有协议)，由于没有公开的协议定义文档，无法通过公开的协议定义文档构建CAN总线的模糊测试模型，对于CAN总线的私有协议构建模糊测试模型，通常有以下两种方法：人工逆向和暴力破解；其中，人工逆向是指通过搭建协议运行环境、软件逆向运行、抓包破解等方式，逆向得到私有协议的语法格式；暴力破解是指逐个比特(bit)或者逐个字节(byte)对私有协议中的各个字段进行改变，监控程序的执行路径，以执行路径的变化规律来确定各个字段的边界大小和取值范围。然而，对于人工逆向的方法，由于CAN总线的私有协议是由不同的车厂定制，不同的车厂、甚至不同的车型都具有不同的协议语法，采用人工逆向的方法耗时太大，在CAN总线的私有协议的模糊测试中并不适用。另外，对于暴力逆向的方法，CAN总线的私有协议通常运行在无操作系统的电子控制单元(Electronic Control Unit，ECU)中，很难运行监控程序去监控协议程序的执行路径，暴力逆向的方法也无法应用在CAN总线的私有协议的模糊测试中。

发明内容

[0004] 有鉴于此，本发明实施例提供一种协议测试方法、装置、电子设备及存储介质，可以自动地构建出CAN总线的模糊测试模型，从而可以实现对CAN总线的私有协议的智能模糊测试。

[0005] 第一方面，本发明实施例提供了一种协议测试方法，所述方法包括：

[0006] 在车辆的CAN总线消息描述文件DBC中提取出每个CAN总线报文消息的整体信息；

[0007] 在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；

[0008] 根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；

[0009] 根据所述CAN总线的模糊测试模型对所述CAN总线的私有协议进行模糊测试。

[0010] 在上述实施例中，所述在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息，包括：

[0011] 将所述DBC文件的当前行与预先设置的第一正则表达式进行匹配；

[0012] 若所述当前行与所述第一正则表达式匹配成功，将所述当前行确定为当前CAN总线报文消息的起始行；并在所述当前CAN总线报文消息的起始行中提取出所述当前CAN总线报文消息的整体信息。

[0013] 在上述实施例中，所述在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息，包括：

[0014] 将所述当前行的下一行作为所述当前行；将所述当前行与预先设置的第二正则表达式进行匹配；

[0015] 若所述当前行与所述第二正则表达式匹配成功，将所述当前行确定为所述当前CAN总线报文消息的当前目标字段；并在所述当前目标字段中提取出所述当前目标字段的字段信息；重复执行上述操作，直到所述当前行与所述第二正则表达式匹配失败。

[0016] 在上述实施例中，在所述根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型之前，所述方法还包括：

[0017] 采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理，并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置；

[0018] 根据各个字段在每个CAN总线报文消息中的偏移位置，在每个CAN总线报文消息中将全部字段进行排序，并填充每个CAN总线报文消息中的保留字段。

[0019] 在上述实施例中，所述根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型，包括：

[0020] 根据每个CAN总线报文消息中的各个字段的字段信息，将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中；

[0021] 根据每个CAN总线报文消息中的各个字段对应的字段类别，构建所述CAN总线的模糊测试模型。

[0022] 第二方面，本发明实施例提供了一种协议测试装置，所述装置包括：提取模块、构建模块和测试模块；其中，

[0023] 所述提取模块，用于在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息；在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；

[0024] 所述构建模块，用于根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；

[0025] 所述测试模块，用于根据所述CAN总线的模糊测试模型对所述CAN总线的私有协议进行模糊测试。

[0026] 在上述实施例中，所述提取模块包括：匹配子模块和提取子模块；其中，

[0027] 所述匹配子模块，用于将所述DBC文件的当前行与预先设置的第一正则表达式进行匹配；

[0028] 所述提取子模块，用于若所述当前行与所述第一正则表达式匹配成功，将所述当前行确定为当前CAN总线报文消息的起始行；并在所述当前CAN总线报文消息的起始行中提

取出所述当前CAN总线报文消息的整体信息。

[0029] 在上述实施例中，所述匹配子模块，还用于若所述当前行与所述第一正则表达式匹配成功，将所述当前行的下一行作为所述当前行；将所述当前行与预先设置的第二正则表达式进行匹配；

[0030] 所述提取子模块，还用于若所述当前行与所述第二正则表达式匹配成功，将所述当前行确定为所述当前CAN总线报文消息的当前目标字段；并在所述当前目标字段中提取出所述当前目标字段的字段信息；重复执行上述操作，直到所述当前行与所述第二正则表达式匹配失败。

[0031] 在上述实施例中，所述提取模块还包括：处理子模块，用于采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理，并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置；根据各个字段在每个CAN总线报文消息中的偏移位置，在每个CAN总线报文消息中将全部字段进行排序，并填充每个CAN总线报文消息中的保留字段。

[0032] 在上述实施例中，所述构建模块包括：划分子模块和构建子模块；其中，

[0033] 所述划分子模块，用于根据每个CAN总线报文消息中的各个字段的字段信息，将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中；

[0034] 所述构建子模块，用于根据每个CAN总线报文消息中的各个字段对应的字段类别，构建所述CAN总线的模糊测试模型。

[0035] 第三方面，本发明实施例提供了一种电子设备，包括：

[0036] 一个或多个处理器；

[0037] 存储器，用于存储一个或多个程序，

[0038] 当所述一个或多个程序被所述一个或多个处理器执行，使得所述一个或多个处理器实现本发明任意实施例所述的协议测试方法。

[0039] 第四方面，本发明实施例提供了一种存储介质，其上存储有计算机程序，该程序被处理器执行时实现本发明任意实施例所述的协议测试方法。

[0040] 本发明实施例提出了一种协议测试方法、装置、电子设备及存储介质，先在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息；在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；然后根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；再根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。也就是说，在本发明的技术方案中，可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型，从而可以根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。而在现有的协议测试方法中，对于人工逆向的方法，由于CAN总线的私有协议是由不同的车厂定制，不同的车厂、甚至不同的车型都具有不同的协议语法，采用人工逆向的方法耗时太大，在CAN总线的私有协议的模糊测试中并不适用。另外，对于暴力逆向的方法，CAN总线的私有协议通常运行在无操作系统的电子控制单元中，很难运行监控程序去监控协议程序的执行路径，暴力逆向的方法也无法应用在CAN总线的私有协议的模糊测试中。因此，和现有技术相比，本发明实施例提出的协议测试方法、装置、电子设备及存储介质，可以自动地构建出CAN总线的模糊测试模型，从而可以实现对CAN总线的私有协议的智能模糊测试；并且，本发明实施例的技术方案实现简单方

