(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 112684773 A
(43)申请公布日 2021.04.20

(21)申请号 202011083912.1

(22)申请日 2020.10.12

(30)优先权数据
19203744.8 2019.10.17 EP

(71)申请人 沃尔沃汽车公司
地址 瑞典哥德堡

(72)发明人 A·安东松

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜

(51)Int.Cl.
G05B 23/02(2006.01)

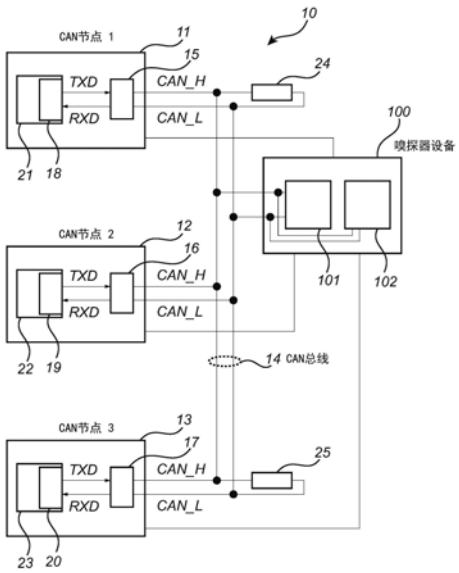
权利要求书2页 说明书15页 附图16页

(54)发明名称

在CAN总线上的数据操纵检测

(57)摘要

本公开涉及一种检测在控制器局域网(CAN)总线上的数据操纵的方法以及执行该方法的设备。在一方面,提供了一种检测在设备连接到的CAN总线(14)上的数据操纵的设备(100、150)的方法。该方法包括检测(S101、S202)总线阻抗低于阈值总线阻抗值;在检测到总线阻抗低于阈值总线阻抗值时,检测(S102、S201)当前在CAN总线(14)上是否可能发生CAN节点仲裁;以及如果未发生,则确定(S103、S203)在CAN总线(14)上已经发生了操纵数据的企图。



CN 112684773 A

1.一种检测在控制器局域网CAN总线(14)上的数据操纵的设备(100、150)的方法,所述设备连接到所述CAN总线(14),所述方法包括:

检测(S101、S202)总线阻抗低于阈值总线阻抗值;

在检测到所述总线阻抗低于所述阈值总线阻抗值时,检测(S102、S201)当前在所述CAN总线(14)上是否可能发生CAN节点仲裁;以及如果未发生;

确定(S103、S203)在所述CAN总线(14)上已经发生了操纵数据的企图。

2.根据权利要求1所述的方法,还包括:

在确定所述CAN总线(14)上已经发生了操纵数据的企图之后,丢弃通过所述CAN总线(14)接收的至少一个当前数据帧。

3.根据权利要求2所述的方法,其中,丢弃所述至少一个当前数据帧包括:

用零覆写所述至少一个当前数据帧的其余部分,或者覆写所述数据帧的被检测为被操纵的第一个比特之后的至少六个相继比特;以及

向所述数据帧旨在到达的CAN协议控制器(180)传递被覆写的所述至少一个当前数据帧。

4.根据权利要求1所述的方法,还包括:

向所述数据帧旨在到达的CAN协议控制器(180)传递已确定被操纵的至少一个当前数据帧。

5.根据前述权利要求的任一项所述的方法,其中,检测当前在所述CAN总线(14)上是否可能发生CAN节点仲裁包括:

在所述CAN总线(14)上检测帧开始SOF比特的出现,其中,在紧随所述SOF比特的预定数量的比特期间,检测到能够发生仲裁。

6.根据前述权利要求的任一项所述的方法,其中,检测(S102、S201)当前是否可能发生节点仲裁还包括:

检测(S102、S201)当前在所述总线(14)上是否发生数据帧确认。

7.根据前述权利要求的任一项所述的方法,所述阈值总线阻抗值为10Ω。

8.一种设备(100、150),所述设备被配置为检测在所述设备连接到的差分电压总线(14)上的数据操纵,所述设备(100、150)包括处理单元(200)和存储器(210),所述存储器包含能够由所述处理单元(200)执行的指令(220),由此所述设备(100、150)用于:

检测总线阻抗低于阈值总线阻抗值;

在检测到所述总线阻抗低于所述阈值总线阻抗值时,检测当前在所述总线(14)上是否可能发生节点仲裁;并且如果未发生;

确定在所述总线(14)上已经发生了操纵数据的企图。

9.根据权利要求8所述的设备(100、150),还被配置为:

在确定所述CAN总线(14)上已经发生了操纵数据的企图之后,丢弃通过所述CAN总线(14)接收的至少一个当前数据帧。

10.根据权利要求9所述的设备(100、150),在丢弃所述至少一个当前数据帧时进一步用于:

用零覆写所述至少一个当前数据帧的其余部分,或者覆写所述数据帧的被检测为被操纵的第一个比特之后的至少六个相继比特;并且

向所述数据帧旨在到达的CAN协议控制器(180)传递被覆写的所述至少一个当前数据帧。

11.根据权利要求8所述的设备(100、150),进一步用于:

向所述数据帧旨在到达的CAN协议控制器(180)传递已确定被操纵的至少一个当前数据帧。

12.根据权利要求8-11的任一项所述的设备(100、150),进一步用于在检测当前在所述CAN总线(14)上是否可能发生CAN节点仲裁时:

在所述CAN总线(14)上检测帧开始SOF比特的出现,其中,在紧随所述SOF比特的预定数量的比特期间,检测到能够发生仲裁。

13.根据权利要求8-12的任一项所述的设备(100、150),进一步用于在检测当前是否可能发生节点仲裁时进一步:

检测当前在所述总线(14)上是否发生数据帧确认。

14.根据权利要求8-13的任一项所述的设备(100、150),所述阈值总线阻抗值为10Ω。

15.一种包括计算机可执行指令的计算机程序(220),用于在所述设备(100、150)中包括的处理单元(200)上执行所述计算机可执行指令时,使得设备(100、150)执行根据权利要求1-7中任一项所述的方法。

16.一种包括计算机可读介质(210)的计算机程序产品,所述计算机可读介质具有在其上呈现为根据权利要求15所述的计算机程序(220)。

在CAN总线上的数据操纵检测

技术领域

[0001] 本公开涉及检测在控制器局域网(CAN)总线上的数据操纵的方法以及执行该方法的设备。

背景技术

[0002] 汽车行业很多年来一直在机动车辆中嵌入的电子控制单元(ECU)和诸如汽车、轮船、卡车等交通工具之间使用基于消息的通信协议。此类协议的示例是控制器局域网(CAN)。该协议由国际标准组织(ISO)标准化。例如,汽车中使用的CAN协议由ISO标准ISO 11898定义,该标准由针对不同部分的若干子规范构成;例如,CAN数据链路层由ISO 11898-1:2016定义,并且CAN高速物理层由ISO 11898-2:2017定义。ISO还定义了也用于机动车辆的其他CAN协议。

[0003] 近年来变得越来越相关的一方面是车载网络(IVN)安全性和车辆数据完整性。有若干攻击方法诸如与威胁相关的欺骗、篡改、拒绝服务(DOS)。一些威胁是以下载到车辆的恶意软件的形式来自车辆自身内部,并且一些威胁来自能够物理访问车辆及其内部通信网络的外部攻击者。

[0004] 例如,门锁模块可能被恶意方篡改,旨在解锁恶意方无权解锁的车辆。任何这样的攻击应该被检测到并阻止。

[0005] 已知有若干方法用于减轻或防止CAN总线系统的数据链路层上的各种攻击。然而,在一些示例中,在能够物理访问CAN总线时,通过在数据链路层和物理层上执行组合攻击,可以成功规避这些方法。

发明内容

[0006] 一个目的是解决,或至少减轻技术中的这个问题,并且从而提供检测在CAN总线上的数据操纵和可能阻止数据操纵的方法。

[0007] 这是由检测在CAN总线上的数据操纵的设备的方法执行的,所述设备连接到CAN总线。该方法包括检测总线阻抗低于阈值总线阻抗值;在检测到总线阻抗低于阈值总线阻抗值时,检测当前在CAN总线上是否发生CAN节点仲裁,并且如果未发生,确定在CAN总线上操纵数据的企图已经发生。

[0008] 通常,除非本文中另外明确定义,将根据其在技术领域中的普通含义解释权利要求中使用的所有术语。除非另外明确指出,对“一/所述元件、装置、部件、模块、步骤等”的所有引用将被开放地解释为指代元件、装置、部件、模块、步骤等的至少一个实例。除非明确指出,不必一定按照公开的精确次序执行本文所公开的任何方法的步骤。

附图说明

[0009] 现在参考附图,以示例的方式描述方面和实施例,在附图中:

[0010] 图1示出了在其中可以实施实施例的形成CAN网络的三个CAN节点;

[0011] 图2示出了根据标准ISO 11898-2的用于通过总线转移的隐性数据和显性数据的CAN总线上的规定电压范围；

[0012] 图3示出了拒绝服务攻击；

[0013] 图4示出了欺骗攻击；

[0014] 图5示出了替代性欺骗攻击；

[0015] 图6示出了篡改攻击；

[0016] 图7示出了重放攻击；

[0017] 图8a和图8b示出了充当到CAN总线的接口的CAN收发器的发射器部分的示意图；

[0018] 图9a和图9b示出了攻击者设备和连接到CAN总线的CAN收发器；

[0019] 图10a示出了根据实施例的被配置为检测在设备连接到的CAN总线上的数据操纵的设备；

[0020] 图10b示出了根据实施例的检测在CAN总线上的数据操纵的方法的流程图；

[0021] 图10c示出了根据另一实施例的检测在CAN总线上的数据操纵的方法的流程图；

[0022] 图11示出了处于经典基础帧格式(CBFF)中的现有技术CAN数据帧；以及

[0023] 图12示出了根据另一实施例的被配置为检测在设备连接到的CAN总线上的数据操纵的设备；以及

[0024] 图13示出了根据实施例的设备。

具体实施方式

[0025] 现在将参考示出了本发明的特定实施例的附图在下文更全面地描述本公开的方面。

[0026] 然而，这些方面可以以许多不同形式呈现，且不应解读为限制性的；相反，通过示例的方式提供这些实施例，使得本公开将是完全和完整的，并且向本领域中的技术人员充分传达本发明所有方面的范围。贯穿说明书中相似的附图标记指示相似的元件。

[0027] 图1示出了连接到线性无源CAN总线14的三个CAN节点11、12、13。CAN总线是由连接到每个CAN节点的相应端子的两条物理线CAN_H和CAN_L构成的多主串行通信总线。CAN网络10中的所有CAN节点(以例如ECU的形式呈现)连接到这两条线。

[0028] 在内部，每个CAN节点11、12、13具有：总线接口电路；CAN收发器15、16、17。每个收发器包括被称为总线驱动器的发射部分和被称为总线比较器(未示出)的接收部分。

[0029] 每个CAN节点还具有根据ISO 11898-1处理数据链路层上的协议比特流的接收和发送的CAN协议控制器18、19、20。微控制器21、22、23连接到相应的CAN协议控制器18、19、20。CAN协议控制器可以可选地是微控制器的一部分。在典型的线性无源CAN总线14中，通常有下文将进一步讨论的两个终端电阻器24、25。

[0030] CAN协议使用具有值0和1(也称为显性比特和隐性比特)的串行比特流，这形成了在CAN总线14上传输的CAN数据帧、CAN远程帧和其他协议符号。CAN数据帧是一个“容器”，其中可以在两个或更多个CAN节点之间传送信号。信号代表CAN节点之间共享的有用信息，例如车速、制动请求、门锁请求等。ISO-11898-1定义了若干CAN数据帧格式，例如，经典基础帧格式(CBFF)、经典扩展帧格式(CEFF)、灵活数据速率(FD)基础帧格式(FBFF)和FD扩展帧格式(FEFF)。

[0031] 所有CAN节点11、12、13能够向彼此传输帧。CAN协议控制器18、19、20处理CAN帧的接收和发送。从CAN协议控制器传输的比特值0和1在每个CAN节点中的CAN收发器15、16、17中被转换成CAN总线14上的两个模拟电压电平，两个模拟电压电平被称为隐性状态和显性状态。

[0032] 亦即，隐性状态是由通过总线发送隐性数据(具有值1的比特)导致的，而显性状态是由通过总线发送显性数据(具有值0的比特)导致的。这些状态涉及CAN总线14上的两个电压范围。对于接收而言是相反的；CAN收发器15、16、17将CAN总线14上的两个电压电平转换成针对CAN协议控制器18、19、20的适当电平。

[0033] 所有CAN节点具有CAN_H和CAN_L总线线上的有线-AND连接；所有CAN节点通过分别连接所有CAN_H线和所有CAN_L线而彼此直接连接。每个CAN节点11、12、13可以将CAN总线14驱动到一系列隐性/显性状态，从而根据ISO 11898-1启用多主通信网络。CAN协议数据链路层定义如何根据载波感应多路访问(CSMA)操作来执行网络的这种多主共享。

[0034] 由CAN节点11、12、13传输的所有数据在CAN总线14上被共享，使得所有CAN节点接收到相同的比特流。如果至少一个CAN节点传输显性比特(逻辑0)，则用于所有CAN节点的CAN总线为显性的(逻辑0)，否则CAN总线为隐性的(逻辑1)。

[0035] 这意味着，任何CAN节点可以覆写隐性状态(1)以变成显性状态(0)；仅在某些限制情况中允许这样做，并且并非对于任何CAN帧都是规律进行的。CAN节点不能覆写显性状态(0)以变成隐性的(1)。这就是CAN如何被设计和CAN应当如何操作。

