(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 102710656 B
(45)授权公告日 2014.03.12

(21)申请号 201210199782.7
(22)申请日 2012.06.14
(73)专利权人 北京理工大学
地址 100081 北京市海淀区中关村南大街5号
(72)发明人 席军强 吴育恩 胡宇辉 陈慧岩
(74)专利代理机构 北京天达知识产权代理事务所(普通合伙) 11386
代理人 王庆海
(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/66(2006.01)

(56)对比文件
CN 101360036 A,2009.02.04,说明书第4页第5-7段、第5页第1-4段及说明书附图2、3.
CN 101431394 A,2009.05.13,说明书第7页第2段及第9页第1-2段.
US 2007/0025249 A1,2007.02.01,全文.
JP 2010-4701 A,2010.01.07,全文.

审查员 张小倩

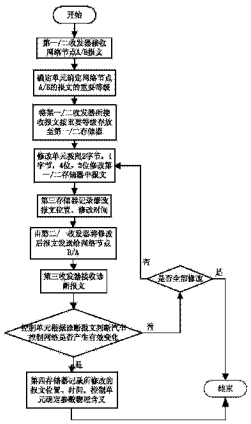
权利要求书2页 说明书6页 附图3页

(54)发明名称

基于汽车网关系统的通信协议逆向解析方法

(57)摘要

本发明公开一种基于汽车网关系统的通信协议解析方法。通过本发明技术方案,可有效解析汽车控制网络中关键的控制和状态信号,并实现各关键系统的准确控制,其增强了协议解析的准确性,提高了解析效率,节约了研究资源。



CN 102710656 B

1. 一种基于汽车网关系统的通信协议解析方法，其特征在于，所述网关系统安装在汽车控制网络的第一网络节点和第二网络节点之间，其包括第一收发器、第二收发器、第三收发器、微控制单元、第一存储器、第二存储器、第三存储器和第四存储器，其中，所述方法包括：

第一步骤，所述第一收发器接收由所述第一网络节点发送并应由所述第二网络节点接收的报文，所述第二收发器接收由所述第二网络节点发送并应由所述第一网络节点接收的报文；

第二步骤，所述微控制单元分别确定所述第一收发器和所述第二收发器所接收的报文的重要等级；

第三步骤，所述微控制单元将所述第一收发器和所述第二收发器的报文按重要等级由高到低的顺序分别对应存放至所述第一存储器和所述第二存储器中；

第四步骤，所述微控制单元按照预定顺序依次修改所述第一存储器和所述第二存储器中各报文数据场中各个字节的值；

第五步骤，所述第三存储器记录在所述第四步骤中所修改的报文、相应修改时间以及该报文所在的数据场位置；

第六步骤，所述第二收发器将所述第一存储器中修改后的报文发送给所述第二网络节点，所述第一收发器将所述第二存储器中修改后的报文发送给所述第一网络节点；

第七步骤，所述第三收发器接收车载诊断系统的诊断信号报文；

第八步骤，所述微控制单元判断相应网络节点接收到修改了字节的报文之后，汽车控制网络是否产生了有效变化；以及

第九步骤，当所述微控制单元判断出相应网络节点接收到修改了字节的报文之后，所述汽车控制网络产生了有效变化时，所述第四存储器记录该被修改的报文、相应修改时间以及该报文所在的数据场位置，所述微控制单元确定该修改字节的具体物理意义，从而实现对协议的解析；

第十步骤，当所述微控制单元判断出相应网络节点接收到修改了字节的报文之后，汽车控制网络并未产生有效变化时，判断报文中字节是否已全部被修改，如果已被全部修改，则结束该方法流程，如果并未全部修改，返回所述第四步骤对尚未修改的报文内容进行修改，

所述微控制单元进一步包括确定单元、修改单元和控制单元，其中，

在所述第二步骤中，所述确定单元根据报文的优先级和刷新率分别确定所述第一收发器和所述第二收发器所接收的报文的重要等级，且在所述第三步骤中，所述确定单元将所述第一收发器和所述第二收发器接收的报文按重要等级由高到低的顺序分别对应存放至所述第一存储器和所述第二存储器中；

在所述第四步骤中，所述修改单元以双字节、单字节、4 位、2 位的顺序依次修改所述第一存储器和所述第二存储器中各报文数据场中各个字节的值；以及

在所述第八步骤中，所述控制单元根据所述第三收发器从所述车载诊断系统接收到的诊断信号报文来判断相应网络节点接收到修改后的报文之后，所述汽车控制网络是否产生有效变化，从而确定所修改字节的物理意义。