便、便于普及，适用范围更广。

附图说明

[0041] 图1为本发明实施例一提供的协议测试方法的流程示意图；

[0042] 图2为本发明实施例二提供的协议测试方法的流程示意图；

[0043] 图3为本发明实施例三提供的协议测试方法的流程示意图；

[0044] 图4为本发明实施例四提供的协议测试装置的第一结构示意图；

[0045] 图5为本发明实施例四提供的协议测试装置的第二结构示意图；

[0046] 图6为本发明实施例五提供的电子设备的结构示意图。

具体实施方式

[0047] 下面结合附图和实施例对本发明作进一步的详细说明。可以理解的是，此处所描述的具体实施例仅仅用于解释本发明，而非对本发明的限定。另外还需要说明的是，为了便于描述，附图中仅示出了与本发明相关的部分而非全部内容。

[0048] 实施例一

[0049] 图1为本发明实施例一提供的协议测试方法的流程示意图，该方法可以由协议测试装置或者电子设备来执行，该装置或者电子设备可以由软件和/或硬件的方式实现，该装置或者电子设备可以集成在任何具有网络通信功能的智能设备中。如图1所示，协议测试方法可以包括以下步骤：

[0050] S101、在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息。

[0051] 在本发明的具体实施例中，电子设备可以在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息。具体地，电子设备可以将DBC文件的当前行与预先设置的第一正则表达式进行匹配；若当前行与第一正则表达式匹配成功，将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。例如，电子设备可以先将DBC文件IDE第一行作为当前行，然后将当前行与第一正则表达式匹配。具体地，第一正则表达式可以预先设定；例如，第一正则表达式＝re.compile(″^BO_[0-9]+.*:[0-9]+.*$″)。

[0052] 在本发明的具体实施例中，DBC文件是一种数据库文件，扩展名为.dbc，可用于定义CAN网络。举例说明，DBC文件中的当前CAN总线报文消息为：

[0053] BO_1126DCDC1:8Vector_XXX

[0054] SG_CRC:63|8@0+(1,0)[0|0]″″Vector__XXX

[0055] SG_DTC:55|8@0+(1,0)[0|0]″″Vector__XXX

[0056] SG_Reserved:47|1@0+(1,0)[0|0]″″Vector__XXX

[0057] SG_DCDC_Counter:46|4@0+(1,0)[0|0]″″Vector__XXX

[0058] SG_DCDC_Enable_State:42|1@0+(1,0)[0|0]″″Vector__XXX

[0059] SG_DCDC_Mode:41|2@0+(1,0)[0|0]″″Vector__XXX

[0060] SG_DCDC_Temperature2:39|8@0+(1,-40)[0|0]″″VCU

[0061] SG_DCDC_Input_Voltage:16|9@0+(1,0)[0|0]″″VCU

[0062] SG_DCDC_Output_Current:15|8@0+(0,0)[0|0]″″VCU

[0063] SG_DCDC_Onput_Voltage:7|8@0+(1,0)[0|0]""VCU

[0064] S102、在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息。

[0065] 在本发明的具体实施例中，电子设备可以在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息。具体地，电子设备可以将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配；若当前行与第二正则表达式匹配成功，将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；重复执行上述操作，直到当前行与第二正则表达式匹配失败。例如，电子设备在将第一行与第一正则表达式匹配成功时，可以将第二行作为当前行，然后将第二行与第二正则表达式进行匹配；假设第二行与第二正则表达式匹配成功，将第二行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息。接着，可以将第三行作为当前行，然后将第三行与第二正则表达式进行匹配；假设第三行与第二正则表达式匹配成功，将第三行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息。以此类推，直到当前行与第二正则表达式匹配失败。具体地，第二正则表达式可以预先设定；例如，第二正则表达式＝re.compile("^.*SG_.*:.*[0-9]+|[0-9]+@*$")。

[0066] S103、根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型。

[0067] 在本发明的具体实施例中，电子设备可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型。具体地，电子设备可以先根据每个CAN总线报文消息中的各个字段的字段信息，将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中；然后根据每个CAN总线报文消息中的各个字段对应的字段类别，构建CAN总线的模糊测试模型。

[0068] 在本发明的具体实施例中，CAN总线的模糊测试模型可以包括以下三部分：数据模型、状态模型和测试配置；其中，数据模型可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息，使用建模工具构建出CAN总线的数据模型。另外，对于状态模型，由于CAN应用报文采用无连接协议传输，其状态只有发送数据，该部门无需借助DBC文件，可由人工预定义最适用的规则，在模糊测试模型自动生成时进行填充。此外，对于测试配置，模糊测试模型中的测试配置包括：状态模型声明、输出声明、变异器声明、策略声明，该部门无需借助DBC文件，可由人工预定义最适用的规则，在模糊测试模型自动生成时进行填充。

[0069] 较佳地，在本发明的具体实施例中，电子设备可以将CAN总线报文消息字段分为三类，分别为：Flag、Number_Length和Number_CRC；其中，Flag是指携带应用报文信息并且以bit为单位的字段；Number_Length是指消息的长度以字节为单位，和消息实际长度相关并且可以动态改变的字段；Number_CRC是指消息的校验字段以字节为单位，与消息实际数据填充相关的字段。电子设备可以使用关键字识别出这三类字段，并生成数据模型。

[0070] 在本发明的具体实施例中，电子设备在根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型之前，还可以采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理，并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置；根据各个字段在每个CAN总线报文消息中的偏移位置，在每个CAN总线报文消息中将全部字段进行排序，并填充每个CAN总线报文消息

中的保留字段。

[0071] 在本发明的具体实施例中，CAN总线的模糊测试模型可以如下所示：

[0072]

```
<DataModel name="DCDC1">
    <Flags endian="big" name="before_crc" size="56">
        <Flag name="DCDC=Output_Voltage" position="0" size="8" value="0" />
        <Flag name="DCDC=Output_Current" position="8" size="8" value="0" />
        <Flag name="reserved_2" position="16" size="7" value="0" />
        <Flag name="DCDC_Input_Voltage" position="23" size="9" value="0" />
        <Flag name="DCDC_Temperature" position="32" size="8" value="0" />
        <Flag name="Reserved" position="40" size="1" value="0" />
        <Flag name="DCDC_Counter" position="41" size="4" value="0" />
        <Flag name="DCDC_Enable_State" position="45" size="2" value="0" />
        <Flag name="DCDC_Mode" position="46" size="2" value="0" />
        <Flag name="DTC" position="48" size="8" value="0" />
    </ Flags>
    <Number endian= "big" name="CRC" size="8">
        <Fixup class="Crc">
            <Param name="ref" value="DCDC1" />
            <Param name="type" value="CRC16" />
        </Fixup>
    </Number>
</DataModel>
```