[0036] 图2示出了根据标准ISO 11898-2的用于通过总线转移的隐性数据和显性数据的CAN总线上的规定电压范围。

[0037] 在图2中，针对在CAN_H和CAN_L线之间测量的预期CAN总线差分电压(称为V_{diff})、针对CAN收发器的发射器部分(即总线驱动器)和CAN收发器的接收器部分(即，总线比较器)示出了细节，其中V_{diff}被测量为从总线线CAN_H到地的电压VCAN_H减去从总线线CAN_L到地的电压VCAN_L。发射器允许电压在相对窄的区间(即，区间241和251)中，而接收器必须接受更宽的区间(即，区间242和252)分别作为隐性状态和显性状态。这导致了接收器针对CAN节点的V_{diff}电压间的差的公差。显性状态中的电压V_{diff}在50Ω到65Ω的正常总线电阻处的传输CAN节点输出上必须在+1.5V和+3.0V之间。对于给定的CAN节点，实际显性数据电压落在这个电压范围之内的任何地方，但或多或少是固定的，在来自总线终端部件和CAN电缆阻抗的温度以及负载上有轻微变化。在一些情况下，在超过一个CAN节点同时传输显性(多达32个CAN节点可以连接到总线)时，如范围240所示，V_{diff}电压可以高于+3.0V。这在下文将更详细地描述。

[0038] 对于单个车辆或车辆的车队中的ECU群体(即，CAN节点)而言，V_{diff}显性电压可以在ECU和ECU之间在范围+1.5V-+3.0V之内变化。该变化是由于若干原因导致的，例如收发器硬件生产公差、不同的收发器品牌设计、温度、老化等。这些众多原因部分是存在从+1.5V到+3.0V的允许范围的原因，以即使在同一CAN网络上的电压电平差很大也给出鲁棒和容忍的系统。

[0039] 遵循ISO 11898-2的接收ECU必须接受两个CAN终端之间的从+0.9V到+8.0V的电压V_{diff}作为显性。对于显性传输而言，V_{diff}在从+1.5V到+3.0V的范围中；对于隐性传输为+0.05到-0.5V，并且对于隐性接收为+0.5V到-3.0V。对于0.5V和0.9V之间的接收器电压，所得到

的状态未定义，但通常存在具有实施迟滞的隐性到显性和显性到隐性状态过渡。

[0040] 现在，在企图操纵CAN帧时，攻击者设备将修改由车辆ECU传输的CAN帧的比特。根据需要，在任何方向上修改帧的任何比特，从隐性(1)到显性(0)，或者从显性(0)到隐性(1)，以便修改CAN总线14上的信号值，例如，从而将门锁信号从LOCK改变为UNLOCK。

[0041] 图3-图7示出了操纵通过CAN总线14发送的数据的可能企图的示例。

[0042] 图3示出了所谓的拒绝服务(DOS)攻击，其中能够访问CAN总线14的攻击者设备30阻碍第一CAN节点11向第二CAN节点12或第三CAN节点13发送数据，或者使得由第一CAN节点11发送的数据变成无效的。

[0043] 图4示出了第二CAN节点12的欺骗攻击，其在向第三CAN节点13发送数据时，假装是第一CAN节点1。因此，攻击者设备可以是CAN网络(被配置为具有恶意硬件或软件)中已经包括的设备，并且未必是强加连接到总线的外部攻击者设备。

[0044] 图5示出了外部攻击者设备30的欺骗攻击，在向第三CAN节点13发送数据时，其假装是第一CAN节点11。被欺骗的帧可以包括被操纵的ACK字段，其中ACK比特＝0已经指示了确认。

[0045] 图6示出了攻击者设备30修改从第一CAN节点11向第三CAN节点13发送的数据而进行的篡改攻击。因此，攻击者设备可以是CAN网络中已经包括的设备，并且未必是强制连接到总线的外部攻击者设备。

[0046] 图7示出了所谓的重放攻击，其中在第一步骤(顶部示图)中能够访问CAN总线14的攻击者设备30记录从第一CAN节点11到第三CAN节点13的正常数据传输。之后，在第二步骤(底部示图)中，攻击者设备30向第三CAN节点13重放所记录的数据传输从而假装是第一CAN节点11。

[0047] 可以得到结论，可以设想操纵CAN网络的很多方式。在下文中，将交替使用“操纵”、“修改”和“篡改”示出如下情形：攻击者修改一个或多个CAN数据帧的比特，或者创建新的CAN数据帧，以引起一个或多个CAN节点以特定方式运转，或者引起CAN节点执行一些特定动作。

[0048] 在汽车行业中的开发和验证中通常用于非恶意目的的现有CAN测试工具可以在操纵CAN网络时被用作图3、图5、图6、图7中的攻击者设备。这些工具不检测CAN总线数据操纵。

[0049] 此外，诸如板载诊断(OBD)-II-加密狗、用于自动生成驾驶日志簿的设备、汽车保险公司提供的驾驶方式监测设备的现有CAN设备被暂时或永久地附接到车辆CAN总线，并可以出于恶意目的被修改。

[0050] 如前所述，利用遵从ISO-11898-2的正常CAN收发器，仅从隐性(1)修改为显性(0)是可能的；隐性总线可能变为显性，而不是反过来的。然而，如果能够将CAN总线上的数据从显性(0)修改为隐性(1)，则可能设计专用CAN收发器。

[0051] 于是，考虑到潜在地操纵CAN总线的恶意方，针对CAN收发器可以设想六种情形：

[0052] -正常隐性

[0053] -正常显性

[0054] -隐性修改为显性(篡改)

[0055] -显性修改为隐性(篡改)

[0056] -隐性到隐性修改，即，总线状态不改变(篡改)

[0057] -显性到显性修改,即,总线状态不改变(篡改)

[0058] 然而,正常CAN收发器自身不能确定是否发生了篡改。只要差分总线电压V_{diff}遵从图2的电压范围242和252,而不论这些电压是如何达到的,CAN收发器将接受正常帧和被操纵的帧。

[0059] 图8a和图8b示出了充当每个CAN节点11、12、13到CAN总线14的接口的每个CAN收发器15、16、17的发射器部分——即总线驱动器——的示意图。

[0060] 在典型的线性无源CAN总线14中,正常有两个终端电阻器24、25。每个终端电阻的典型值为120Ω,以匹配120Ω的典型的CAN总线电缆或传输线阻抗。以下描述基于两个120Ω终端电阻器24、25、单个60Ω电阻器、或由终端/收发器部件实现的任何其他形式的60Ω总线电阻的配置。本发明不限于这些电阻器/阻抗值,而是可以与任何电阻/总线阻抗使用。

[0061] 每个CAN收发器具有与CAN总线并联连接的总线偏置电阻器34,然而,它们的电阻在几千欧姆的量级(R_{diff}=12kΩ到100kΩ),因此总的总线阻抗仍然主要由终端电阻器24、25的低得多的电阻值支配。在下文中无视总线偏置电阻器34的电阻,因为它们对总线电阻和总线阻抗没有显著影响。

[0062] 现在,参考图8a的电路,CAN总线14的特征差分电阻和阻抗在闲置总线状态期间和在向CAN总线14传输隐性数据期间在正常隐性状态中大约为60Ω。在正常隐性传输状态中,在利用开关31示出的场效应晶体管(FET)导通时,由于终端电阻器24、25与CAN总线14的CAN_H和CAN_L线并联连接,并且两条CAN线是并联的,因此所得到的总线阻抗为120×120/(120+120)=60Ω。

[0063] 此外,参考图8b的示例性电路,其示出了在CAN总线14上传输显性状态的单个CAN收发器15。机动车辆中使用的正常CAN收发器的常用电源电压Vcc为+5.0V。在一个CAN节点向60Ω总线电阻传输显性数据时,典型的V_{diff}显性驱动能力为+2.0V(尽管允许完整的+1.5V到+3.0V范围并且也用于机动车辆)。在本示例中,可以计算CAN总线阻抗和CAN收发器阻抗。CAN收发器15和CAN总线终端电阻器24、25形成分压器,所述分压器将CAN收发器Vcc电源电压向下划分成CAN总线14上的更低的电压V_{diff}。

[0064] 在+2.0V CAN总线电压V_{diff}和60Ω总线电阻下,通过电源35、CAN收发器15和终端电阻器24、25的电流为2.0/60=0.033A。由于Vcc为5.0V,所以在CAN收发器15及其两个驱动级33中的总线驱动器部件31、32、33a之上生成了5.0-2.0=3.0V的总电压降。CAN收发器15的内阻大约为90Ω,因为在收发器之上有3.0V的总电压降,并且0.033A的电流流经收发器。在本示例中,收发器阻抗等于其内阻,从而是3.0/0.033=90Ω。在本示例中,Vcc电压源35的内阻和阻抗大约为0Ω,并且因为它与每个收发器驱动级33串联连接,所以将0Ω添加到收发器内阻90Ω,得到电源和收发器的总内阻和阻抗为90Ω。

[0065] 图8b中的CAN总线14的特征阻抗在正常显性传输状态(开关31闭合)中大约为36Ω,因为CAN收发器15的90Ω内阻有效地变为与CAN总线14的60Ω电阻并联耦合,并且从而所得到的阻抗是60×90/(60+90)=36Ω。假设任何总线状态中的收发器阻抗等价于其内阻。

[0066] 图8b中的总线驱动器开关31、二极管32和内阻33a是总线驱动器的内部部件的简化示意图。它们形成两个相同的总线驱动器级33。在这里所示的+2.0V之外的其他所得到的显性总线电压(根据图2中的241,允许+1.5到+3.0V)下,收发器内阻和所得到的CAN总线阻

抗将是不同的，但仍然显著低于隐性状态中的60Ω。例如，在V_{diff}＝+1.5V下，收发器内阻大约为140Ω，并且与60Ω的总线电阻并联连接，从而导致大约42Ω的总线阻抗。在V_{diff}＝+3.0V下，收发器内阻大约为40Ω，并且与60Ω的总线电阻并联连接，从而导致大约24Ω的总线阻抗。

[0067] 再次参考图8b的电路，通常可能发生另一种情况，这是针对图8b前述的变化。在所述另一种情况中，在CAN总线上可能有大量CAN节点，例如，最多32个CAN节点。对于CAN网络而言，可能难以事先知道是否超过一个CAN节点将同时开始帧传输，并在任何给定时间参与仲裁。如果总线当前不闲置，并且在两个CAN节点中至少两个帧排队以用于传输，它们将(在下一次总线闲置检测之后)参与仲裁过程。

[0068] 在一些示例中，若干或全部CAN节点能够同时开始帧传输。在发生这种情况时，由多达32个CAN节点同时将所谓的帧开始(SOF)比特(其始终为显性)和CAN帧仲裁字段中的显性比特驱动到显性。ISO-11898-2规范允许超过+1.5V到+3.0V的正常范围(即图2中的范围241)的总线电压V_{diff}。对于多个发射器而言，允许高达+5.0V的总线电压，即图2中的范围240。这在70Ω的总线电阻下是适用的。在所有CAN收发器具有相等的输出电压/电流能力的情况下，由于总线负载在所有32个CAN节点之中共享，所以每个CAN收发器确保等价总线电阻为70×32＝2240Ω(图8b中未示出)。

[0069] 机动车辆中使用的CAN总线收发器的典型实施方式使用两个驱动级33，其中所得到的显性总线电压强烈依赖于总线负载。更高的负载(终端电阻器的更低电阻值)导致更低的总线电压。更低的负载(终端电阻器的更高电阻值，或者仅将电流的一部分驱动到终端电阻器中，如在同时发生SOF和仲裁字段的显性比特、ACK比特期间的情况)导致更高的总线电压。

[0070] 如图8b中所示，在32个CAN节点同时驱动显性并共享60Ω而不是70Ω的总线负载的情况下，可以预计低于+5.0V的总线电压，例如+4.6V的总线电压。每个CAN收发器共享总线电阻的负载，并且在相等的电压/电流能力驱动相等量的电流的情况下，4.6/60/32＝0.0024A，在使用+5.0V电源的CAN收发器之上的电压降为0.4V，并且CAN收发器的内阻为0.4V/0.0024＝167Ω。由于所有收发器并联耦合，全部CAN收发器的所得到的并联内阻为167/32＝5.2Ω。CAN收发器的并联电阻变得与60Ω总线电阻并联耦合，并且所得到的CAN总线阻抗为5.2×60/(5.2+60)＝4.8Ω。在ACK字段中的ACK比特(始终显性)期间，预计总线阻抗也接近4.8Ω，其中，除了一个之外的全部接收器(具有32个CAN节点的网络中的31个)同时传输ACK。在具有少于32个CAN节点的CAN网络中，对应的更低数量的CAN节点传输ACK，并且因此所得到的总线阻抗可以高于4.8Ω。

[0071] 如果在32个CAN节点同时传输SOF和显性仲裁比特期间达到+4.0V的显性总线电压，假设每个CAN收发器驱动相等量的电流，4.0/60/32＝0.002A，则在每个CAN收发器之上的电压降为5.0-4.0＝1.0V。CAN收发器的内阻为1.0V/0.002A＝500Ω。从而所有收发器的所得到的并联内阻为500/32＝15Ω。CAN收发器的并联电阻变得与60Ω总线电阻并联耦合，从而所得到的总线阻抗为15×60/(15+60)＝12Ω。

[0072] 图8b示出了具有单个电源35的单个CAN收发器15。在一些示例中，可以有两个电源。亦即，单独的电压电源用于与CAN_H相关的上驱动器级33，并且单独的电压电源用于与CAN_L相关的下驱动器级33。所得到的CAN收发器内阻在这里也适用，并且变得与CAN总线14

并联耦合，并且以相同的方式计算总线阻抗。

[0073] 因此，在CAN节点传输操作期间，这些分别是针对隐性状态和显性状态的CAN总线14的正常预计的特征阻抗。

[0074] 然而，在正常操作期间，不能强迫显性状态变为隐性。再次参考图8a和图8b，二极管32将仅在一个(正向)方向上导通，从而使得能够强迫隐性总线变为显性，而不是反过来的。

[0075] 在传输CAN节点传输隐性比特(即，具有在图2的范围251中的电压)时，这个比特被攻击者设备或任何正常CAN节点覆写，以变为显性比特(即，具有在图2的范围241中的电压)。因此，可以由攻击者设备中的正常CAN收发器进行从隐性到显性的这种比特修改。