2. 根据权利要求 1 所述的方法，其特征在于，所述汽车控制网络是基于总线技术的网

络，所述总线是 CAN 总线、RS485 总线、FlexRay 总线或 Lin 总线。

3. 根据权利要求 1 所述的方法，其特征在于，在完成对通信协议的解析后，通过所述网关系统手动修改控制信号中的关键参数值，观察系统是否产生预期的变化，从而验证所述网关系统解析出的结果是否正确。

4. 根据权利要求 1-3 中任意一项所述的方法，其特征在于，所述第一网络节点或第二网络节点是单一汽车控制节点或包含一个或多个汽车控制节点的网络功能模块，所述汽车控制节点选自下面的组：发动机控制器、变速箱控制器、制动控制器、整车控制模块、自动离合器控制器、电机控制器、电源控制器和车载诊断系统。

基于汽车网关系统的通信协议逆向解析方法

技术领域

[0001] 本发明涉及汽车控制领域，尤其涉及一种基于汽车网关系统的通信协议逆向解析方法。

背景技术

[0002] 总线技术在国内汽车市场的应用越来越多，随着行业成本的逐年降低，各类开发工具和解决方案逐步渗透，单纯的技术应用层面已经没有问题。国内在网络开发方面与国外的差距主要是通信协议的制定与测试。国外的总线网络设计已经进行了二十多年，各公司成熟的网络通信协议都是通过多年积累得到的，很多已形成了具有自身特色的网络开发协议。国内厂商要发展自主网络通信协议，对国外的网络通信协议进行逆向解析、吸收并改进，不失为一条快速提高国内研究水平的捷径。

[0003] 国内多家厂商已开始进行汽车通信协议的解析工作，但目前并没有形成一套有效可行的总线通信协议的解析技术，较多地采用设计特殊工况试验并采集大量数据的方式，在数据处理时，则通过试凑法获取网络通信协议，这样工作效率低且会耗费大量资源。

发明内容

[0004] 本发明的目的在于提供一种用于对汽车系统控制网络中的通信协议进行逆向解析的技术，增强协议解析的准确性，提高解析效率，节约研究资源。

[0005] 根据本发明的一个方面，提供一种基于汽车网关系统的通信协议解析方法，所述网关系统安装在汽车控制网络的第一网络节点和第二网络节点之间，其包括第一收发器、第二收发器、第三收发器、微控制单元、第一存储器、第二存储器、第三存储器和第四存储器，其中，所述方法包括：

[0006] 第一步骤，所述第一收发器接收由所述第一网络节点发送并应由所述第二网络节点接收的报文，所述第二收发器接收由所述第二网络节点发送并应由所述第一网络节点接收的报文；

[0007] 第二步骤，所述微控制单元分别确定所述第一收发器和所述第二收发器所接收的报文的重要等级；

[0008] 第三步骤，所述微控制单元将所述第一收发器和所述第二收发器的报文按重要等级由高到低的顺序分别对应存放至所述第一存储器和所述第二存储器中；

[0009] 第四步骤，所述微控制单元按照预定顺序依次修改所述第一存储器和所述第二存储器中各报文数据场中各个字节的值；

[0010] 第五步骤，所述第三存储器记录在所述第四步骤中所修改的报文、相应修改时间以及该报文所在的数据场位置；

[0011] 第六步骤，所述第二收发器将所述第一存储器中修改后的报文发送给所述第二网络节点，所述第一收发器将所述第二存储器中修改后的报文发送给所述第一网络节点；

[0012] 第七步骤，所述第三收发器接收车载诊断系统的诊断信号报文；

[0013] 第八步骤，所述微控制单元判断相应网络节点接收到修改了字节的报文之后，汽车控制网络是否产生了有效变化；以及

[0014] 第九步骤，当所述微控制单元判断出相应网络节点接收到修改了字节的报文之后，所述汽车控制网络产生了有效变化时，所述第四存储器记录该被修改的报文、相应修改时间以及该报文所在的数据场位置，所述微控制单元确定该修改字节的具体物理意义，从而实现对协议的解析；

[0015] 第十步骤，当所述微控制单元判断出相应网络节点接收到修改了字节的报文之后，汽车控制网络并未产生有效变化时，判断报文中字节是否已全部被修改，如果已被全部修改，则结束该方法流程，如果并未全部修改，返回所述第四步骤对尚未修改的报文内容进行修改，