[0073]

[0074] S104、根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。

[0075] 在本发明的具体实施例中，电子设备可以根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。具体地，电子设备可以将CAN总线的私有协议输入到CAN总线的模糊测试模型中，然后CAN总线的模糊测试模型可以输出CAN总线的私有协议的测试结果。

[0076] 本发明实施例提出的协议测试方法，先在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息；在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；然后根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；再根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。也就是说，在本发明的技术方案中，可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型，从而可以根据CAN总线的模糊测试模型对CAN总线的私有协

议进行模糊测试。而在现有的协议测试方法中，对于人工逆向的方法，由于CAN总线的私有协议是由不同的车厂定制，不同的车厂、甚至不同的车型都具有不同的协议语法，采用人工逆向的方法耗时太大，在CAN总线的私有协议的模糊测试中并不适用。另外，对于暴力逆向的方法，CAN总线的私有协议通常运行在无操作系统的电子控制单元中，很难运行监控程序去监控协议程序的执行路径，暴力逆向的方法也无法应用在CAN总线的私有协议的模糊测试中。因此，和现有技术相比，本发明实施例提出的协议测试方法，可以自动地构建出CAN总线的模糊测试模型，从而可以实现对CAN总线的私有协议的智能模糊测试；并且，本发明实施例的技术方案实现简单方便、便于普及，适用范围更广。

[0077] 实施例二

[0078] 图2为本发明实施例二提供的协议测试方法的流程示意图。如图2所示，协议测试方法可以包括以下步骤：

[0079] S201、将DBC文件的当前行与预先设置的第一正则表达式进行匹配；若当前行与第一正则表达式匹配成功，执行S202；否则，执行S205。

[0080] 在本发明的具体实施例中，电子设备可以将DBC文件的当前行与预先设置的第一正则表达式进行匹配；若当前行与第一正则表达式匹配成功，执行S202；若当前行与第一正则表达式匹配失败，执行S205。例如，电子设备可以先将DBC文件的第一行与第一正则表达式进行匹配；若第一行与第一正则表达式匹配成功，执行S202；若第一行与第一正则表达式匹配失败，执行S205。

[0081] S202、将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。

[0082] 在本发明的具体实施例中，若当前行与第一正则表达式匹配成功，电子设备可以将将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。例如，若第一行与第一正则表达式匹配成功，电子设备可以将第一行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。具体地，当前DBC报文消息的整体信息至少可以包括：报文名称、请求ID、消息大小。

[0083] S203、将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配；若当前行与第二正则表达式匹配成功，执行S204；否则，返回执行S201。

[0084] 在本发明的具体实施例中，电子设备可以将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配；若当前行与第二正则表达式匹配成功，执行S204；若当前行与第二正则表达式匹配失败，返回执行S201。例如，假设第一行与第一正则表达式匹配成功，在本步骤中，电子设备可以将第二行作为当前行，将第二行与第二正则表达式进行匹配；若第二行与第二正则表达式匹配成功，执行S204；若第二行与第二正则表达式匹配失败，返回执行S201。

[0085] S204、将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；返回执行S203。

[0086] 在本发明的具体实施例中，若当前行与第二正则表达式匹配成功，电子设备可以将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；返回执行S203。例如，假设第二行与第二正则表达式匹配成功，在本

步骤中，电子设备可以将第二行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；返回执行S203。具体地，当前目标字段的字段信息至少包括：字段名称、字段位置、字段大小、字节序、默认值。

[0087] S205、判断是否获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息，若是，执行S206；否则，执行S208。

[0088] 在本步骤中，电子设备可以判断是否获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息；若电子设备获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息，执行S206；若电子设备未获取到任何CAN总线报文消息的整体信息和各个字段的字段信息，执行S208。

[0089] S206、根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型。

[0090] 在本发明的具体实施例中，电子设备可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型。具体地，电子设备可以先根据每个CAN总线报文消息中的各个字段的字段信息，将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中；然后根据每个CAN总线报文消息中的各个字段对应的字段类别，构建CAN总线的模糊测试模型。

[0091] 在本发明的具体实施例中，电子设备在根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型之前，还可以采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理，并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置；根据各个字段在每个CAN总线报文消息中的偏移位置，在每个CAN总线报文消息中将全部字段进行排序，并填充每个CAN总线报文消息中的保留字段。

[0092] S207、根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。

[0093] 在本发明的具体实施例中，电子设备可以根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。具体地，电子设备可以将CAN总线的私有协议输入到CAN总线的模糊测试模型中，然后CAN总线的模糊测试模型可以输出CAN总线的私有协议的测试结果。

[0094] S208、结束协议测试流程。

[0095] 在本发明的具体实施例中，若电子设备未获取到任何CAN总线报文消息的整体信息和各个字段的字段信息，结束协议测试流程；或者，根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试之后，结束协议测试流程。

[0096] 本发明实施例提出的协议测试方法，先在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息；在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；然后根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；再根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。也就是说，在本发明的技术方案中，可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型，从而可以根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。而在现有的协议测试方法中，对于人工逆向的方法，由于CAN总线的私有协议是由不同的车厂定制，不同的车厂、甚至不同的车型都具有不同的协议语法，采用人工逆向的方法耗时太大，在CAN总线的私有协议的模糊测试中并不适用。另外，对于暴力逆向

的方法，CAN总线的私有协议通常运行在无操作系统的电子控制单元中，很难运行监控程序去监控协议程序的执行路径，暴力逆向的方法也无法应用在CAN总线的私有协议的模糊测试中。因此，和现有技术相比，本发明实施例提出的协议测试方法，可以自动地构建出CAN总线的模糊测试模型，从而可以实现对CAN总线的私有协议的智能模糊测试；并且，本发明实施例的技术方案实现简单方便、便于普及，适用范围更广。