[0076] 参考图9a，攻击者设备30装备有切换显性电压并具有4Ω的低内阻和阻抗的专用CAN收发器/总线驱动器，以向CAN总线14上强加显性总线状态。CAN总线电阻为60Ω。如果攻击者收发器电源为+5.0V且攻击者收发器总内阻为4Ω，5.0/(60+4)＝0.078A的电流流经攻击者收发器、CAN总线14和终端电阻器24、25。攻击者收发器之上的所得到的总电压降为0.078×4＝0.31V。所得到的总线电压V_{diff}为5.0-0.31＝4.69V，这落在了图2中的显性接收电压范围之内。攻击者内阻变得与CAN总线14的60Ω总线电阻(电阻器24、25)并联耦合，并且从而所得到的总线阻抗将是60×4/(60+4)＝3.75Ω。

[0077] 可以得到结论，如果攻击者设备的内阻为4Ω，则CAN总线14的特征阻抗将远低于36Ω。

[0078] 在传输CAN节点传输显性比特(即，具有在图2的范围241中的电压)时，这个比特被攻击者设备覆写以变成隐性比特(即，具有在图2的范围252中的电压)，并且从而被其他接收CAN节点感知为隐性比特。如前所述，不能通过正常CAN收发器进行从显性到隐性的这种比特修改。

[0079] 参考图9b，从而攻击者设备30需要装备有专用CAN收发器/总线驱动器，其将CAN总线14上的仅几欧姆量级的低阻抗负载切换成CAN节点的CAN收发器15的负载。在提供显性总线电压的同时，这一总线负载比正常CAN收发器15设计的显著更重，并将(从图2的范围242中为显性)大大减小差分电压V_{diff}，使得CAN总线14上的电压将低于0.5V，或者甚至为负，并且从而成为隐性(即，在图2的电压范围252中)。

[0080] 在另一个示例中，攻击者设备30的专用CAN收发器可以切换具有在+0.5V之下或低于+0.5V或甚至为负的电压的电压源(未示出)，并引起CAN总线上的电压处于图2中的隐性范围252中。在其他示例中，攻击者可以切换地电势0V和车辆电源电压+12V，并引起CAN总线上的电压处于隐性范围中。

[0081] CAN节点11中的正常CAN收发器15不能向CAN总线14供应足够的电流(如ISO-11898-2:2017中规定的，最大电源电流I_{CAN_H}、I_{CAN_L}达到115mA)以便维持显性电压，并胜过攻击者设备30的专用CAN收发器/总线驱动器低阻抗负载或低电压源，从而强加隐性电压。

[0082] 不幸地，攻击者设备30可以成功利用CAN节点上的这种约束，攻击者设备30被设计成供应比115mA显著更大的电流。攻击者设备可以在已知保证正常CAN收发器15提供最大115mA时，故意地使其过载。除了需要完成图2的范围242/252的CAN总线电压之外，攻击者设备30还具有少数物理层约束，未必是电压241/251。

[0083] 在图9b中，假设攻击者设备30具有4Ω的内阻38。这个电阻变得与CAN总线14的60

Ω总线电阻(电阻器24、25)并联耦合,并且从而所得到的总线电阻将是60×4/(60+4)=3.75Ω。

[0084] 在115mA的最大允许正常收发器显性状态电流进入到3.75Ω的总线电阻中时,正常CAN收发器提供0.115×3.75=0.43V,这将不能达到显性状态的最低0.9V阈值,即图2中的242。相反,0.43V落在隐性电压的范围之内,即图2中的252。由于正常CAN收发器15之上的电压降为5.0-0.43=4.57V,所以收发器的内阻为4.57/0.115=39.7Ω。CAN总线14的所得到的特征阻抗从而将降低到39.7×3.75/(39.7+3.75)=3.3Ω。可以得到结论,如果攻击者设备的电阻为4Ω,则CAN总线14的特征阻抗将远低于36Ω。

[0085] 因此,如果检测到CAN总线14的特征阻抗的这种急剧降低,则认为检测到操纵CAN总线14的企图,并且从而可以例如通过在检测到该企图时丢弃总线上的任何CAN帧来避开该企图。

[0086] 通过收发器15的隐性总线电压的上阈值+0.5V(即图2中的范围252)确定与由CAN收发器15驱动到显性状态的总线电阻(由24、25代表)并联连接的攻击者设备30的最大可用内阻38。在115mA的最大正常收发器电流能力下,总的总线电阻为0.5/0.115=4.3Ω。由于终端电阻(由24、25代表)为60Ω,因为4.6×60/(4.6+60)=4.3Ω,所以最大攻击者设备电阻从而为4.6Ω。

[0087] 在机动车辆中使用的正常CAN收发器的一些示例中,在显性下提供的最大总线电流远低于115mA。在这样的情况下,能够强加隐性电压的最大攻击者电阻因此高于4.6Ω。在机动车辆中使用的CAN收发器的一些实施方式中,5到10Ω的攻击者电阻能够强迫总线电压为隐性。

[0088] 此外,对于攻击者存在两种情形。攻击者可能事先不知道传输CAN节点15要在例如数据字段的比特中传输什么数据(隐性或显性)。攻击者可以尝试在CAN总线14上强加隐性或显性状态,而事先不考虑CAN节点15传输的内容,并且一些比特可以是与CAN节点15传输相同的数据。在这种情况下,总线状态(隐性或显性)实际上不改变,而是保持相同。然而,总线阻抗将被操纵。

[0089] 在CAN节点15传输隐性状态数据时,总线电阻和阻抗为60Ω,并且攻击者还企图强加隐性状态,并切换4Ω的电阻负载,其变得与总线并联耦合。CAN总线阻抗从而是60×4/(60+4)=3.75Ω。

[0090] 在CAN节点15传输显性时,总线阻抗为36Ω。攻击者利用电源35切换显性电压,并具有4Ω的内阻,该内阻变得与总线14并联耦合。所得到的CAN总线阻抗从而为36×4/(36+4)=3.4Ω。替代性的,由于在CAN收发器15和攻击者之间的显性电压/电流驱动能力有很大差异,CAN收发器15将不会处于其二极管32工作于正向模式的操作点,因此,正常收发器15不会影响CAN总线阻抗,并且攻击者将支配总线电压和总线阻抗。CAN总线阻抗因此反而是60×4/(60+4)=3.75Ω。

[0091] 可以得到结论,在这两种情形中,总线状态不会实际改变。处于隐性状态中的CAN总线14的特征阻抗被操纵并将远低于60Ω。处于显性状态中的CAN总线14的特征阻抗被操纵并将远低于36Ω。

[0092] 可以得到结论,在传输SOF的正常情况下和在仲裁字段中的显性比特传输期间,以及在多个CAN节点传输ACK字段中的ACK比特期间,可以检测到类似的低CAN总线阻抗。

[0093] 现有的CAN总线可以由具有比先前所述的120Ω+120Ω＝60Ω更低或大得多的电阻的电阻器终止。终端电阻可以是从例如45Ω直到几百Ω的范围。所得到的总线电压、总线电流、收发器电流、收发器内部阻抗、所得到的总线阻抗将是不同的。总线操纵所需的攻击者设备的电压或电阻可以是不同的，但将遵从前述原则。

[0094] 因此，布置根据实施例的设备，使得其可以检测CAN总线阻抗从第一预期阻抗到第二更低阻抗的变化(通过测量CAN总线14的适当电性质，例如实际阻抗，或者间接通过测量总线电压和/或电流)。其他电性质例如包括总线共模电压、CAN_L或CAN_H线的单端总线电压、单端总线阻抗等。

[0095] 基于由CAN接收器(总线比较器)确定的实际总线电压，确定CAN总线状态为隐性(即，处于图2的范围242之内的电压)或显性(即，处于图2的范围252之内的电压)。实际总线电压可以是或可以不是凭借操纵总线电阻或阻抗而操纵总线状态的结果。所确定的总线状态(隐性或显性)控制着用于确定总线阻抗是正常的还是操纵的结果的阻抗阈值。

[0096] 因此，根据实施例的设备将检测CAN总线阻抗是否低于预定阈值。如果低于预定阈值，则对该设备给出CAN总线14上的数据可能被操纵的指示。

[0097] 在图10a中示出的其最基本形式中，图10a示出了图1的CAN网络10，这样的设备100可以被呈现为“嗅探器”，其可容易地连接到CAN总线14，以用于利用阻抗检测部件101检测CAN总线阻抗中的上述变化。

[0098] 将进一步参考图10b，图10b示出了根据实施例的示出了检测在CAN总线14上的数据操纵的方法的流程图。

[0099] 嗅探器设备100因此能够在步骤S101中利用阻抗检测部件101检测到CAN总线阻抗中的急剧变化时，例如从36Ω的第一值降低到大约3-4Ω的第二值(如参考图9b所讨论的)，改变每个CAN节点11、12、13或一些中央控制器(未示出)，因此CAN节点11、12、13可以得到结论，应当丢弃当前通过CAN总线14正在传送的CAN帧。出于安全原因，可以决定在检测到总线阻抗的这种降低时，丢弃多个CAN帧。要指出的是，嗅探器设备100不需要确定在两个值之间的阻抗存在降低，而是仅仅需要得出结论，总线阻抗值低于预定阈值，例如5Ω或10Ω。

[0100] 然而，如前所述，在一些情况下，在通过CAN总线传输CAN数据帧时，总线阻抗在正常显性状态数据传输期间也可能从36Ω显著降低到3-4Ω。在传输SOF比特以用信号通知通过CAN总线传输的CAN帧的开始和后续总线仲裁期间，可能会发生这种情况，因为在若干CAN节点同时传输显性时，其总线驱动器并行操作，并且因此减小总的总线阻抗。为了解决这个问题，嗅探器设备100将进一步装备有CAN帧解码器102。

[0101] 将参考图11简要讨论根据经典基本帧格式(CBFF)的CAN数据帧的格式。首先，由CAN节点检测到SOF比特，这表示CAN数据帧的开始。在CAN协议中，11个隐性比特的序列之后的任何显性比特将被解释为SOF比特。之后，仲裁字段由11比特的IDENTIFIER字段和后续远程传输请求(RTR)比特组成。IDENTIFIER字段将识别哪个CAN节点是CAN帧的发射器。换言之，在IDENTIFIER字段和RTR比特(即，12个比特)的传输期间发生仲裁，以便确定/识别多个CAN节点中的哪一个将获得对总线的访问权以用于CAN帧传输。

[0102] 根据CBFF格式的CAN数据帧还包括标识符扩展(IDE)比特、灵活数据速率帧(FDF)比特、4比特数据长度代码(DLC)字段、多达64个数据比特(对于数据帧而言)、15比特循环冗余校验(CRC)字段、CRC定界符比特、确认(ACK)比特、ACK定界符比特和7比特帧结束(EOF)字

段。

[0103] 对于根据CEFF格式的CAN数据帧，仲裁字段由11比特IDENTIFIER字段、替代远程请求(SRR)比特、IDE比特、18比特IDENTIFIER扩展字段和RTR比特(即，32个比特)组成。

[0104] 对于根据FBFF格式的CAN数据帧，仲裁字段由11比特IDENTIFIER字段和RTR比特(即，12个比特)组成。

[0105] 对于根据FEFF格式的CAN数据帧，仲裁字段由11比特IDENTIFIER字段、SRR比特、IDE比特、18比特IDENTIFIER扩展字段和远程请求替代(RRS)比特(即，32个比特)组成。因此，在图10a和图10b的实施例中，嗅探器设备100还将装备有CAN帧解码器102，从而能够对接收的CAN帧解码，使得嗅探器设备100能够在步骤S102中识别在CAN总线14上是否可能发生仲裁。亦即，CAN帧解码器102将使得嗅探器设备100能够在步骤S102中检测SOF比特和IDENTIFIER比特字段，以便确定在可能的CAN总线仲裁期间是否发生了总线阻抗从36Ω急剧地降低到大约3-4Ω的检测。如果发生了，将不认为阻抗降低是恶意总线操纵企图的结果，而是CAN总线14上正常进行的仲裁的后果(并且通常将执行连续阻抗测量)。要指出的是，在可能发生仲裁的期间，嗅探器设备100的CAN帧解码器102检测IDENTIFIER字段，但将不检测CAN总线14上发生的实际仲裁。

[0106] 然而，如果已经通过CAN总线14传递了仲裁字段数据比特，则不再发生仲裁，并且CAN帧解码器102将在步骤S103中有利地确定总线阻抗中的急剧增大是操纵企图的结果。

[0107] 要指出的是，本实施例中的嗅探器设备100不一定装备有CAN发射器。因此，与前文所述的正常CAN收发器相比，嗅探器设备100仅必须装备有CAN总线比较器(即，CAN接收器)，而不装备有CAN总线驱动器(即，CAN发射器)，因为嗅探器设备100仅从CAN总线14接收数据而不向CAN总线14传输任何数据。CAN帧解码器102可以包括CAN节点11、12、13中包括的类型的CAN协议控制器18、19、20，以对接收的CAN数据帧解码，即使嗅探器设备100中使用的CAN帧解码器102严格地必须不能装备有将数据解码成将通过CAN总线14传输的CAN帧的任何能力。

[0108] 替代性地，参考图10c，图10c示出了根据另一实施例的示出了检测在CAN总线14上的数据操纵的方法的流程图，可以设想，嗅探器设备100首先在步骤S201中检测当前是否可能发生仲裁，并且如果可能发生仲裁，在CAN总线14上当前正在发生的潜在仲裁过程期间抑制检测总线阻抗中的任何改变。因此，在这样的替代实施例中，将仅在当前没有正在进行仲裁时，才在步骤S202中进行总线阻抗的检测。如前所述，如果嗅探器设备100在步骤S202中检测到总线阻抗从36Ω急剧地降低到大约3-4Ω，并且当前在CAN总线上未遇到仲裁字段(如在先前步骤S201中所确定的)——即，未传输IDENTIFIER数据和RTR比特——则在步骤S203中认为已经检测到恶意CAN总线操纵企图，并且相应地警告CAN节点11、12、13或中央单元从而可以避开企图。

[0109] 在利用CBFF帧格式的实施例中，嗅探器设备100的CAN帧解码器102检测SOF比特，并且从而知道后续11个比特属于IDENTIFIER字段和随后的单个RTR比特，其信号的传输指示正在发生潜在仲裁。因此，仲裁字段中传输的任何显性数据潜在地指示正在发生仲裁。CAN帧解码器意识到CAN总线上正遇到的CAN数据帧(或CAN远程帧)的当前字段(仲裁字段、控制字段、数据字段等)的配置。在传递这13个比特之后(即，SOF比特、11比特IDENTIFIER字段和RTR比特)，嗅探器设备100的阻抗检测部件101将执行CAN总线阻抗降低的检测。替代性