[0016] 所述微控制单元进一步包括确定单元、修改单元和控制单元，其中，

[0017] 在所述第二步骤中，所述确定单元根据报文的优先级和刷新率分别确定所述第一收发器和所述第二收发器所接收的报文的重要等级，且在所述第三步骤中，所述确定单元将所述第一收发器和所述第二收发器接收的报文按重要等级由高到低的顺序分别对应存放至所述第一存储器和所述第二存储器中；

[0018] 在所述第四步骤中，所述修改单元以双字节、单字节、4 位、2 位的顺序依次修改所述第一存储器和所述第二存储器中各报文数据场中各个字节的值；以及在所述第八步骤中，所述控制单元根据所述第三收发器从所述车载诊断系统接收到的诊断信号报文来判断相应网络节点接收到修改后的报文之后，所述汽车控制网络是否产生有效变化，从而确定所修改字节的物理意义。

[0019] 优选地，所述汽车控制网络是基于总线技术的网络，所述总线是 CAN 总线、RS485 总线、FlexRay 总线或 Lin 总线。

[0020] 优选地，在完成对通信协议的解析后，通过所述网关系统手动修改控制信号中的关键参数值，观察系统是否产生预期的变化，从而验证所述网关系统解析出的结果是否正确。

[0021] 优选地，所述第一网络节点或第二网络节点是单一汽车控制节点或包含一个或多个汽车控制节点的网络功能模块，所述汽车控制节点选自下面的组：发动机控制器、变速箱控制器、制动控制器、整车控制模块、自动离合器控制器、电机控制器、电源控制器和车载诊断系统。

[0022] 通过上述技术方案，本发明可有效解析汽车控制网络中关键的控制和状态信号，并实现各关键系统的准确控制，其增强了协议解析的准确性，提高了解析效率，节约了研究资源。

附图说明

[0023] 图 1 是本发明中网关系统的应用场景示意图；

[0024] 图 2 是本发明中网关系统的系统结构示意图；

[0025] 图 3 是本发明中网关系统的微控制单元的结构示意图；

[0026] 图 4 是本发明的通信协议解析方法的步骤流程图；

[0027] 图 5 是本发明实施例中设置网关系统之前的汽车控制网络的拓扑图；

[0028] 图 6 是本发明实施例中设置网关系统之后的汽车控制网络的拓扑图。

具体实施方式

[0029] 为解决现有技术中的上述技术问题，本发明公开了一种基于汽车网关系统的通信协议解析方法，该方法可以接收汽车控制网络中某控制节点的报文信号(真实信号)，对其信号值进行处理，并将处理后的报文信号(虚拟信号)发送给其他控制节点，这样可有效解析汽车控制网络中关键的控制和状态信号，并实现各关键系统的准确控制。

[0030] 图 1 是本发明中网关系统的应用场景示意图。本发明中的网关系统在实际应用时可串联接入在汽车控制网络中的网络节点 A 和网络节点 B 之间，由该网关系统实现该汽车控制网络中网络节点 A 和网络节点 B 之间所传输的控制信号的通信协议解析方法。需要指出的是，在本发明网关系统的应用场景中，网络节点 A 或网络节点 B 均代表可实现控制信号收发的网络单元，可为汽车中具体的单一网络控制节点，也可以是包含一个或多个网络控制节点的网络功能模块。

[0031] 本发明的通信协议解析方法的基本原理是基于具有在线学习功能的优化匹配法。具体地，该优化匹配法可利用类似于穷举法的方式对根据某通信协议传输的大量报文进行字节甚至是位一级的分析，确定报文中有效内容所代表的物理意义，从而实现对通信协议的解析。其间，该方法还通过自我学习机制不断优化处理方式，以提高解析效率。

[0032] 图 2 是本发明中网关系统的系统结构示意图。如图 2 所示，该网关系统包括 :第一收发器、第二收发器、第三收发器、微控制单元、第一存储器、第二存储器、第三存储器和第四存储器。下面就进一步介绍网关系统中的各模块的功能及其原理。

[0033] 第一收发器，其连接汽车控制网络中的某网络节点 A 和该网关系统的微控制单元，用于接收由网络节点 A 发送并应由汽车控制网络中的另一网络节点 B 接收的所有通信报文(后简称“报文”)，还用于将由微控制单元处理过的报文发送到网络节点 A。

[0034] 第二收发器，其连接汽车中的网络节点 B 和该网关系统的微控制单元，用于接收由网络节点 B 发送并应由网络节点 A 接收的所有通信报文，还用于将由微控制单元处理过的报文发送到网络节点 B。