[0097] 实施例三

[0098] 图3为本发明实施例三提供的协议测试方法的流程示意图。如图3所示，协议测试方法可以包括以下步骤：

[0099] S301、将DBC文件的当前行与预先设置的第一正则表达式进行匹配；若当前行与第一正则表达式匹配成功，执行S302；否则，执行S305。

[0100] 在本发明的具体实施例中，电子设备可以将DBC文件的当前行与预先设置的第一正则表达式进行匹配；若当前行与第一正则表达式匹配成功，执行S302；若当前行与第一正则表达式匹配失败，执行S305。例如，电子设备可以先将DBC文件的第一行与第一正则表达式进行匹配；若第一行与第一正则表达式匹配成功，执行S302；若第一行与第一正则表达式匹配失败，执行S305。

[0101] S302、将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。

[0102] 在本发明的具体实施例中，若当前行与第一正则表达式匹配成功，电子设备可以将将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。例如，若第一行与第一正则表达式匹配成功，电子设备可以将第一行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息。具体地，当前DBC报文消息的整体信息至少可以包括：报文名称、请求ID、消息大小。

[0103] S303、将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配；若当前行与第二正则表达式匹配成功，执行S304；否则，返回执行S301。

[0104] 在本发明的具体实施例中，电子设备可以将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配；若当前行与第二正则表达式匹配成功，执行S304；若当前行与第二正则表达式匹配失败，返回执行S301。例如，假设第一行与第一正则表达式匹配成功，在本步骤中，电子设备可以将第二行作为当前行，将第二行与第二正则表达式进行匹配；若第二行与第二正则表达式匹配成功，执行S304；若第二行与第二正则表达式匹配失败，返回执行S301。

[0105] S304、将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；返回执行S303。

[0106] 在本发明的具体实施例中，若当前行与第二正则表达式匹配成功，电子设备可以将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；返回执行S303。例如，假设第二行与第二正则表达式匹配成功，在本步骤中，电子设备可以将第二行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息；返回执行S303。具体地，当前目标字段的字段信息至少包括：字段名称、字段位置、字段大小、字节序、默认值。

[0107] S305、判断是否获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息;若是,执行S306;否则,执行S309。

[0108] 在本步骤中,电子设备可以判断是否获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息;若电子设备获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息,执行S306;若电子设备未获取到任何CAN总线报文消息的整体信息和各个字段的字段信息,执行S309。

[0109] S306、根据每个CAN总线报文消息中的各个字段的字段信息,将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中。

[0110] 在本发明的具体实施例中,电子设备可以根据每个CAN总线报文消息中的各个字段的字段信息,将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中。具体地,电子设备可以将CAN总线报文消息字段分为三类,分别为:Flag、Number_Length和Number_CRC;其中,Flag是指携带应用报文信息并且以bit为单位的字段;Number_Length是指消息的长度以字节为单位,和消息实际长度相关并且可以动态改变的字段;Number_CRC是指消息的校验字段以字节为单位,与消息实际数据填充相关的字段。电子设备可以使用关键字识别出这三类字段。

[0111] S307、根据每个CAN总线报文消息中的各个字段对应的字段类别,构建CAN总线的模糊测试模型。

[0112] 在本发明的具体实施例中,电子设备可以根据每个CAN总线报文消息中的各个字段对应的字段类别,构建CAN总线的模糊测试模型。具体地,CAN总线的模糊测试模型可以包括以下三部分:数据模型、状态模型和测试配置;其中,数据模型可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息,使用建模工具构建出CAN总线的数据模型。另外,对于状态模型,由于CAN应用报文采用无连接协议传输,其状态只有发送数据,该部门无需借助DBC文件,可由人工预定义最适用的规则,在模糊测试模型自动生成时进行填充。此外,对于测试配置,模糊测试模型中的测试配置包括:状态模型声明、输出声明、变异器声明、策略声明,该部门无需借助DBC文件,可由人工预定义最适用的规则,在模糊测试模型自动生成时进行填充。

[0113] S308、根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。

[0114] 在本发明的具体实施例中,电子设备可以根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。具体地,电子设备可以将CAN总线的私有协议输入到CAN总线的模糊测试模型中,然后CAN总线的模糊测试模型可以输出CAN总线的私有协议的测试结果。

[0115] S309、结束协议测试流程。

[0116] 在本发明的具体实施例中,若电子设备未获取到任何CAN总线报文消息的整体信息和各个字段的字段信息,结束协议测试流程;或者,根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试之后,结束协议测试流程。

[0117] 本发明实施例提出的协议测试方法,在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息;在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息;然后根据每个CAN总线报文消息的整体信息和各个字段的字段信息,构建CAN总线的模糊测试模型;再根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。也就是说,在本发明的技术方案中,可以根据每个CAN总线报文消息的整体信息和各个字段的字段信息,构

建CAN总线的模糊测试模型，从而可以根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试。而在现有的协议测试方法中，对于人工逆向的方法，由于CAN总线的私有协议是由不同的车厂定制，不同的车厂、甚至不同的车型都具有不同的协议语法，采用人工逆向的方法耗时太大，在CAN总线的私有协议的模糊测试中并不适用。另外，对于暴力逆向的方法，CAN总线的私有协议通常运行在无操作系统的电子控制单元中，很难运行监控程序去监控协议程序的执行路径，暴力逆向的方法也无法应用在CAN总线的私有协议的模糊测试中。因此，和现有技术相比，本发明实施例提出的协议测试方法，可以自动地构建出CAN总线的模糊测试模型，从而可以实现对CAN总线的私有协议的智能模糊测试；并且，本发明实施例的技术方案实现简单方便、便于普及，适用范围更广。

[0118] 实施例四

[0119] 图4为本发明实施例四提供的协议测试装置的第一结构示意图。如图4所示，本发明实施例所述的协议测试装置可以包括：提取模块401、构建模块402和测试模块403；其中，

[0120] 所述提取模块401，用于在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息；在所述DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息；

[0121] 所述构建模块402，用于根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型；

[0122] 所述测试模块403，用于根据所述CAN总线的模糊测试模型对所述CAN总线的私有协议进行模糊测试。

[0123] 图5为本发明实施例四提供的协议测试装置的第二结构示意图。如图5所示，所述提取模块401包括：匹配子模块4011和提取子模块4012；其中，

[0124] 所述匹配子模块4011，用于将所述DBC文件的当前行与预先设置的第一正则表达式进行匹配；

[0125] 所述提取子模块4012，用于若所述当前行与所述第一正则表达式匹配成功，将所述当前行确定为当前CAN总线报文消息的起始行；并在所述当前CAN总线报文消息的起始行中提取出所述当前CAN总线报文消息的整体信息。