地，无视在总线上转移这13个比特期间发生的显性状态下的CAN总线阻抗降低的任何检测。其他帧格式可以被使用并可以包括不同长度的仲裁字段和标识符字段，例如，CEFF、FEFF、FBFF，如前所述。

[0110] 在其他实施例中，如果通过多个CAN节点在CAN总线14上同时发送ACK比特期间发生CAN总线阻抗的这种降低(如总线阻抗低于预定阈值所指示的)，则不认为降低是CAN总线操纵的结果，因为它可能在正常操作期间发生。替代性地，在转移ACK比特期间不执行阻抗检测。

[0111] 在实施例中，由于总线阻抗未必从36Ω下降到3-4Ω(如参考图9a所讨论的)，但可能潜在地会下降到刚刚低于10Ω，同时仍然能够将隐性状态修改为变成显性，嗅探器设备100将检测如果总线阻抗低于T＝10Ω的阈值，则总线可能被操纵。

[0112] 在实施例中，由于总线阻抗未必从60Ω下降到3-4Ω(如参考图9a和图9b所讨论的)，但可能潜在地会下降到刚刚低于10Ω，同时仍然能够将显性状态修改为变成隐性，嗅探器设备100将检测如果总线阻抗低于T＝10Ω的阈值，则总线可能被操纵。

[0113] 将设备呈现为可容易连接到CAN总线14的嗅探器设备100的优点在于，可以将此类设备添加到已获得的CAN网络10而无需较大的修改。

[0114] 如将在以下实施例中的一些中所讨论的，该设备可以集成有CAN收发器，从而生成能够进行完整尺度的CAN数据通信以及总线阻抗检测的增强CAN收发器。然而，图10a的嗅探器设备100具有的优点在于，在功能性方面相对不复杂，并且不需要装备有远更复杂的CAN收发器的所有部件。

[0115] 图12示出了先前称为增强CAN收发器150以集成有CAN节点110(例如ECU)的其它实施例。如先前描述的现有技术CAN收发器15、16、17，CAN节点110包括被配置为向/从主机130传送数据的CAN协议控制器180(参考图1的CAN协议控制器18、19、20)，主机130例如是门锁模块或类似物。进一步类似于现有技术的CAN收发器15、16、17，增强CAN收发器150包括遵从先前参考图2所述的电压电平的总线比较器103和总线驱动器104。

[0116] 然而，除了现有技术的CAN收发器之外，增强CAN收发器150还包括类似于根据实施例的参考图10a-c所述的嗅探器设备100的阻抗检测部件101，其被配置为检测CAN总线阻抗是否在3-4Ω附近(或至少低于10Ω)。

[0117] 进一步类似于嗅探器设备100，增强CAN总线收发器150包括CAN帧解码器102，其被配置为对通过CAN总线14传输(并经由线路108接收)的CAN数据帧和CAN远程帧解码，以便检测SOF比特和指示可能发生仲裁的后续IDENTIFIER数据字段。同样，CAN帧解码器102可以(经由线路106)控制阻抗检测部件101以仅在CAN接收器103检测到未发生潜在仲裁(即，在总线14上未检测到SOF比特+IDENTIFIER数据字段和RTR比特)时才测量CAN总线阻抗，因为在正常操作期间可能发生总线阻抗的急剧降低，其中在CAN总线14上遇到SOF比特或IDENTIFIER数据字段。

[0118] 要指出的是，可以使用完整的CAN协议控制器来实施CAN帧解码器102，尽管CAN帧解码器102不用于将数据编码成将通过CAN总线14传输的CAN帧，而是用于对通过CAN总线14接收的CAN数据帧解码。

[0119] 现在，如果CAN帧解码器102与阻抗检测部件101合作在可能未发生仲裁时检测总线阻抗低于阈值(参考图10b的步骤S101和S102或图10c的步骤S202和S201)，即，在遇到SOF

比特和IDENTIFIER数据字段和RTR比特之外，则认为已经检测到恶意CAN总线操纵企图(参考图10b的步骤S103或图10c的步骤S203)。

[0120] 对于正常未篡改的CAN总线，需要不干扰正常CAN数据帧从CAN控制器180向和从CAN总线14的传输和接收。这涉及例如帧和帧的数据内容的时序性质。接收的CAN数据帧从而将经由总线比较器103传递以经由RXD线路112到CAN协议控制器180。CAN协议控制器180然后将CAN数据帧的有效载荷数据(即，图11中所示的帧的DATA字段)传递到主机130。所传输的CAN帧将从CAN控制器180经由TXD线路111传递到总线驱动器104并传递到CAN总线14。

[0121] 然而，在实施例中，为了避免任何潜在被操纵的CAN数据到达CAN协议控制器180并最终到达主机130，引入第一开关114，在如前所述检测到任何操纵企图的情况下，可以由CAN帧解码器102控制第一开关114。因此，如果CAN帧解码器102检测到操纵企图，则CAN帧解码器102可以通过经由线路107控制第一开关114来丢弃潜在被操纵的CAN帧，使得CAN协议控制器180接收显性数据(例如是由至少六个相继比特(由“0”代表)组成的错误标记(EF))而不是潜在被操纵的(一个或多个)CAN数据帧。

[0122] 可选地，引入第二开关113以避免经由TXD线路111传输的来自CAN协议控制器180的任何错误响应。于是，如果CAN帧解码器102检测到操纵企图，CAN帧解码器102可以通过经由线路107控制第二开关113而丢弃来自CAN协议控制器180的响应信号，以经由总线驱动器104向CAN总线14输出隐性数据(由“1”代表)。

[0123] 由于要基于总线电性质来批准或不批准接收的帧，并且增强CAN收发器150必须要保持未篡改帧的时序和内容，所以它必须最初允许接收接收的帧的开始，直到该帧稍晚可能被检测为被篡改为止；只能在构成SOF比特和IDENTIFIER数据字段+RTR比特的CAN帧的部分被CAN帧解码器102解码并且同一部分已经被传递到CAN协议控制器180之后，才能确定这种情况。如果未检测到CAN帧被操纵，则必须透明地传递完整的CAN帧，直到其结束为止。因此，需要确定新接收的帧的开始，CAN帧解码器102(可能使用完整的CAN协议控制器实施)确实能够这样做。

[0124] ISO-11898-1中定义的CAN数据链路协议定义了在检测到数据链路层上的错误(例如，CRC错误、填塞错误、格式错误)时发信号通知错误(使接收的帧无效)的方式。如果检测到接收的CAN数据帧已经被篡改，则在被篡改的比特期间或在该比特已经被篡改之后紧随的比特期间作出这一决策。必须始终在CAN帧结束之前作出这样的决策，以便防止CAN帧被认为有效并由CAN控制器180接收。

[0125] 对于被操纵的帧，在实施例中，也由增强CAN收发器150使用使接收的帧无效的ISO-11898-1方式来丢弃可能被操纵的接收的CAN帧。这种无效在CAN收发器150和CAN节点110内部，并且不在CAN总线14上传输。在通过CAN帧解码器102与阻抗检测部件101合作检测到接收的CAN帧已经被篡改时，CAN帧解码器102控制第一开关114以通过用错误标记(EF)覆写CAN帧通过有效地破坏经由RXD线路112传递的CAN帧而丢弃接收的CAN帧，该错误标记在至少六个相继比特持续时间的持续时间内展现逻辑0。优选地，错误标记被扩展超过六个比特，或直到在总线14上遇到CAN数据帧的结束，如通过CAN帧解码器102所确定的。

[0126] 以这种方式覆写CAN帧的其余部分将：a)防止CAN协议控制器180将该帧作为有效帧接收，并将从而防止帧内容从CAN协议控制器180被传递并被传递到主机130上；以及b)使得CAN协议控制器180在遇到帧结束之前不会检测到总线闲置，并且由此等待任何未决帧传

输，直到CAN总线14闲置。主机130将不会意识到任何被篡改的CAN帧。在已经检测到被操纵的CAN帧时，可以可选地有从CAN帧解码器102到主机130的通知信号。这可以由主机130用于执行适当步骤，例如，以改变主机的操作状态或任何其他合适的动作。

[0127] 在可选实施例中，CAN帧解码器102可以在使在RXD信号112上接收的CAN帧无效的同时，通过在ACK字段中的ACK比特期间在TXD信号111上传输显性比特来确认CAN总线14上的被篡改的CAN帧。这将由CAN收发器150对被篡改的CAN帧的检测相对于攻击者或CAN总线14上的任何其他CAN节点隐藏起来。于是，CAN节点110将看起来接受被篡改的帧，然而在内部实际上丢弃了它。

[0128] 在实施例中，阻抗检测部件101可以在CAN帧的比特接收期间感测CAN总线阻抗，该比特接收与由ISO-11898-1定义的一个或多个比特时间段一致，比特时间段例如Sync_Seg、Prop_Seg、Phase_Seg 1、Phase_Seg 2或采样点附近。阻抗感测也可以是连续的。

[0129] 在实施例中，可以执行CAN总线阻抗检测，使得其在时间上不与从显性到隐性或从隐性到显性的总线状态的过渡一致，或者不在其后预定时间执行检测。

[0130] 可以使用除ISO-11898-1和ISO-11898-2之外的其他CAN协议。

[0131] 从本实施例可以得出结论，正常未篡改的CAN数据帧可以被透明地向和从主机130和CAN总线14传递，而被检测到潜在地被操纵的任何(一个或多个)CAN数据帧被阻挡，不会到达主机130(和/或CAN总线14)，由此防止篡改和任何后续车辆故障。

[0132] 在替代实施例中，再次参考图12，设想了替代用法。例如，车辆系统设计者或原始设备制造商(OEM)可能希望经由CAN总线通信并且仅在出于保密或安全原因(例如在车间中或在R&D开发期间)能够物理访问车辆时，才允许激活某些功能或车辆模式。其他原因可能是仅在严格控制的情况下解锁、禁用或启用某些车辆功能，并且它们可能受制于针对OEM的商业或数据完整性原因，例如，增大推进系统性能(扭矩、马力)或读取敏感车辆数据。在这样的情况下，实际上可能希望测试CAN网络的鲁棒性或CAN网络如何对恶意攻击做出反应。

[0133] 于是，代替丢弃任何检测到的被操纵的CAN数据帧(由车辆系统设计者或OEM发起)，CAN接收器103检测被操纵的CAN数据帧并控制第一开关114以转发被操纵的CAN数据帧而不是丢弃该帧。甚至可以设想将被操纵的CAN帧转发到CAN协议控制器180并进一步转发到主机130，同时丢弃正常未被操纵的CAN数据帧。

[0134] 如图10a和图12所示，嗅探器设备100和增强CAN收发器150分别包括诸如阻抗检测101和CAN帧解码102的功能，这可以使用合适的(一个或多个)部件来实施。

[0135] 参考图13，根据实施例的设备——这里由增强CAN收发器150代表——包括一个或多个处理单元200，其中可以实施上文所述功能的部分或全部。典型地，增强CAN收发器150的所有功能可以由这样的(一个或多个)处理单元200执行，处理单元200例如CAN帧解码器102、总线阻抗检测器101、开关113、114等的处理单元。

[0136] 在实践中，根据实施例的CAN收发器150(或嗅探器设备100)检测该设备连接到的CAN总线上的数据操纵的方法步骤可以由呈现为一个或多个微处理器形式的处理单元200执行，一个或多个微处理器被布置成执行下载到与微处理器相关联的适当储存介质210的计算机程序220，储存介质例如是随机存取存储器(RAM)、闪存存储器或硬盘驱动器。处理单元200被布置成引起设备150在包括计算机可执行指令的合适的计算机程序220被下载到储存介质210(例如，是非暂态储存介质)并通过处理单元200执行时，执行根据实施例的方法。

储存介质210也可以是包括计算机程序220的计算机程序产品。替代地，可以利用适当的计算机程序产品(例如数字通用光盘(DVD)或存储棒)将计算机程序220转移到存储介质210。作为其他替代，可以通过网络将计算机程序220下载到储存介质210。处理单元200可以替代地呈现为数字信号处理器(DSP)、专用集成电路(ASIC)、现场可编程门阵列(FPGA)、复杂可编程逻辑器件(CPLD)、系统基础芯片(SBC)等形式。

[0137] CAN收发器150可以是在同一IC封装中具有总线驱动器和总线比较器的集成电路(IC)封装器件。替代地，可以通过多个无源部件并通过线性或数字半导体部件来构建收发器150。总线驱动器104和总线比较器103可以由同一IC封装中的集成电路(IC)呈现，例如，现有技术CAN收发器，并且总线特征传感器101、CAN帧解码器102、开关113、114可以独立于收发器IC封装。

[0138] 上文参考其若干实施例和示例主要描述了本公开的方面。然而，本领域中的技术人员将容易认识到，在如所附专利权利要求定义的本发明的范围之内，除了上文公开的那些之外的其他实施例是同样可能的。

[0139] 于是，尽管本文已经公开了各个方面和实施例，但其他方面和实施例对于本领域中的技术人员而言将是显而易见的。本文公开的各个方面和实施例处于说明的目的，而并非旨在使限制性的，真正的范围和精神由以下权利要求指定。