[0035] 第三收发器，其连接汽车的车载诊断系统和该网关系统的微控制单元，用于接收该车载诊断系统的诊断信号报文。

[0036] 微控制单元，用于对报文进行一系列处理，并实现对通信协议的解析。具体地，图 3 示出了微控制单元的结构示意图，该微控制单元进一步包括确定单元、修改单元和控制单元。

[0037] 确定单元，用于分别确定第一收发器和第二收发器所接收的报文的重要等级，并将第一收发器和第二收发器的报文按重要等级由高到低的顺序分别对应存放至第一存储器和第二存储器中。其中，该重要等级可由报文的优先级和刷新率共同确定，具体例如可将两者相乘，所得结果越小，重要等级越高。

[0038] 需要说明的是，确定单元根据重要等级对报文进行排序的目的实际上是为了提高协议解析的效率。因为，重要等级高的报文中包含重要信号的概率更高，通过对它们的分析更容易获取用于解析协议的信息，因而将它们进行优先处理会提高协议解析的整体效率。优先级和刷新率是代表报文重要等级的两个重要参数。其中，优先级是报文仲裁场中的字

节数据，通常可以以报文的 ID 表示报文的优先级，在 CAN 总线协议中报文通过非破坏性逐位仲裁机制确定各报文的发送顺序，0 是显性 1 是隐性，因此报文的 ID 越小，报文的优先级越高(逐位比较)。同时，报文的刷新率即为该报文连续两次出现的时间间隔，因此报文的刷新率高显然也体现了其重要程度高。例如，报文 a 的 ID 虽然比报文 b 小，但报文 a 的刷新率为 1000ms，报文 b 的刷新率为 10ms，因此报文 b 的重要程度可能优于报文 a。因此在本发明中，综合考虑报文的优先级和刷新率两个参数，由它们共同确定报文的重要等级。

[0039] 修改单元，用于按照预定顺序依次修改第一存储器和第二存储器中各报文数据场中各个字节的值。在汽车生产厂商制定通信协议的时候，可能会在报文中包含不同长度字节或位的数据参数，该长度可在报文信号解析开始前通过自学习机制来确定，而在确定该参数的长度之后，就可依据该结果(先验知识)来确定修改报文所依据的顺序。在本发明具体实施例中，根据先验知识，修改单元可以双字节、单字节、4 位、2 位的顺序对第一、第二存储器中各报文数据场中各个字节的值进行依次修改。需要说明的是，本发明中的该数据场是指各参数在报文中所在的位置，例如，每帧 CAN 报文有 8 字节的数据场。

[0040] 控制单元，用于控制第一收发器、第二收发器将由修改单元修改后的报文发送到对应的网络节点，并根据第三收发器从车载诊断系统接收到的诊断信号报文，判断相应网络节点接收到修改了字节的报文之后，汽车控制网络是否产生了有效变化，并根据判断结果确定该字节的具体物理意义。

[0041] 上述修改单元对报文数据场中字节的值进行改变实际上是在改变汽车控制网络中所传输的控制信号。某控制信号会使得所控制的网络节点产生相应的动作，当控制信号被修改单元修改后，相应动作也可能产生变化，就可以根据相应动作的变化来判断出所修改字节的物理意义，从而实现对协议的解析，这也体现了本发明进行协议解析的基本原理。

[0042] 第一存储器，用于按重要等级由高到低的顺序存储由第一收发器接收并由确定单元确定顺序的各报文。

[0043] 第二存储器，用于按重要等级由高到低的顺序存储由第二收发器接收并由确定单元确定顺序的各报文。

[0044] 第三存储器，用于记录该修改单元所修改的报文、相应修改时间以及该报文所在的数据场位置。

[0045] 第四存储器，当控制单元判断出相应网络节点接收到修改了字节的报文之后，汽车控制系统产生了有效变化时，用于记录该被修改的报文、相应修改时间以及该报文所在的数据场位置。

[0046] 当然，本发明中的网关系统还可包括一电源模块，从而为该网关系统提供电力供应。

[0047] 图 4 是本发明的通信协议解析方法的步骤流程图。下面接结合附图 4 来说明通信协议解析方法中的各步骤。

[0048] 步骤 1：网关系统中的第一收发器接收由网络节点 A 发送并应由网络节点 B 接收的报文，同时网关系统中的第二收发器接收由网络节点 B 发送并应由网络节点 A 接收的报文。