[0126] 进一步的，所述匹配子模块4011，还用于若所述当前行与所述第一正则表达式匹配成功，将所述当前行的下一行作为所述当前行；将所述当前行与预先设置的第二正则表达式进行匹配；

[0127] 所述提取子模块4012，还用于若所述当前行与所述第二正则表达式匹配成功，将所述当前行确定为所述当前CAN总线报文消息的当前目标字段；并在所述当前目标字段中提取出所述当前目标字段的字段信息；重复执行上述操作，直到所述当前行与所述第二正则表达式匹配失败。

[0128] 进一步的，所述提取模块还包括：处理子模块(图中未示出)，用于采用大端字节序模式将每个CAN总线报文消息中的各个字段进行字节序转换处理，并根据处理后的各个字段调整各个字段在每个CAN总线报文消息中的偏移位置；根据各个字段在每个CAN总线报文消息中的偏移位置，在每个CAN总线报文消息中将全部字段进行排序，并填充每个CAN总线报文消息中的保留字段。

[0129] 进一步的，所述构建模块402包括：划分子模块4021和构建子模块4022；其中，

[0130] 所述划分子模块4021，用于根据每个CAN总线报文消息中的各个字段的字段信息，

将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中；

[0131] 所述构建子模块4022，用于根据每个CAN总线报文消息中的各个字段对应的字段类别，构建所述CAN总线的模糊测试模型。

[0132] 上述协议测试装置可执行本发明任意实施例所提供的方法，具备执行方法相应的功能模块和有益效果。未在本实施例中详尽描述的技术细节，可参见本发明任意实施例提供的协议测试方法。

[0133] 实施例五

[0134] 图6为本发明实施例五提供的电子设备的结构示意图。图6示出了适于用来实现本发明实施方式的示例性电子设备的框图。图6显示的电子设备12仅仅是一个示例，不应对本发明实施例的功能和使用范围带来任何限制。

[0135] 如图6所示，电子设备12以通用计算设备的形式表现。电子设备12的组件可以包括但不限于：一个或者多个处理器或者处理单元16，系统存储器28，连接不同系统组件(包括系统存储器28和处理单元16)的总线18。

[0136] 总线18表示几类总线结构中的一种或多种，包括存储器总线或者存储器控制器，外围总线，图形加速端口，处理器或者使用多种总线结构中的任意总线结构的局域总线。举例来说，这些体系结构包括但不限于工业标准体系结构(ISA)总线，微通道体系结构(MAC)总线，增强型ISA总线、视频电子标准协会(VESA)局域总线以及外围组件互连(PCI)总线。

[0137] 电子设备12典型地包括多种计算机系统可读介质。这些介质可以是任何能够被电子设备12访问的可用介质，包括易失性和非易失性介质，可移动的和不可移动的介质。

[0138] 系统存储器28可以包括易失性存储器形式的计算机系统可读介质，例如随机存取存储器(RAM)30和/或高速缓存存储器32。电子设备12可以进一步包括其它可移动/不可移动的、易失性/非易失性计算机系统存储介质。仅作为举例，存储系统34可以用于读写不可移动的、非易失性磁介质(图6未显示，通常称为“硬盘驱动器”)。尽管图6中未示出，可以提供用于对可移动非易失性磁盘(例如“软盘”)读写的磁盘驱动器，以及对可移动非易失性光盘(例如CD-ROM，DVD-ROM或者其它光介质)读写的光盘驱动器。在这些情况下，每个驱动器可以通过一个或者多个数据介质接口与总线18相连。存储器28可以包括至少一个程序产品，该程序产品具有一组(例如至少一个)程序模块，这些程序模块被配置以执行本发明各实施例的功能。

[0139] 具有一组(至少一个)程序模块42的程序/实用工具40，可以存储在例如存储器28中，这样的程序模块42包括但不限于操作系统、一个或者多个应用程序、其它程序模块以及程序数据，这些示例中的每一个或某种组合中可能包括网络环境的实现。程序模块42通常执行本发明所描述的实施例中的功能和/或方法。

[0140] 电子设备12也可以与一个或多个外部设备14(例如键盘、指向设备、显示器24等)通信，还可与一个或者多个使得用户能与该电子设备12交互的设备通信，和/或与使得该电子设备12能与一个或多个其它计算设备进行通信的任何设备(例如网卡，调制解调器等等)通信。这种通信可以通过输入/输出(I/O)接口22进行。并且，电子设备12还可以通过网络适配器20与一个或者多个网络(例如局域网(LAN)，广域网(WAN)和/或公共网络，例如因特网)通信。如图所示，网络适配器20通过总线18与电子设备12的其它模块通信。应当明白，尽管图6中未示出，可以结合电子设备12使用其它硬件和/或软件模块，包括但不限于：微代码、

设备驱动器、冗余处理单元、外部磁盘驱动阵列、RAID系统、磁带驱动器以及数据备份存储系统等。

[0141] 处理单元16通过运行存储在系统存储器28中的程序，从而执行各种功能应用以及数据处理，例如实现本发明实施例所提供的协议测试方法。

[0142] 实施例六

[0143] 本发明实施例六提供了一种计算机存储介质。

[0144] 本发明实施例的计算机可读存储介质，可以采用一个或多个计算机可读的介质的任意组合。计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质。计算机可读存储介质例如可以是——但不限于——电、磁、光、电磁、红外线、或半导体的系统、装置或器件，或者任意以上的组合。计算机可读存储介质的更具体的例子(非穷举的列表)包括：具有一个或多个导线的电连接、便携式计算机磁盘、硬盘、随机存取存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本文件中，计算机可读存储介质可以是任何包含或存储程序的有形介质，该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。

[0145] 计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号，其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式，包括但不限于电磁信号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。

[0146] 计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括——但不限于无线、电线、光缆、RF等等，或者上述的任意合适的组合。