[0140] 缩写列表

[0141] ACK-确认

[0142] ASIC-专用集成电路

[0143] CAN-控制器局域网

[0144] CBFF-经典基本帧格式

[0145] CSMA-载波感测多路访问

[0146] CEFF-经典扩展帧格式

[0147] CPLD-复杂可编程逻辑器件

[0148] CRC-循环冗余校验

[0149] DLC-数据长度代码

[0150] DSO-拒绝服务

[0151] DSP-数字信号处理器

[0152] DVD-数字通用光盘

[0153] ECU-电子控制单元

[0154] EF-错误标记

[0155] EOF-帧结束

[0156] FBFF-灵活数据速率基本帧格式

[0157] FDF-灵活数据速率帧

[0158] FEFF-灵活数据速率扩展帧格式

[0159] FET-场效应晶体管

[0160] FPGA-现场可编程门阵列

[0161] IDE-标识符扩展

[0162] IC-集成电路

[0163] ISO-国际标准组织

[0164] OBD-板载诊断

[0165] RAM-随机存取存储器

[0166] RRS-远程请求替代

[0167] RTR-远程传输请求

[0168] RXD-接收数据

[0169] SBC-系统基本芯片

[0170] SOF-帧开始

[0171] SRR-替代远程请求

[0172] TXD-传输数据

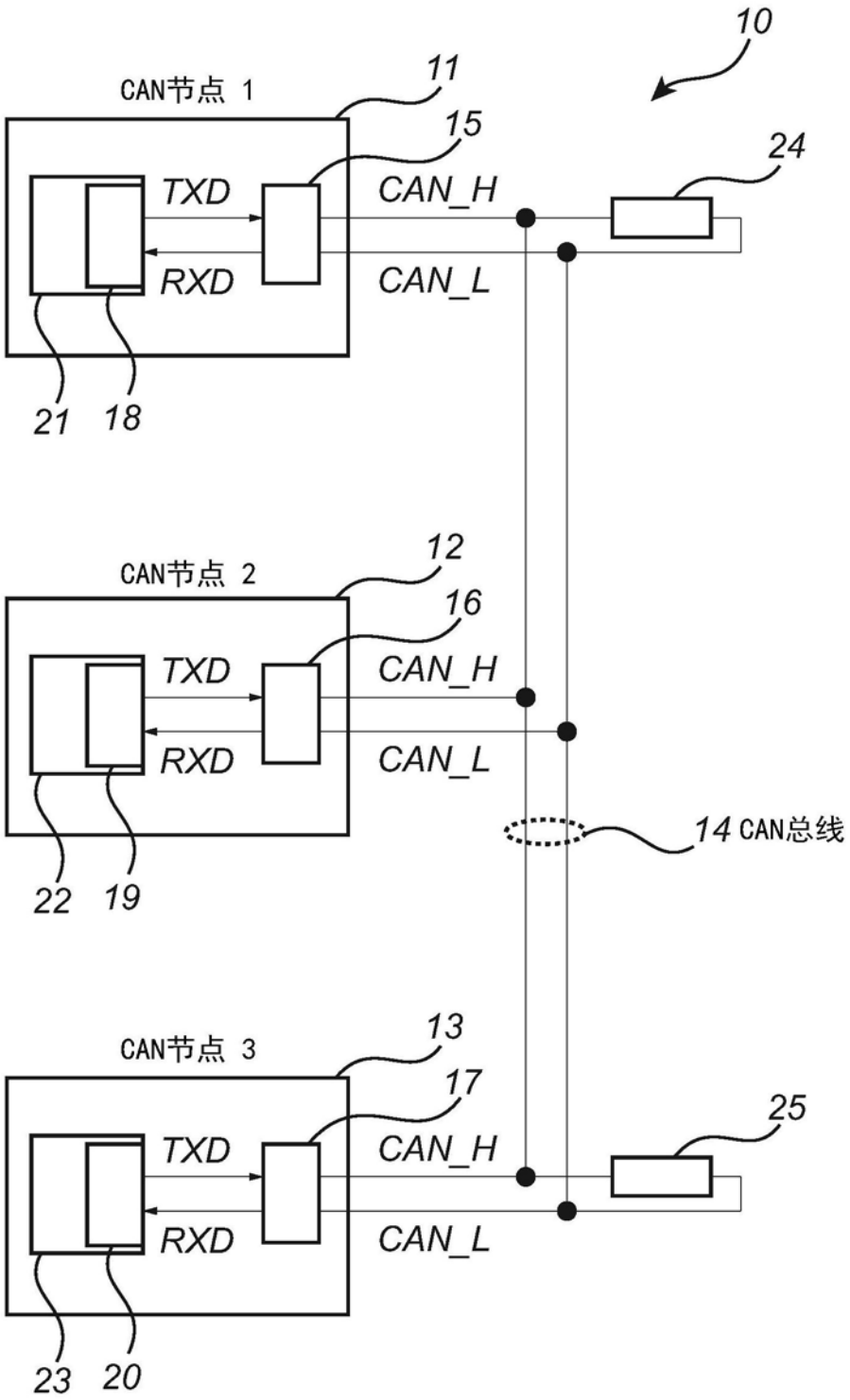

10
CAN节点 1
11
15
24
TXD
CAN_H
RXD
CAN_L
21
18
CAN节点 2
12
16
TXD
CAN_H
RXD
CAN_L
14 CAN总线
22
19
CAN节点 3
13
17
25
TXD
CAN_H
RXD
CAN_L
23
20

图1

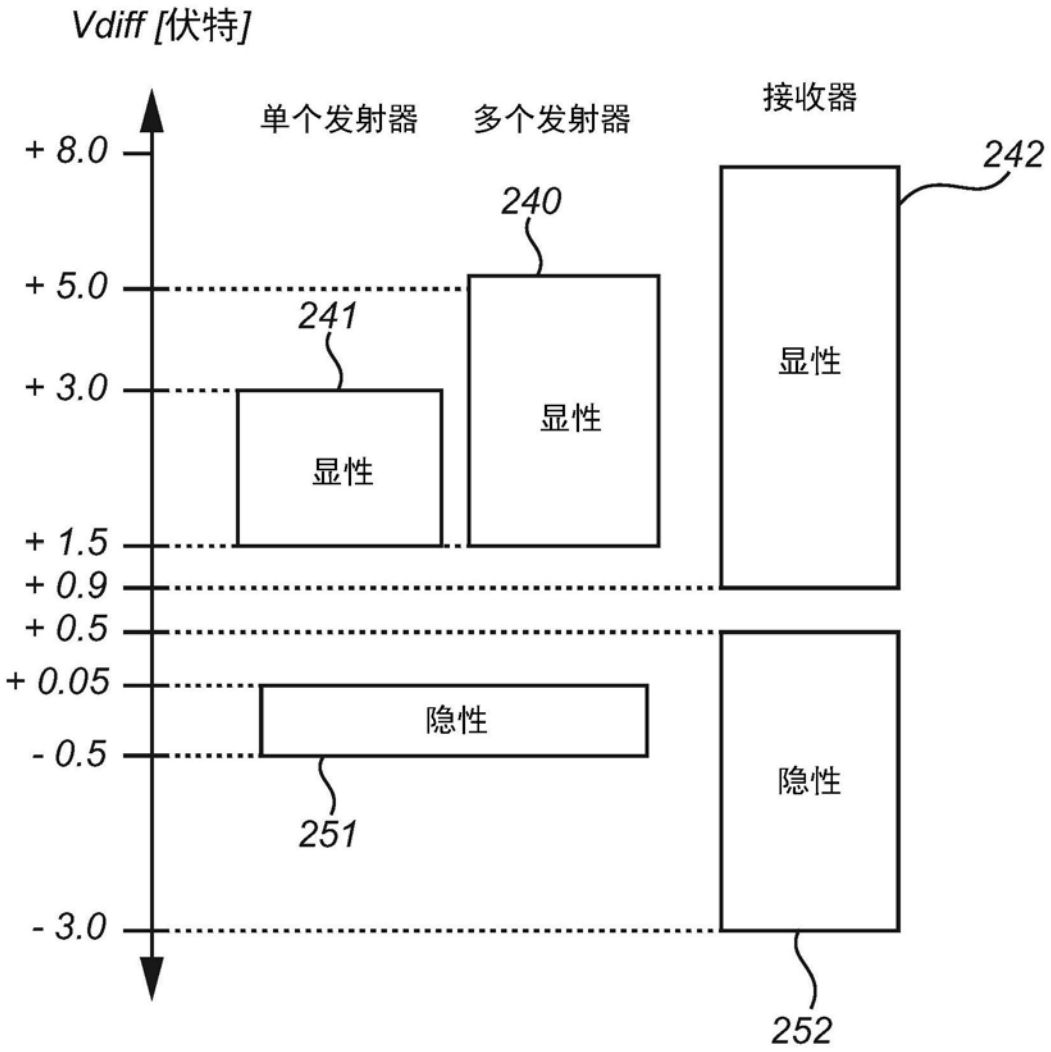

Vdiff [伏特]
单个发射器
多个发射器
接收器
+ 8.0
+ 5.0
+ 3.0
+ 1.5
+ 0.9
+ 0.5
+ 0.05
- 0.5
- 3.0
240
241
242
显性
显性
显性
隐性
隐性
251
252