[0049] 步骤 2：微控制单元中的确定单元分别确定第一收发器和第二收发器所接收的报文的重要等级。其中，该重要等级可由报文的优先级和刷新率共同确定，具体例如可将两者

相乘，所得结果越小，重要等级越高。

[0050] 步骤 3：确定单元将第一收发器和第二收发器的报文按重要等级由高到低的顺序分别对应存放至第一存储器和第二存储器中。

[0051] 步骤 4：微控制单元中的修改单元按照预定顺序依次修改第一存储器和第二存储器中各报文数据场中各个字节的值。具体地，修改单元可以双字节、单字节、4 位、2 位的顺序对第一、第二存储器中各报文数据场中各个字节的值进行依次修改。

[0052] 步骤 5：第三存储器记录该修改单元在步骤 4 中所修改的报文、相应修改时间以及该报文所在的数据场位置。

[0053] 步骤 6：第二收发器将第一存储器中修改后的报文发送给网络节点 B，同时第一收发器将第二存储器中修改后的报文发送给网络节点 A。

[0054] 步骤 7：第三收发器接收车载诊断系统的诊断信号报文。

[0055] 步骤 8：控制单元根据第三收发器从车载诊断系统接收到的诊断信号报文，判断相应网络节点接收到修改了字节的报文之后，汽车控制网络是否产生了有效变化。

[0056] 步骤 9：当判断出相应网络节点接收到修改了字节的报文之后，汽车控制网络产生了有效变化时，第四存储器记录该被修改的报文、相应修改时间以及该报文所在的数据场位置。同时，控制单元确定该修改字节的具体物理意义，从而实现对协议的解析。

[0057] 步骤 10：当判断出相应网络节点接收到修改了字节的报文之后，汽车控制系统并未产生有效变化时，判断报文中字节是否已全部被修改，如果已被全部修改，则结束协议解析流程，如果并未全部修改，返回步骤 4 对尚未修改的报文内容进行修改。

[0058] 本发明通信协议解析方法的上述流程可以完成对通信协议的自动解析。此外，当该自动解析完成后，即获得了控制网络的报文信号中有效的控制状态信号后，还可以通过网关系统手动修改控制信号中的关键参数值，观察系统是否产生预期的变化，从而确定网关系统自动解析出的结果是否正确，即通过手工操作对网关系统的自动操作进行验证。作为本发明进一步的功能，在最终完成通信协议解析从而获得报文信号中有效的控制信号后，还可以对该信号进行修改，从而实现对各关键部件的有效控制。

[0059] 实施例

[0060] 图 5、6 分别是本发明实施例中设置网关系统前后的汽车控制网络的拓扑图。下面就参考图 5、6，以解析汽车控制网络中离合器分离 / 接合的控制命令为目标，对本发明的实施例进行详细说明。

[0061] 如图 5 所示，某未知汽车控制网络的总线拓扑结构包括两条 CAN 总线，其中一条 CAN 总线涉及的网络节点包括：发动机控制器、变速箱控制器、制动控制器和整车控制模块，CAN 总线的传输速率为 250Kbit/s，将其命名为 CAN250，如图 5、6 中细实线所示；另外一条 CAN 总线涉及的网络节点包括：自动离合器控制器、电机控制器，电源控制器和整车控制模块，CAN 总线的传输速率为 500Kbit/s，将其命名为 CAN500，如图 5 中粗实线所示。整车控制模块为汽车控制系统的控制核心，其通过上述两条 CAN 总线构成的网络下达各种控制指令给各部件，接收各部件所上传的信号，并作为网络的中心连接点来实现两条总线上数据的交互。此外，该汽车控制系统中还包含一条基于 RS485 总线的 J1587 通信网络，如图 5 中虚线所示，该总线用于传输和记录车载诊断系统产生的车载诊断信息。

[0062] 如图 6 所示，在整车控制模块与自动离合器控制器之间串联接入本发明中的网关

系统，其对整车控制模块与自动离合器控制器之间的报文通讯进行物理屏蔽以实现通信协议的解析。图 2 中的第一收发器用于接收整车控制模块发送给自动离合器控制器的报文信号，第二收发器用于接收自动离合器控制器发送给整车控制模块的报文信号，第三收发器用于接收车载诊断系统通过诊断接口发出的车载诊断信息报文。