[0147] 可以以一种或多种程序设计语言或其组合来编写用于执行本发明操作的计算机程序代码，所述程序设计语言包括面向对象的程序设计语言—诸如Java、Smalltalk、C++，还包括常规的过程式程序设计语言—诸如“C”语言或类似的程序设计语言。程序代码可以完全地在用户计算机上执行、部分地在用户计算机上执行、作为一个独立的软件包执行、部分在用户计算机上部分在远程计算机上执行、或者完全在远程计算机或服务器上执行。在涉及远程计算机的情形中，远程计算机可以通过任意种类的网络——包括局域网(LAN)或广域网(WAN)—连接到用户计算机，或者，可以连接到外部计算机(例如利用因特网服务提供商来通过因特网连接)。

[0148] 注意，上述仅为本发明的较佳实施例及所运用技术原理。本领域技术人员会理解，本发明不限于这里所述的特定实施例，对本领域技术人员来说能够进行各种明显的变化、重新调整和替代而不会脱离本发明的保护范围。因此，虽然通过以上实施例对本发明进行了较为详细的说明，但是本发明不仅仅限于以上实施例，在不脱离本发明构思的情况下，还可以包括更多其他等效实施例，而本发明的范围由所附的权利要求范围决定。

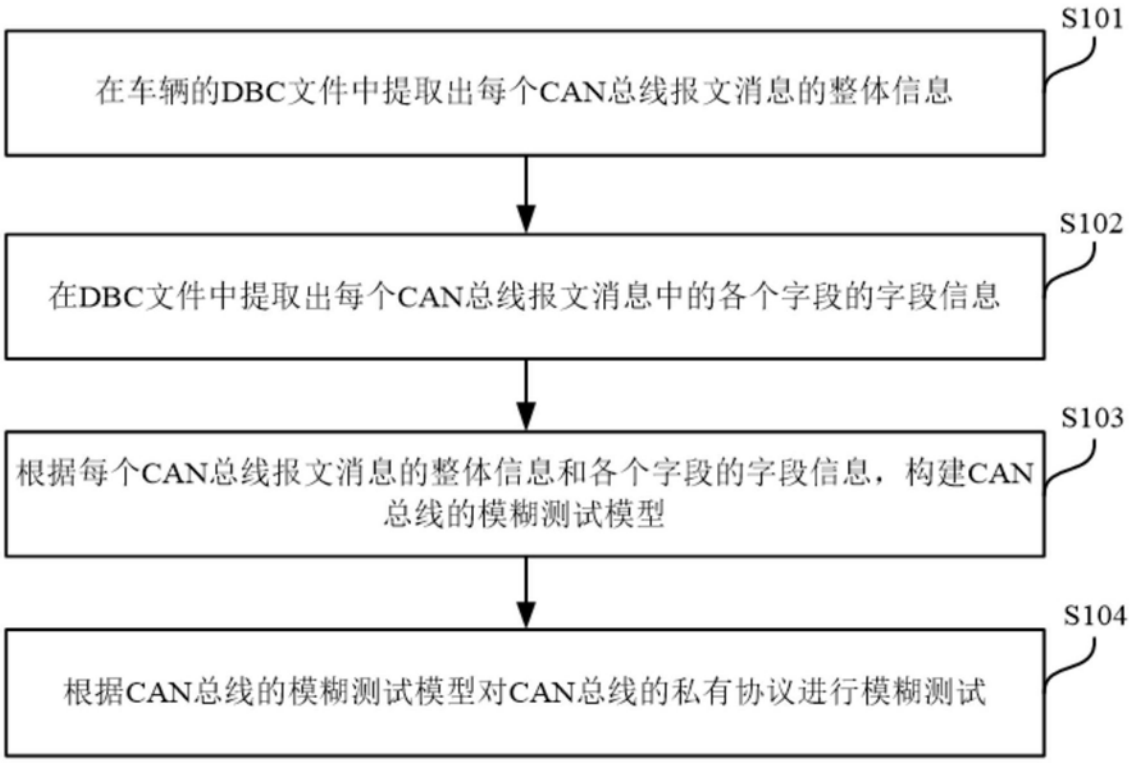

S101
在车辆的DBC文件中提取出每个CAN总线报文消息的整体信息
S102
在DBC文件中提取出每个CAN总线报文消息中的各个字段的字段信息
S103
根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型
S104
根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试