图2

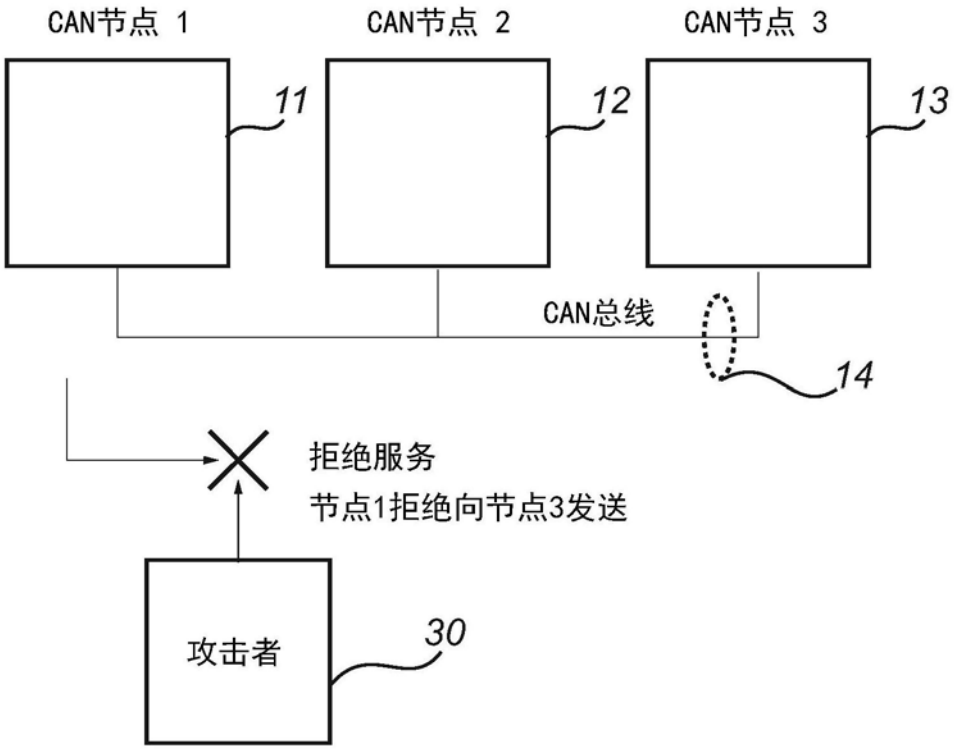

CAN节点 1
CAN节点 2
CAN节点 3
11
12
13
CAN总线
14
拒绝服务
节点1拒绝向节点3发送
攻击者
30

图3

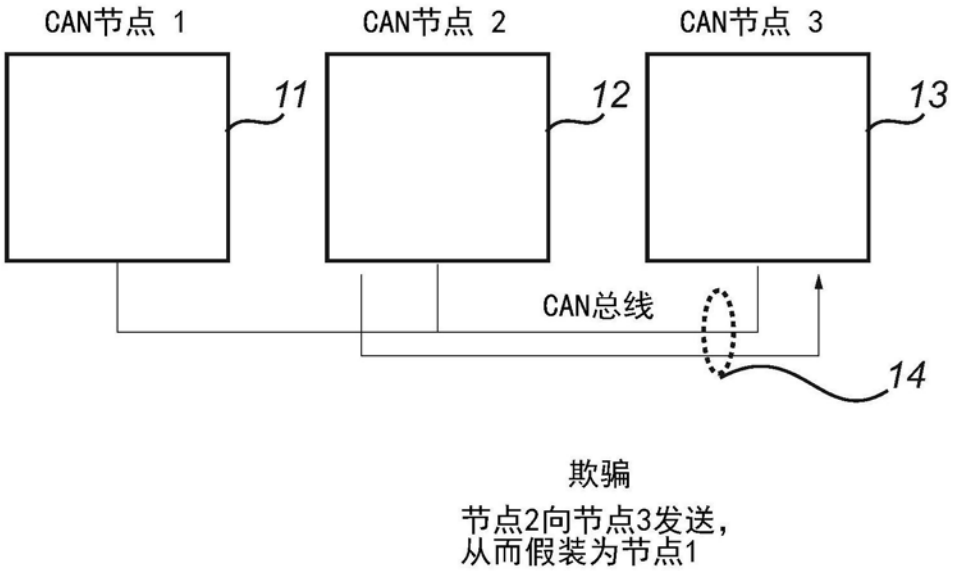

CAN节点 1
CAN节点 2
CAN节点 3
11
12
13
CAN总线
14
欺骗
节点2向节点3发送，
从而假装为节点1

图4

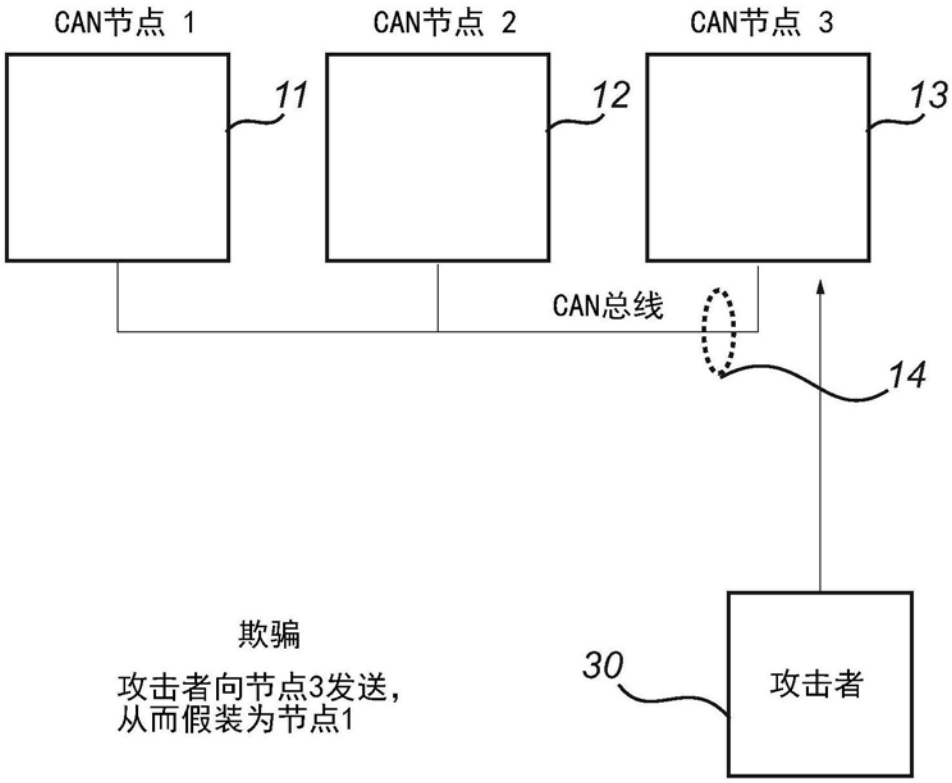

CAN节点 1
CAN节点 2
CAN节点 3
11
12
13
CAN总线
14
欺骗
攻击者向节点3发送，
从而假装为节点1
30
攻击者

图5

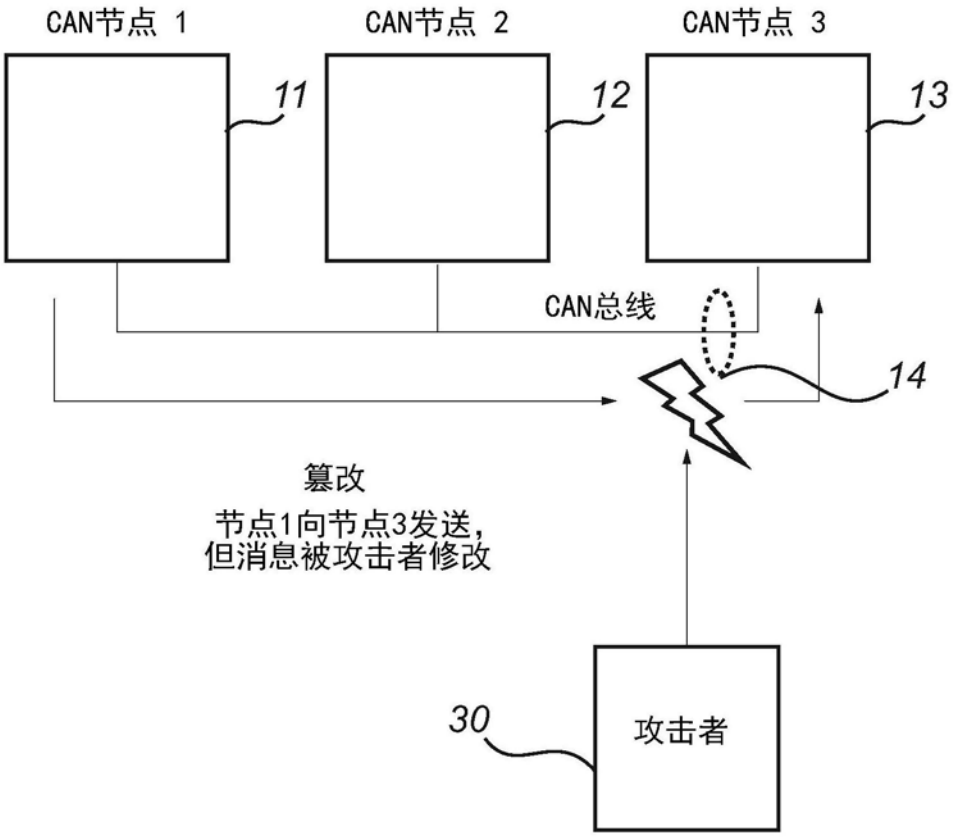

CAN节点 1
CAN节点 2
CAN节点 3
11
12
13
CAN总线
14
篡改
节点1向节点3发送，
但消息被攻击者修改
30
攻击者

图6

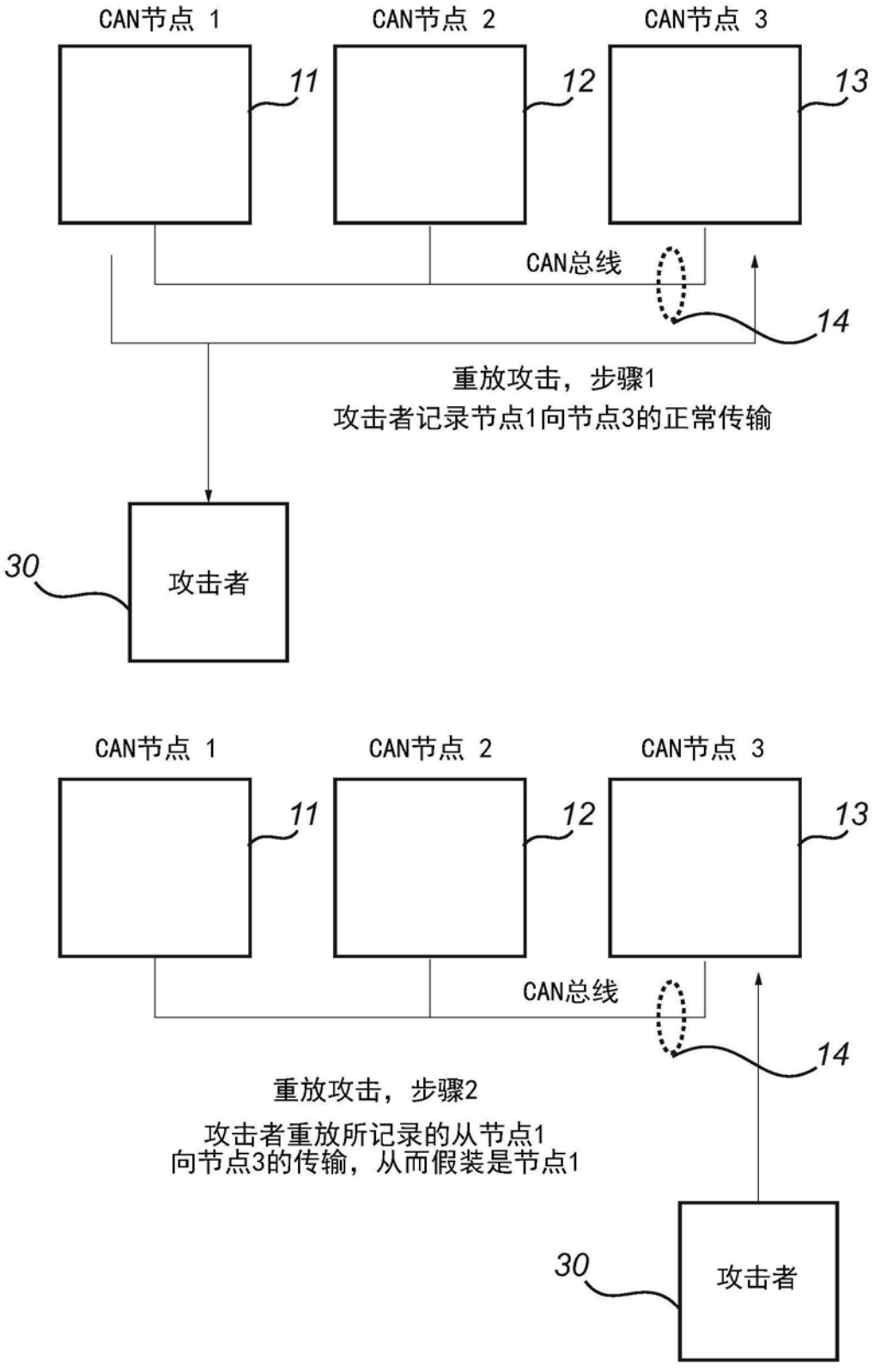

CAN节点 1
CAN节点 2
CAN节点 3
11
12
13
CAN总线
14
重放攻击，步骤1
攻击者记录节点1向节点3的正常传输
30
攻击者
CAN节点 1
CAN节点 2
CAN节点 3
11
12
13
CAN总线
14
重放攻击，步骤2
攻击者重放所记录的从节点1
向节点3的传输，从而假装是节点1
30
攻击者

图7

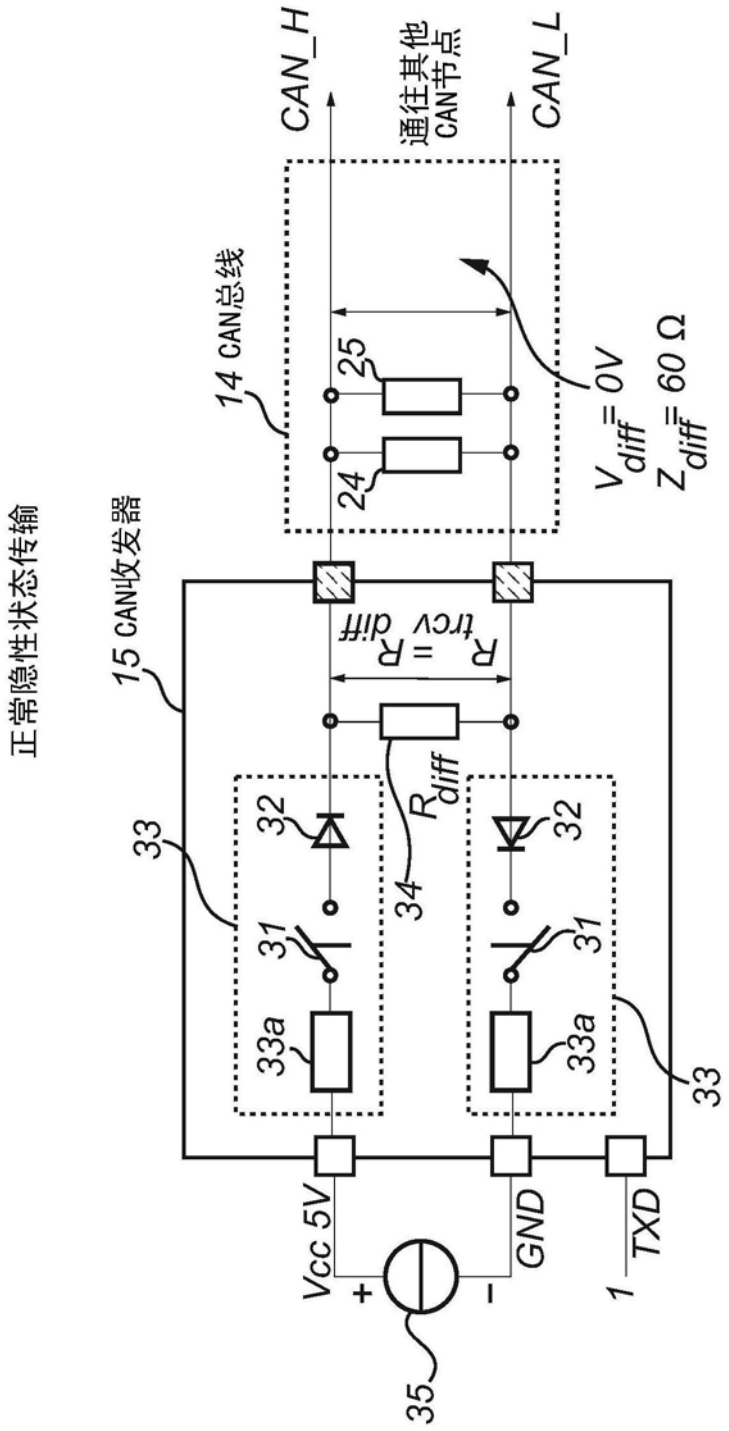

正常隐性状态传输
15 CAN收发器
14 CAN总线
CAN_H
CAN_L
通往其他CAN节点
25
24
V_{diff} = 0V
Z_{diff} = 60 Ω
R_{trcv_diff} = R_{diff}
R_{diff}
32
31
33a
33
34
Vcc 5V
GND
TXD
1
35

图8a

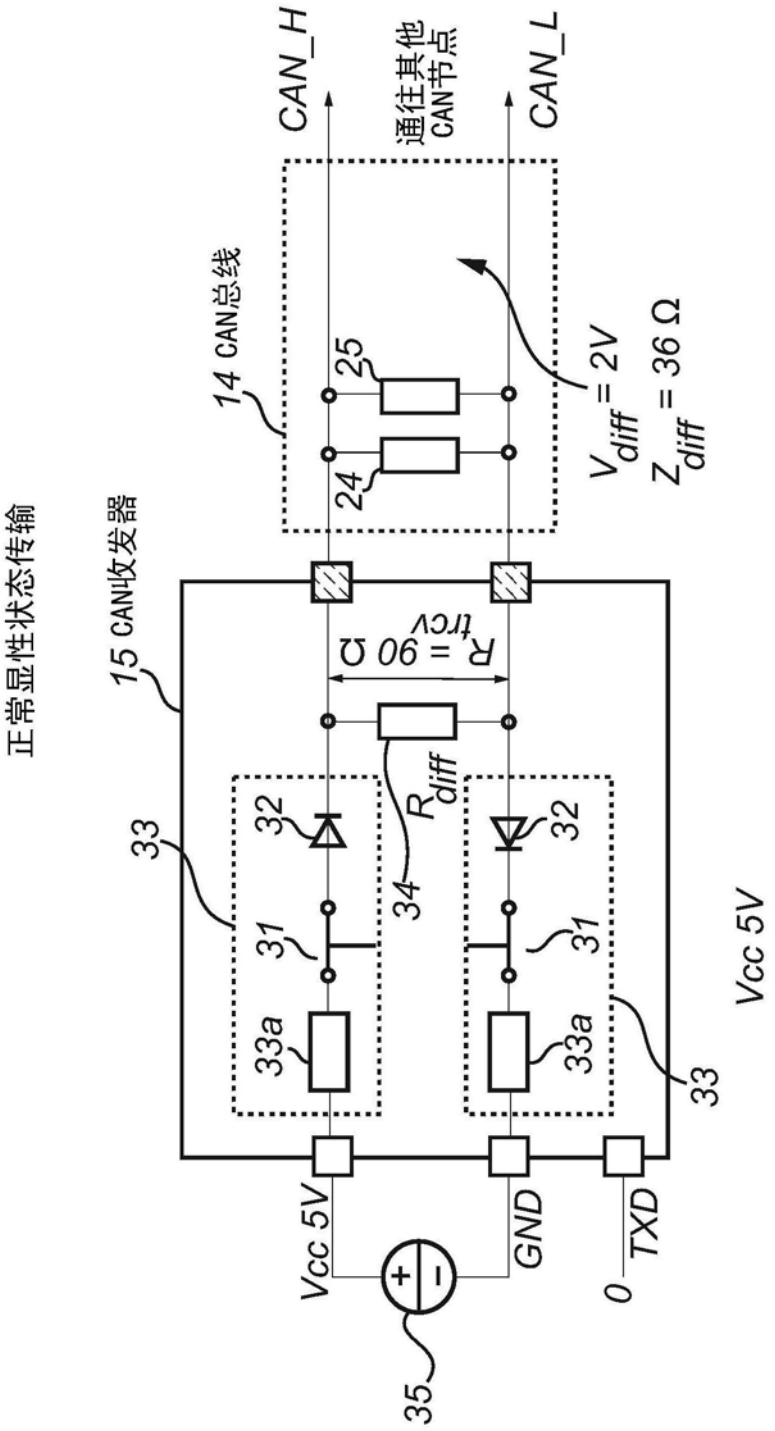

正常显性状态传输
15 CAN收发器
14 CAN总线
CAN_H
CAN_L
通往其他CAN节点
25
24
V_{diff} = 2V
Z_{diff} = 36 Ω
R_{trcv} = 90 Ω
R_{diff}
32
31
33a
33
34
35
Vcc 5V
GND
TXD
0