[0063] 总线上电后，第一、第二收发器分别接收整车控制模块和自动离合器控制器之间的通讯信号，并由确定单元按重要等级由高到低分别存放至第一存储器和第二存储器中。由先验知识可知，离合器分离 / 接合的控制命令应该由整车控制模块发送给自动离合器控制器，因此在本实施例中修改单元可以仅针对第一存储器中的报文进行数据场值的修改。具体地，修改单元按照双字节、单字节、4 位、2 位的顺序依次修改第一存储器中各报文数据场中各个字节的值，由第二收发器发送给自动离合器控制器，并由第三存储器依次记录被修改报文、修改时间、修改的字节位置等。同时，控制单元根据第三收发器自诊断接口接收的诊断信号报文，判断修改字节后自动离合器是否产生了分离或接合的状态改变，并且也可以人为地依靠声音判断离合器是否有动作来辅助解析。当判断修改字节后自动离合器产生了状态改变，第四存储器存储记录该被修改的报文、相应修改时间以及该报文所在的数据场位置。同时，控制单元确定该修改字节的具体物理意义，从而实现对自动离合器控制器的控制信号的协议解析。

[0064] 在实现对自动离合器控制器的控制信号的协议解析后，还可以进一步实现对该自动离合器控制器的有效控制。例如，当整车控制模块发送给自动离合器控制器的控制信号是使自动离合器进行分离操作的，在解析了相应协议后就可以通过网关系统将该控制信号修改为进行接合操作的信号之后再转发给自动离合器控制器。

[0065] 本领域技术人员应该理解，虽然本实施例具体应用 CAN 总线系统，但本发明也可以使用 FlexRay，Lin 等总线系统实现。

[0066] 通过上述技术方案，本发明可有效解析汽车控制网络中关键的控制和状态信号，并实现各关键系统的准确控制，其增强了协议解析的准确性，提高了解析效率，节约了研究资源。