图1

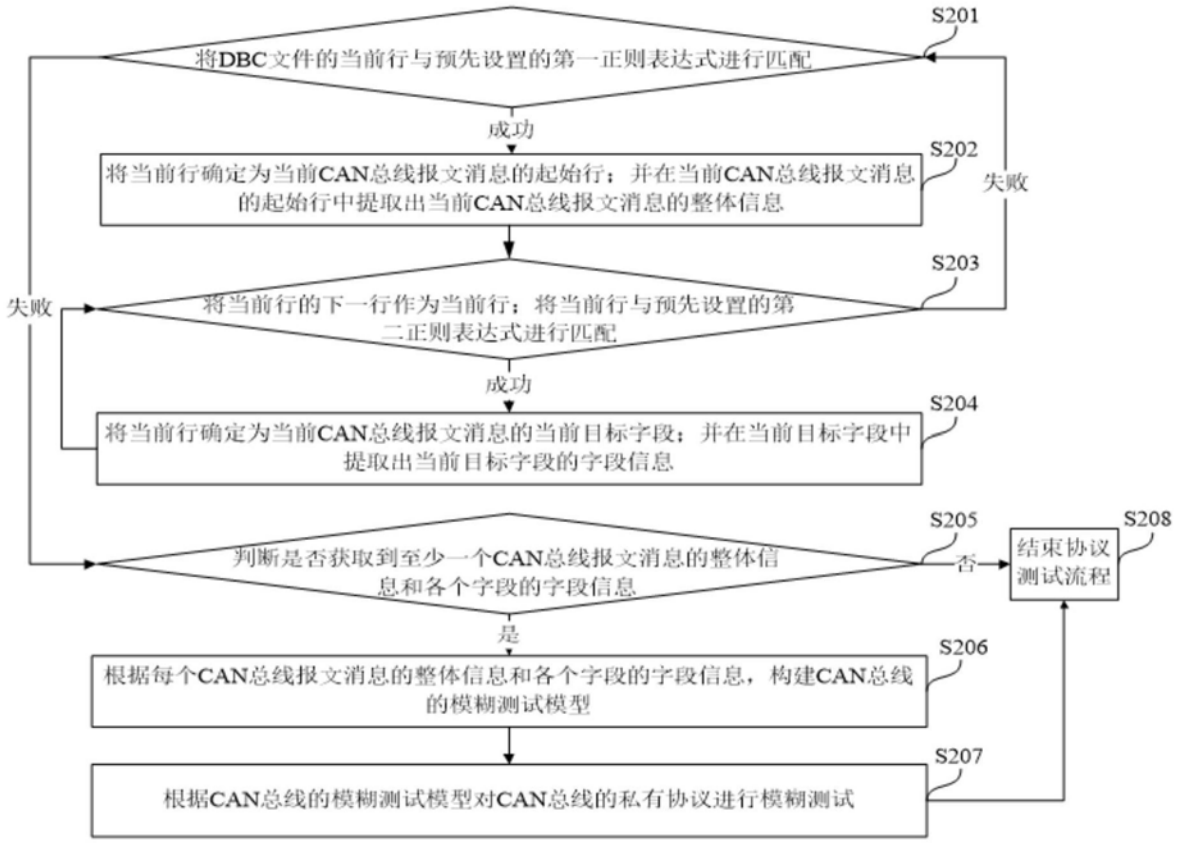

S201
将DBC文件的当前行与预先设置的第一正则表达式进行匹配
成功
失败
S202
将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息
S203
将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配
失败
成功
S204
将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息
S205
判断是否获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息
否
S208
结束协议测试流程
是
S206
根据每个CAN总线报文消息的整体信息和各个字段的字段信息，构建CAN总线的模糊测试模型
S207
根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试

图2

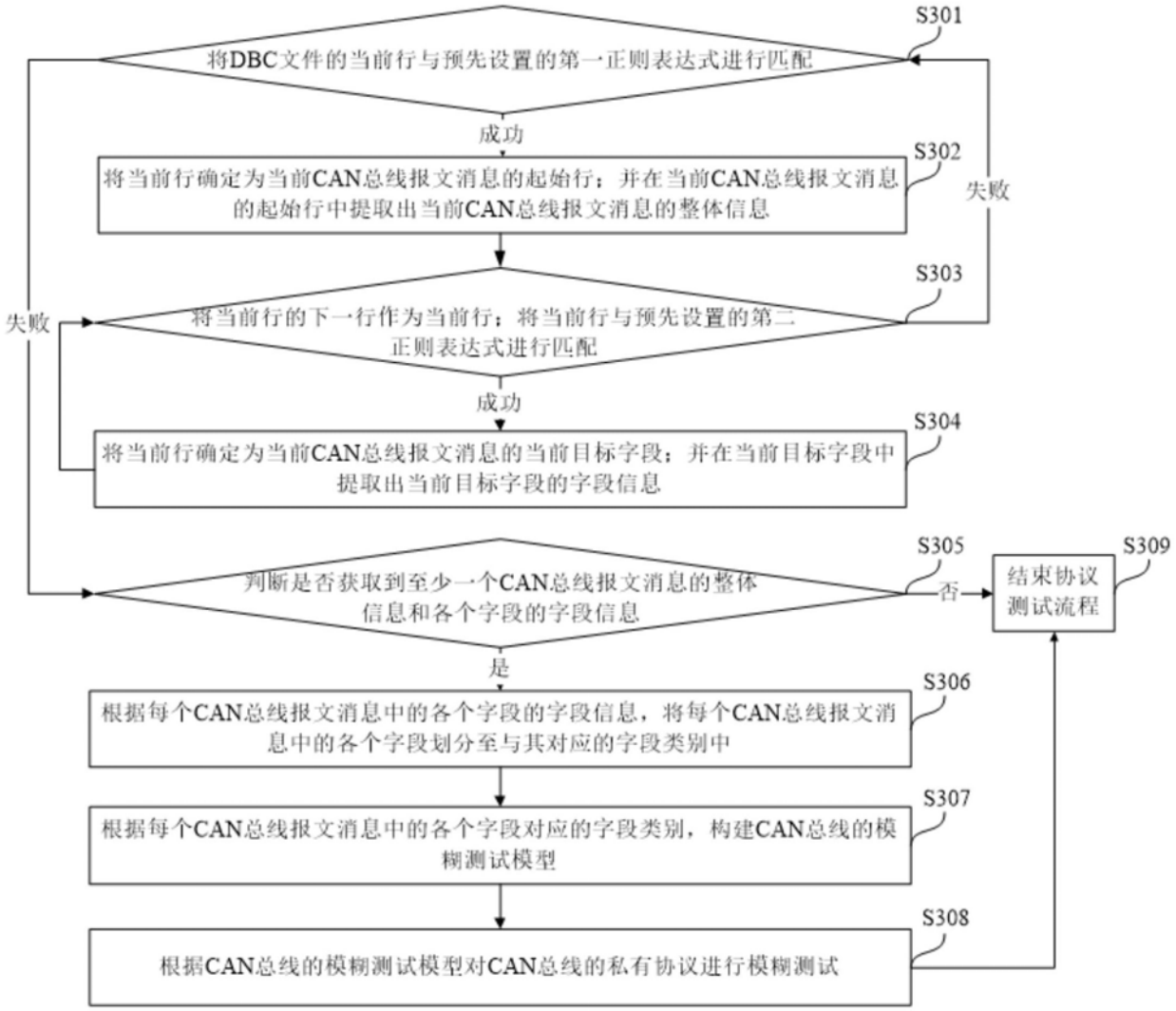

S301
将DBC文件的当前行与预先设置的第一正则表达式进行匹配
成功
失败
S302
将当前行确定为当前CAN总线报文消息的起始行；并在当前CAN总线报文消息的起始行中提取出当前CAN总线报文消息的整体信息
S303
将当前行的下一行作为当前行；将当前行与预先设置的第二正则表达式进行匹配
失败
成功
S304
将当前行确定为当前CAN总线报文消息的当前目标字段；并在当前目标字段中提取出当前目标字段的字段信息
S305
判断是否获取到至少一个CAN总线报文消息的整体信息和各个字段的字段信息
否
S309
结束协议测试流程
是
S306
根据每个CAN总线报文消息中的各个字段的字段信息，将每个CAN总线报文消息中的各个字段划分至与其对应的字段类别中
S307
根据每个CAN总线报文消息中的各个字段对应的字段类别，构建CAN总线的模糊测试模型
S308
根据CAN总线的模糊测试模型对CAN总线的私有协议进行模糊测试