图8b

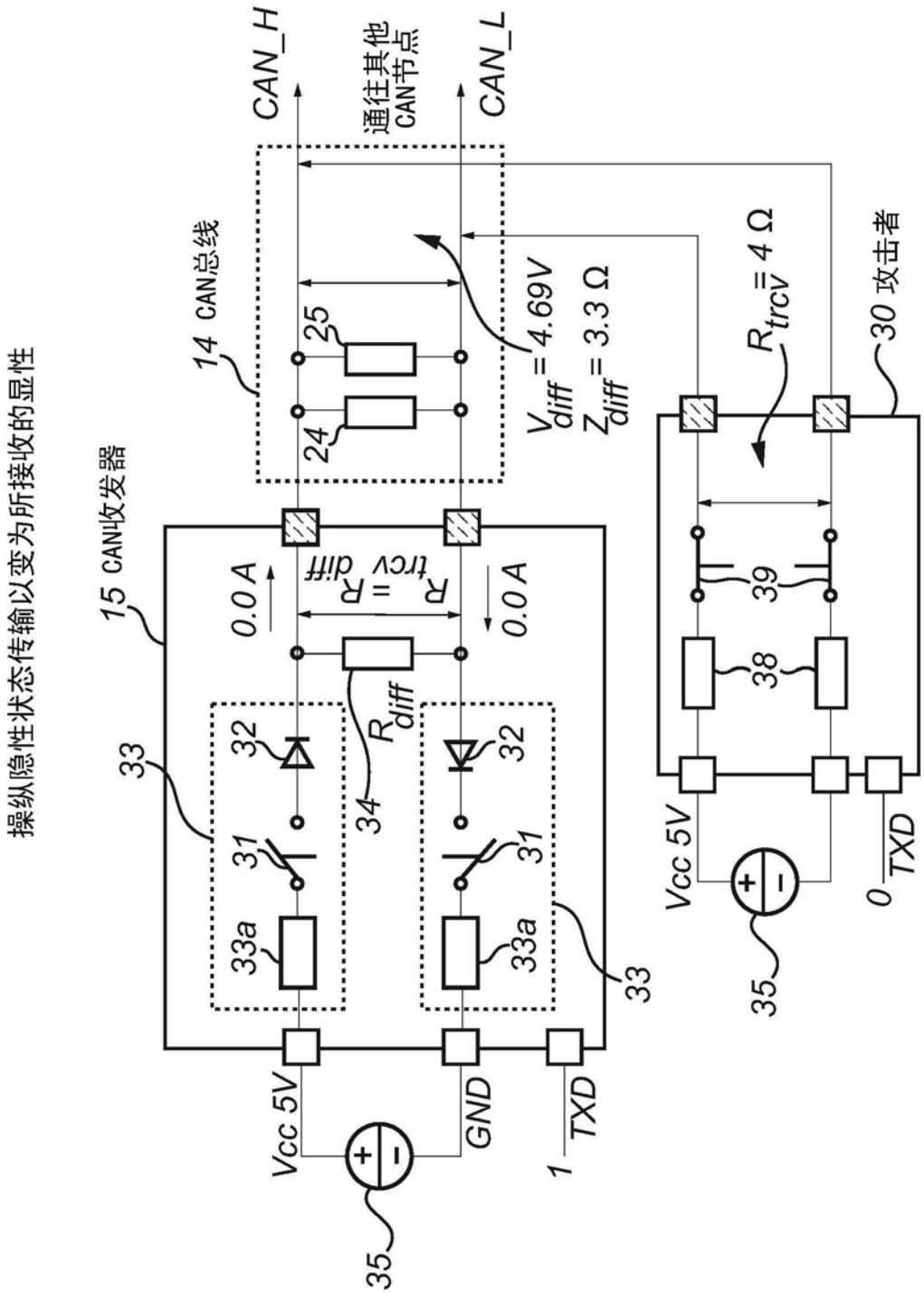

操纵隐性状态传输以变为所接收的显性
CAN_H
CAN_L
通往其他CAN节点
14 CAN总线
15 CAN收发器
25
24
V_{diff} = 4.69V
Z_{diff} = 3.3 Ω
R_{trcv} = 4 Ω
30 攻击者
0.0 A
0.0 A
R_{trcv_diff}
R_{diff}
32
32
31
31
33a
33a
33
33
34
39
38
Vcc 5V
Vcc 5V
GND
1 TXD
0 TXD
35
35

图9a

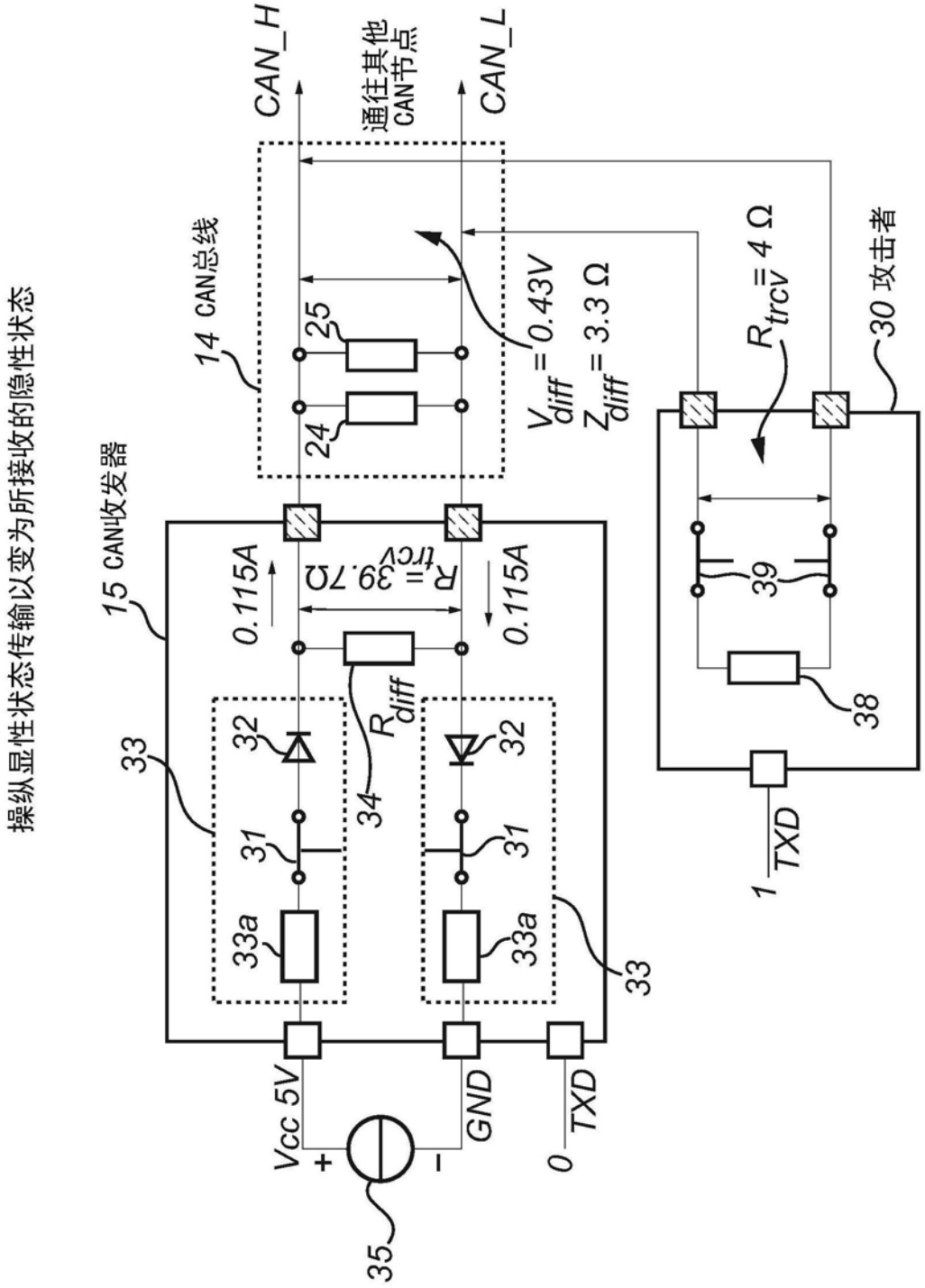

操纵显性状态传输以变为所接收的隐性状态
CAN_H
通往其他CAN节点
CAN_L
14 CAN总线
25
24
V_{diff} = 0.43V
Z_{diff} = 3.3 Ω
R_{trcV} = 4 Ω
30 攻击者
15 CAN收发器
0.115A
R_{trcV} < 39.7Ω
0.115A
R_{diff}
39
38
33
32
34
31
33a
Vcc 5V
GND
TXD
35
1
0

图9b

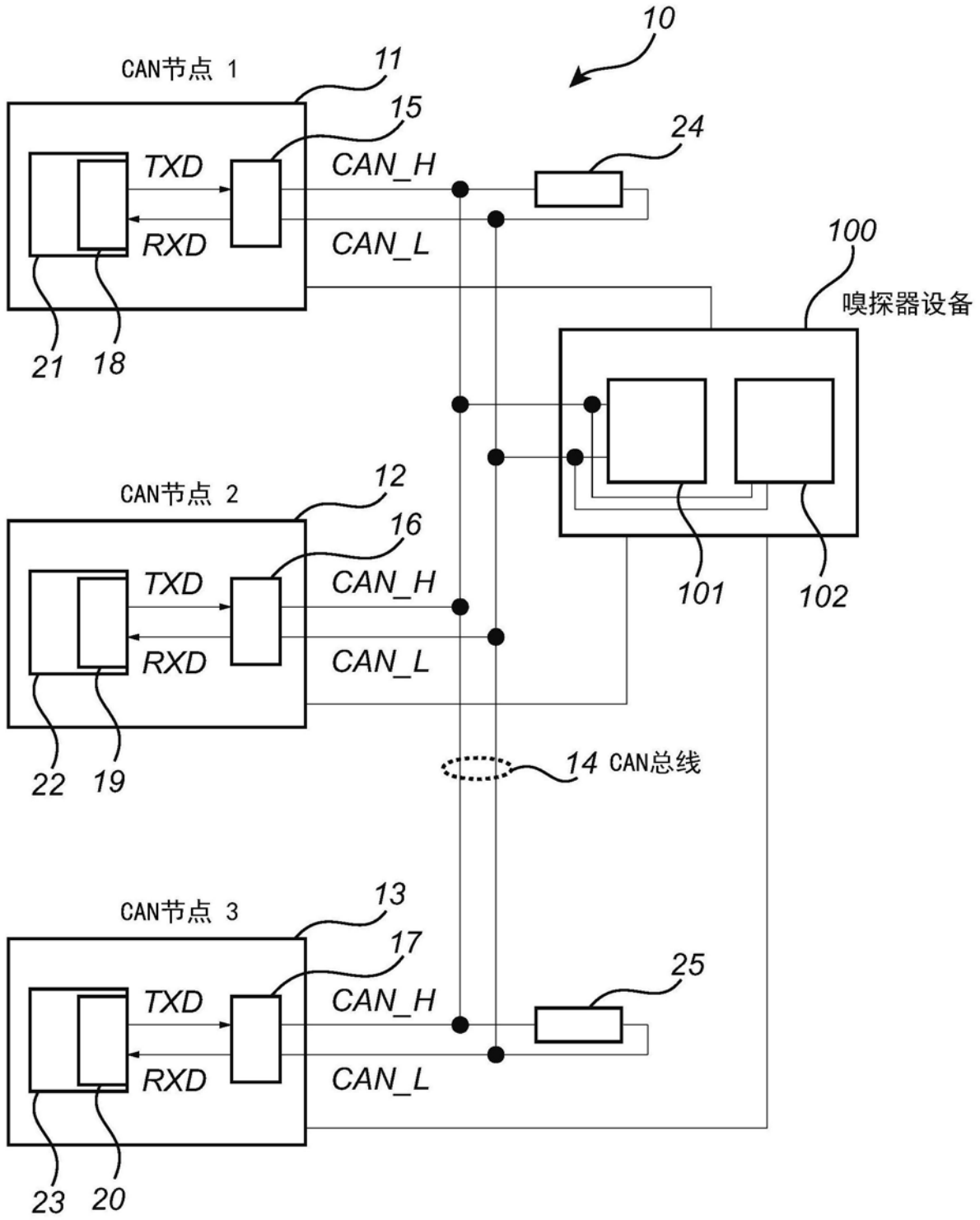

10
CAN节点 1
11
15
TXD
RXD
CAN_H
CAN_L
24
100
嗅探器设备
21
18
CAN节点 2
12
16
TXD
RXD
CAN_H
CAN_L
101
102
22
19
14 CAN总线
CAN节点 3
13
17
TXD
RXD
CAN_H
CAN_L
25
23
20