[0067] 本发明包括但不限于以上的实施例，凡是在本发明的精神和原则之下进行的任何局部改进，等同替换都将视为在本发明的保护范围之内。

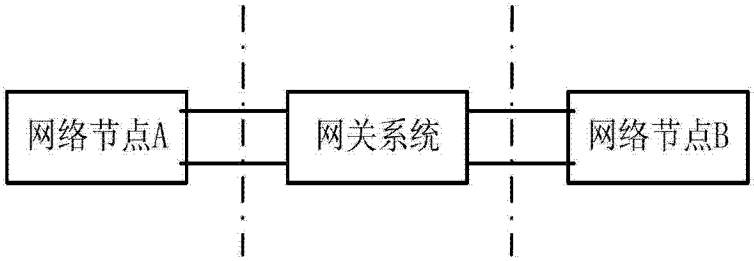

网络节点A
网关系统
网络节点B

图 1

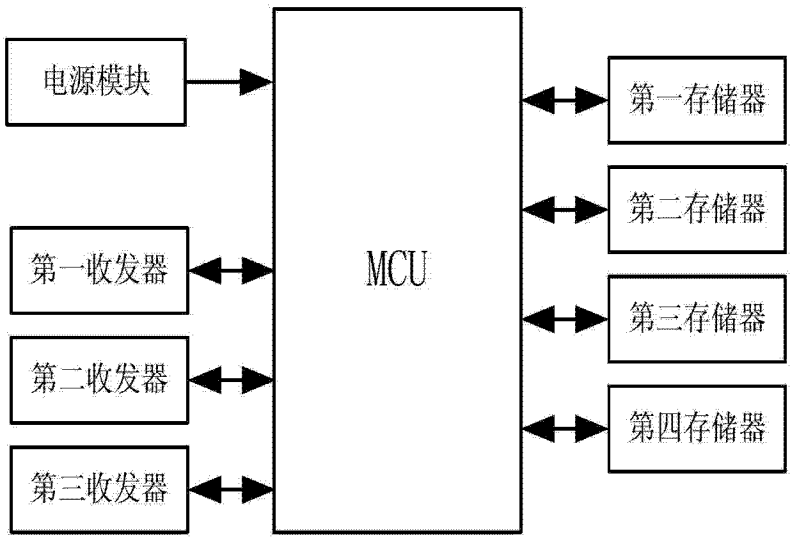

电源模块
第一收发器
第二收发器
第三收发器
MCU
第一存储器
第二存储器
第三存储器
第四存储器

图 2

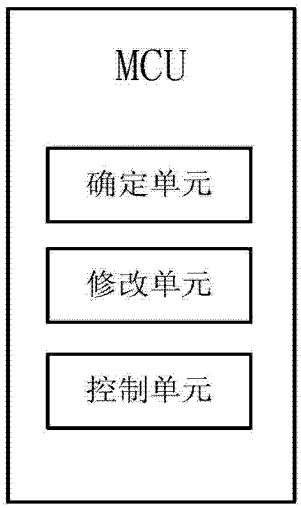

MCU
确定单元
修改单元
控制单元

图 3

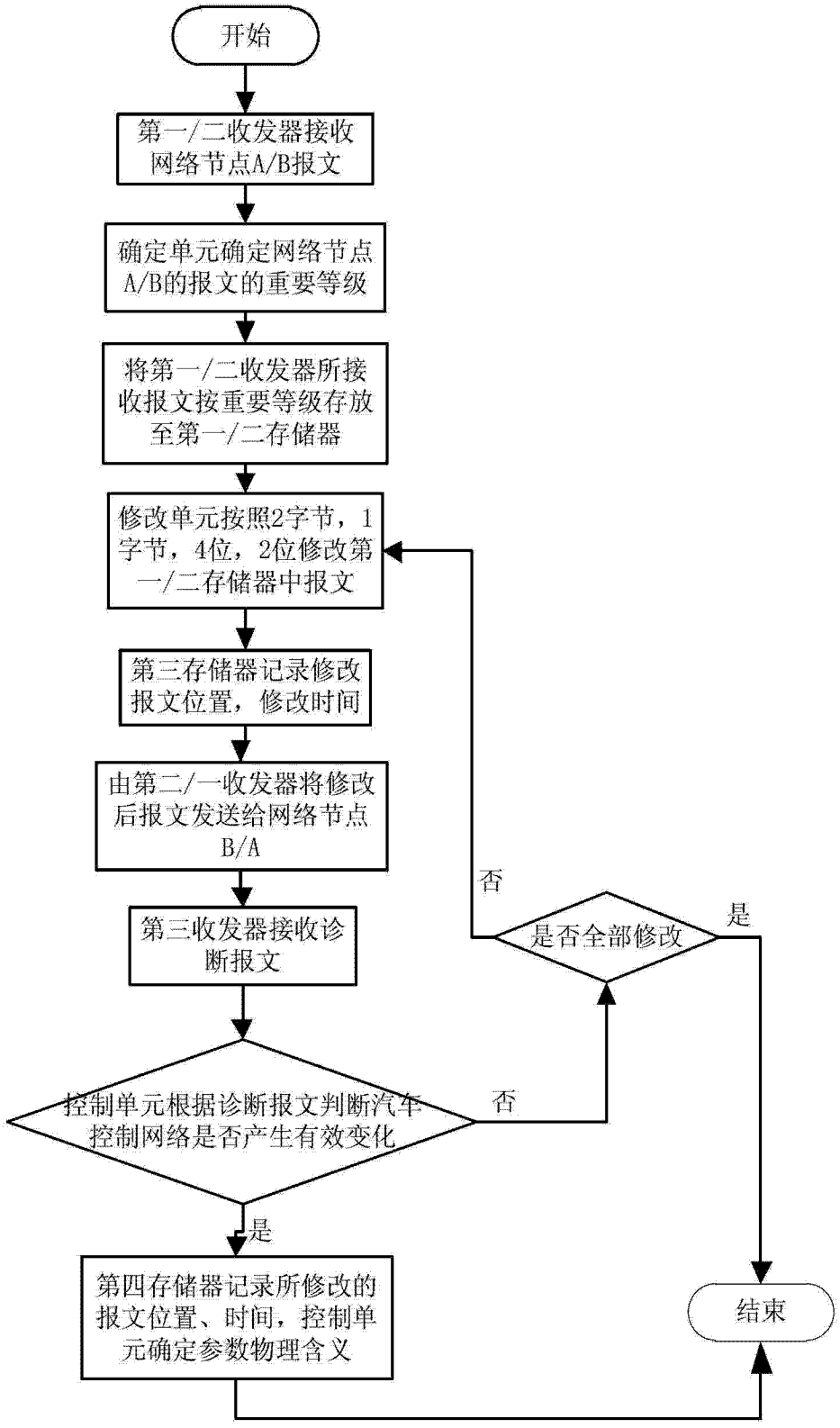

开始
第一/二收发器接收网络节点A/B报文
确定单元确定网络节点A/B的报文的重要等级
将第一/二收发器所接收报文按重要等级存放至第一/二存储器
修改单元按照2字节，1字节，4位，2位修改第一/二存储器中报文
第三存储器记录修改报文位置，修改时间
由第二/一收发器将修改后报文发送给网络节点B/A
第三收发器接收诊断报文
控制单元根据诊断报文判断汽车控制网络是否产生有效变化
否
是
第四存储器记录所修改的报文位置、时间，控制单元确定参数物理含义
是否全部修改
否
是
结束