图3

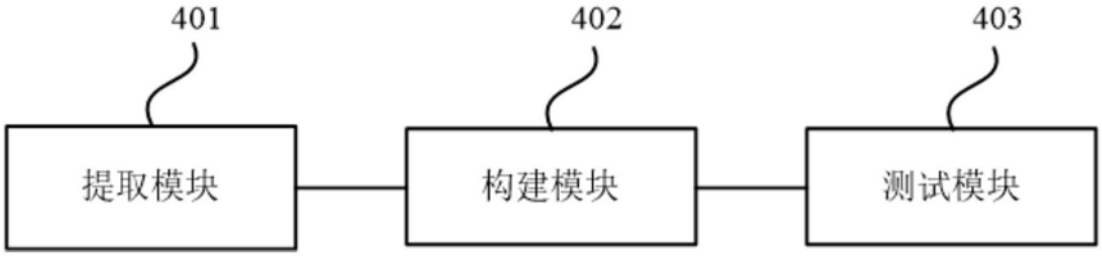

401
402
403
提取模块
构建模块
测试模块

图4

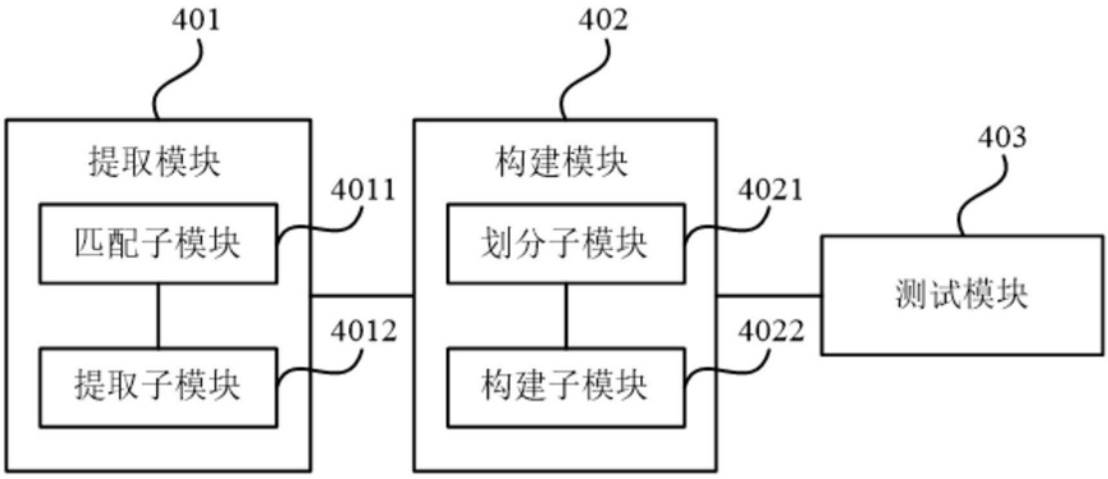

401
402
403
提取模块
构建模块
测试模块
匹配子模块
划分子模块
提取子模块
构建子模块
4011
4012
4021
4022

图5

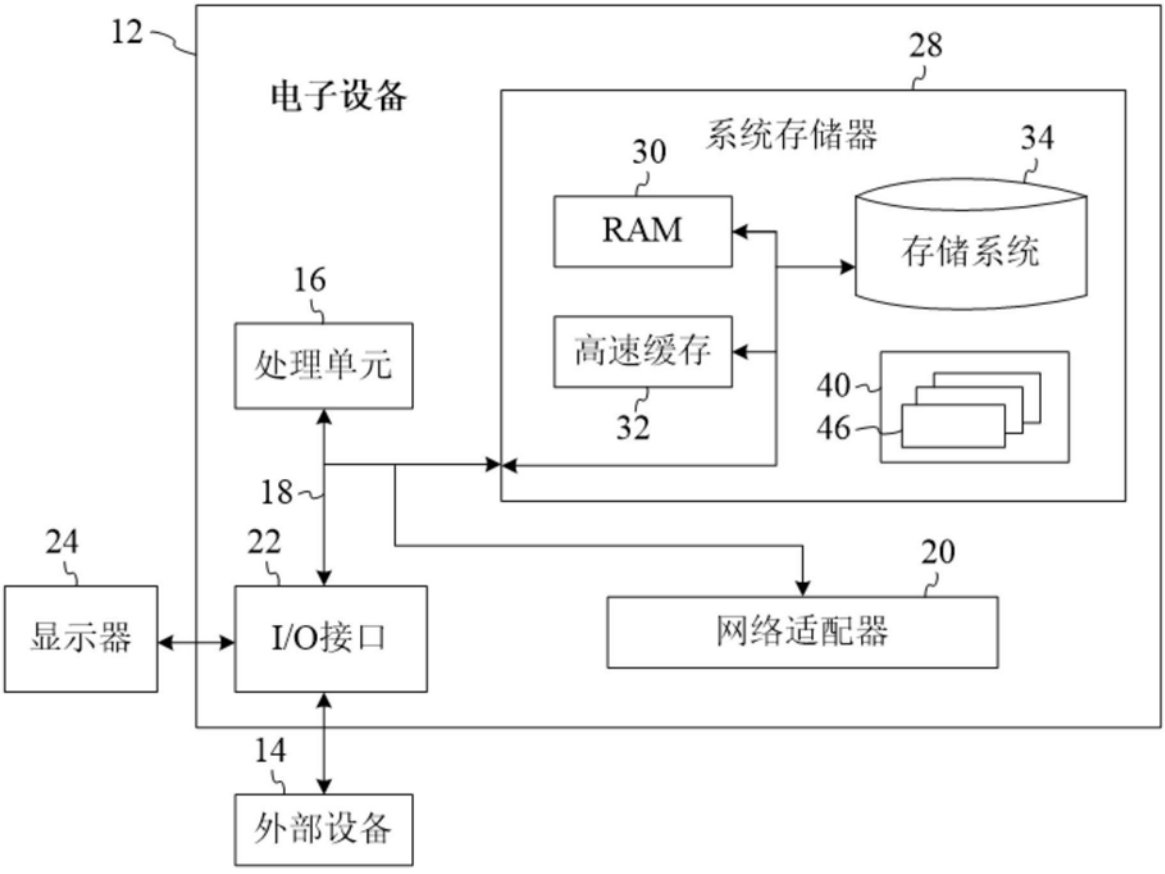

12
电子设备
28
系统存储器
30
34
RAM
存储系统
16
处理单元
高速缓存
32
40
46
18
24
22
20
显示器
I/O接口
网络适配器
14
外部设备

图6