图10a

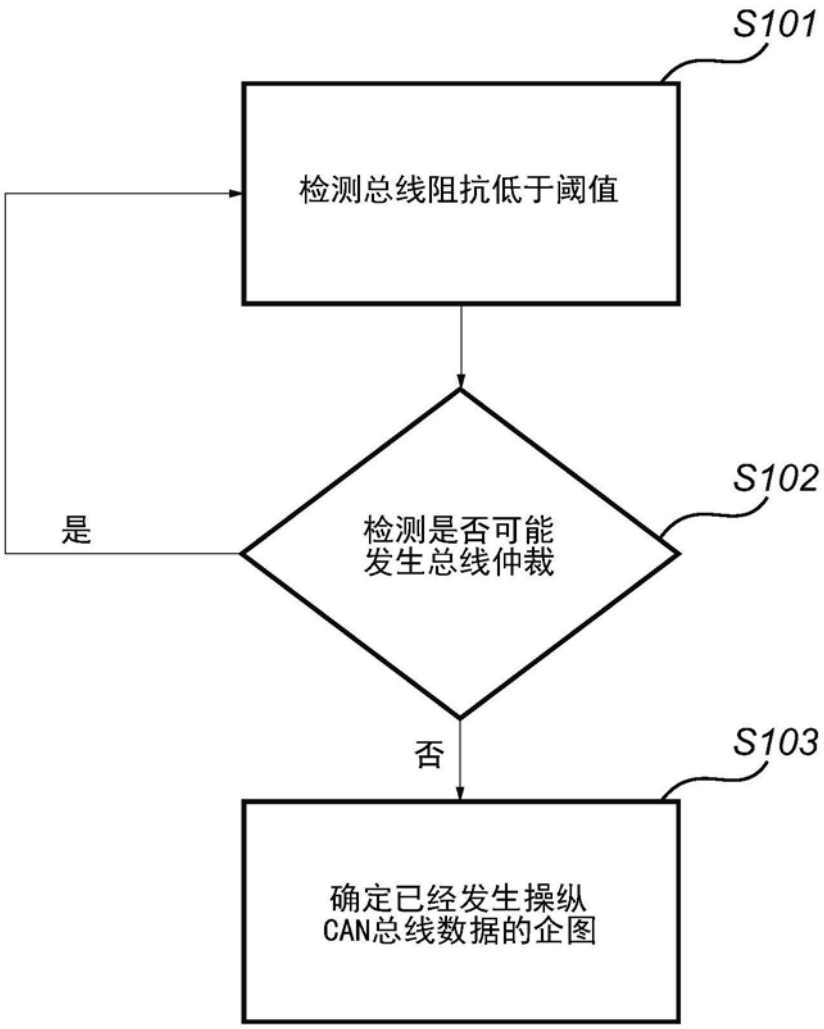

S101
检测总线阻抗低于阈值
S102
检测是否可能
发生总线仲裁
是
否
S103
确定已经发生操纵
CAN总线数据的企图

图10b

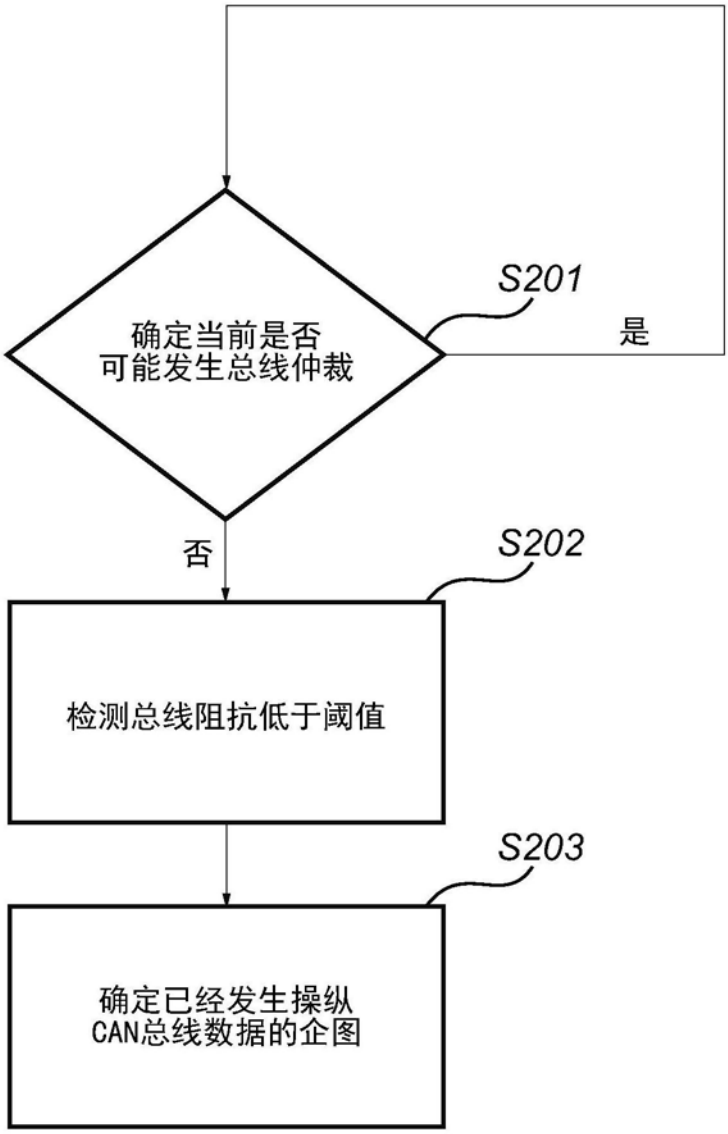

S201
确定当前是否
可能发生总线仲裁
是
否
S202
检测总线阻抗低于阈值
S203
确定已经发生操纵
CAN总线数据的企图

图10c

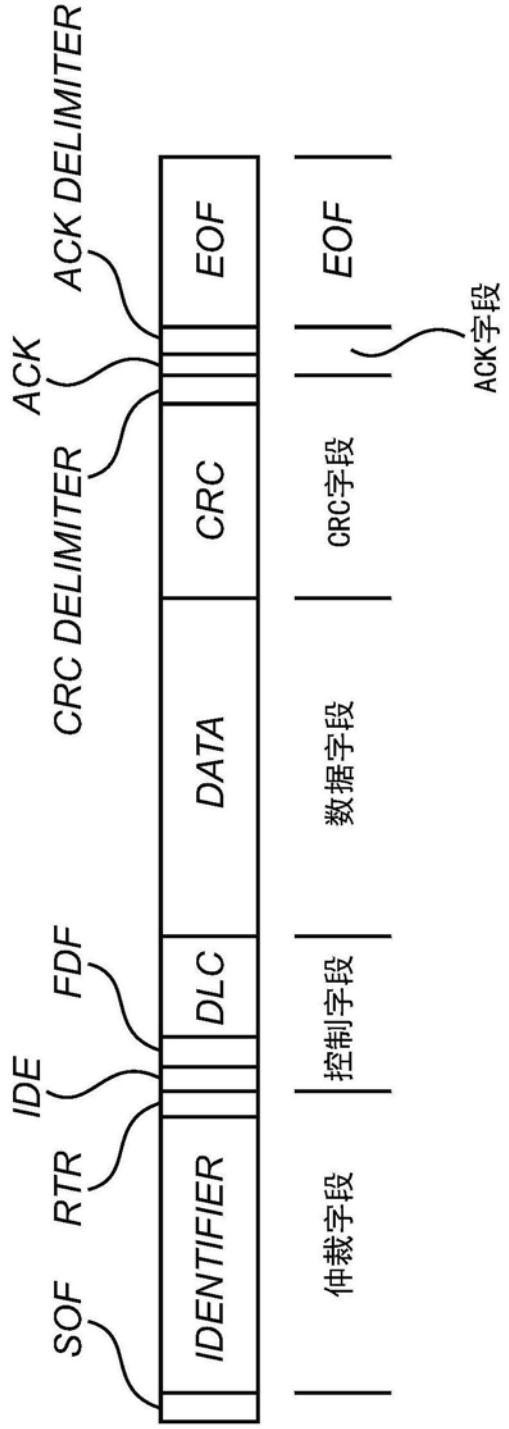

SOF
IDENTIFIER
RTR
IDE
FDF
DLC
DATA
CRC DELIMITER
CRC
ACK
ACK DELIMITER
EOF
仲裁字段
控制字段
数据字段
CRC字段
ACK字段
EOF

图11

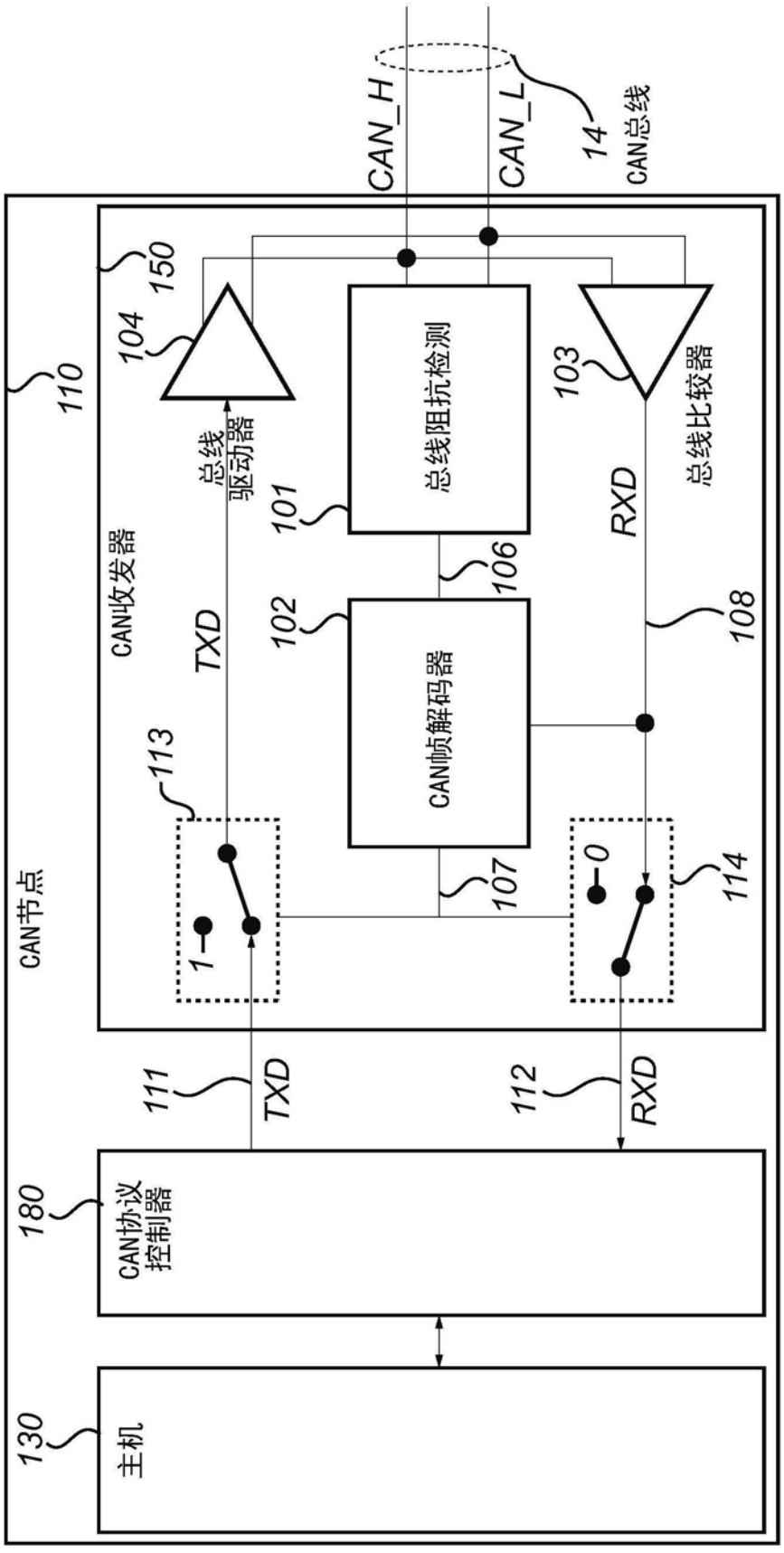

CAN_H
CAN_L
14
CAN总线
150
104
110
总线驱动器
101
总线阻抗检测
103
总线比较器
CAN收发器
TXD
102
106
RXD
108
CAN帧解码器
113
107
114
CAN节点
1
0
111
TXD
112
RXD
180
CAN协议控制器
130
主机

图12

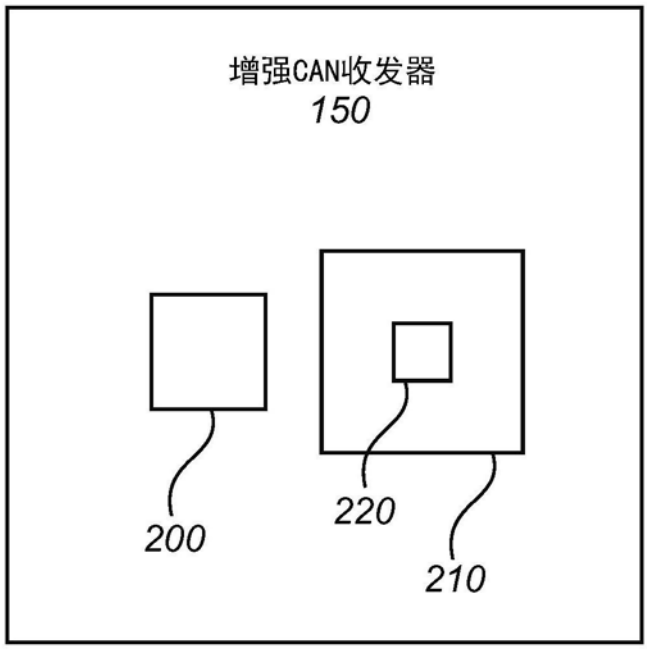


图13