图 4

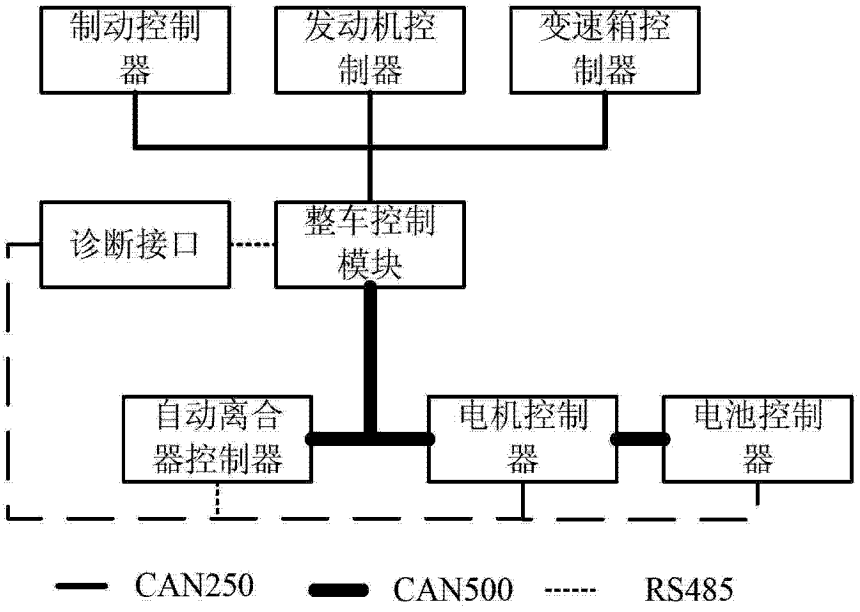

制动控制器
发动机控制器
变速箱控制器
诊断接口
整车控制模块
自动离合器控制器
电机控制器
电池控制器
CAN250
CAN500
RS485

图 5

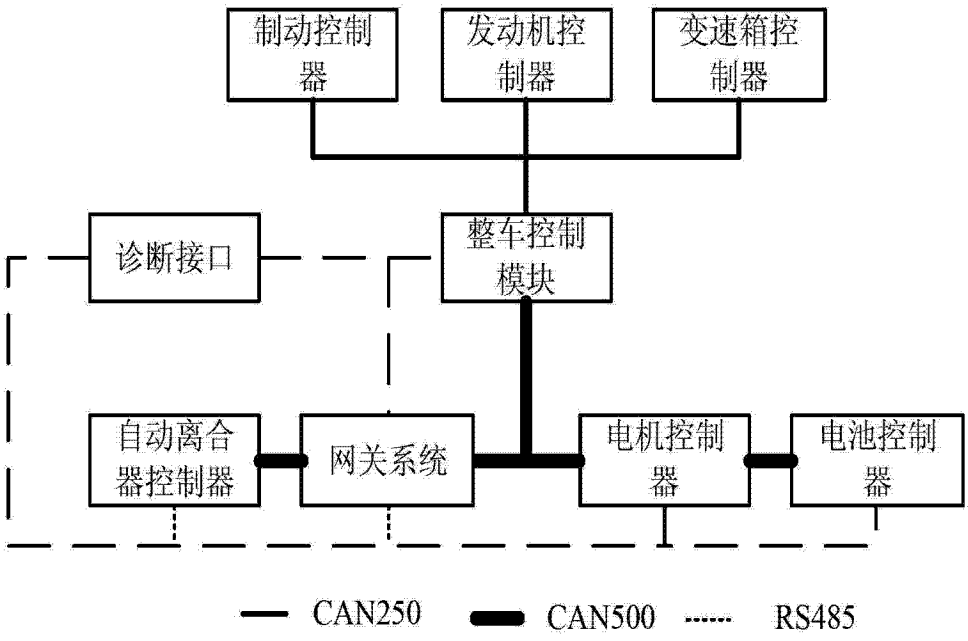

制动控制器
发动机控制器
变速箱控制器
诊断接口
整车控制模块
自动离合器控制器
网关系统
电机控制器
电池控制器
CAN250
CAN500
RS485

图 6