(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 107547572 B
(45)授权公告日 2021.03.02

(21)申请号 201710950454.9

(22)申请日 2017.10.13

(65)同一申请的已公布的文献号
申请公布号 CN 107547572 A

(43)申请公布日 2018.01.05

(73)专利权人 北京梆梆安全科技有限公司
地址 100083 北京市海淀区学院路30号天工大厦A座20层

(72)发明人 阚志刚 卢佐华 裴元奇 彭建芬 陈彪

(74)专利代理机构 北京三友知识产权代理有限公司 11127
代理人 贾磊

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 12/40(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 104796430 A,2015.07.22
CN 104464057 A,2015.03.25

审查员 谭美玲

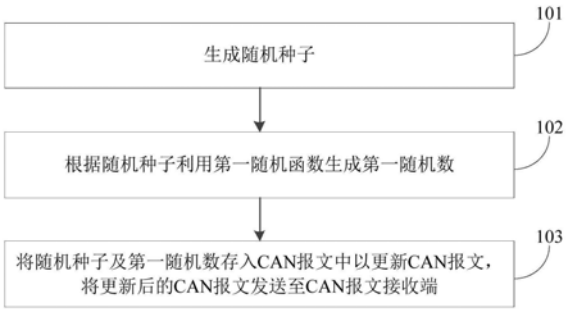
权利要求书1页 说明书6页 附图3页

(54)发明名称

一种基于伪随机数的CAN总线通信方法

(57)摘要

本申请提供了一种基于伪随机数的CAN总线通信方法，包括：CAN报文发送端用于生成随机种子；根据随机种子利用第一随机函数生成第一随机数；将随机种子及第一随机数存入CAN报文中以更新CAN报文，将更新后的CAN报文发送至CAN报文接收端。CAN报文接收端用于接收CAN报文发送端发送的CAN报文；解析CAN报文得到随机种子及第一随机数，根据随机种子利用第一随机函数生成第一随机数；判断生成的第一随机数与解析得到的第一随机数是否相同，如果相同，则响应CAN报文。本申请通过在CAN报文中存入随机生成的随机种子及第一随机数，能够保证每个CAN报文都不同，从而使得CAN报文不具有预见性，能够防止伪造攻击，具有安全性高的特点。



CN 107547572 B

1.一种基于伪随机数的CAN总线通信方法,其特征在于,适用于CAN报文发送端,包括:

生成随机种子;

根据随机种子利用第一随机函数生成第一随机数,根据第一随机数利用第二随机函数生成第二随机数,所述第一随机函数和所述第二随机函数不同;将第一随机数及第二随机数存入CAN报文中以更新CAN报文,将更新后的CAN报文发送至CAN报文接收端。

2.如权利要求1所述的方法,其特征在于,生成随机种子的过程包括:

随机生成一随机数;

获取CAN报文发送端所在设备的模拟量参数;

组合所述随机数与所述模拟量参数得到随机种子。

3.如权利要求1所述的方法,其特征在于,生成随机种子的过程包括:

获取系统时间戳;

获取CAN报文发送端所在设备的模拟量参数;

组合所述时间戳与所述模拟量参数得到随机种子。

4.如权利要求2或3所述的方法,其特征在于,模拟量参数包括车辆VIN、CAN报文发送端设备的实时电压、实时温度及实时湿度中的一个或多个。

5.一种基于伪随机数的CAN总线通信方法,其特征在于,适用于CAN报文接收端,包括:

接收CAN报文发送端发送的CAN报文;

解析CAN报文得到第一随机数及第二随机数,根据第一随机数利用第二随机函数生成第二随机数,所述第一随机数由随机种子通过第一随机函数得到,所述第一随机函数和所述第二随机函数不同;

判断生成的第二随机数与解析得到的第二随机数是否相同,若生成的第二随机数与解析得到的第二随机数相同,则响应CAN报文。

一种基于伪随机数的CAN总线通信方法

技术领域

[0001] 本申请属于CAN总线通信领域，尤其涉及一种基于伪随机数的CAN总线通信方法。

背景技术

[0002] 现有技术中，防止CAN总线攻击的方式为CAN总线滚动码机制，CAN总线滚动码机制多为等差或等比方式变化，即采用等差或等比方式生成一序列，发送报文时按顺序从序列中提取数值放入报文中。

[0003] 上述防止CAN总线攻击的方式存在如下缺陷：

[0004] 1)具有可预见性和可推导性，安全性不高，攻击者通过对滚动码变化规律的学习，可轻松实现伪造攻击。

[0005] 2)对于丢包、延迟的情况会出现误判。

发明内容

[0006] 本申请提供一种基于伪随机的CAN总线通信方法，用于解决现有技术中CAN总线通信存在易被攻击，安全性不高，对于丢包及延迟的情况会出现错误判断或误判的问题。

[0007] 为了解决上述技术问题，本申请一实施例中，基于伪随机数的CAN总线通信方法包括：

[0008] CAN报文发送端用于生成随机种子；根据随机种子利用第一随机函数生成第一随机数；将随机种子及第一随机数存入CAN报文中以更新CAN报文，将更新后的CAN报文发送至CAN报文接收端；

[0009] CAN报文接收端用于接收CAN报文发送端发送的CAN报文；解析CAN报文得到随机种子及第一随机数，根据随机种子利用第一随机函数生成第一随机数；判断生成的第一随机数与解析得到的第一随机数是否相同，若生成的第一随机数与解析得到的第一随机数相同，则响应CAN报文。

[0010] 本申请另一实施例中，基于伪随机数的CAN总线通信方法，包括：

[0011] CAN报文发送端用于生成随机种子；根据随机种子利用第一随机函数生成第一随机数；根据第一随机数按预定校验准则生成校验信息；将随机种子、第一随机数及校验信息存入CAN报文中以更新CAN报文，将更新后的CAN报文发送至CAN报文接收端；

[0012] CAN报文接收端用于接收CAN报文发送端发送的CAN报文；解析CAN报文得到随机种子、第一随机数及校验信息；根据随机种子利用第一随机函数生成第一随机数；判断生成的第一随机数与解析得到的第一随机数是否相同，若生成的第一随机数与解析得到的第一随机数相同，则响应CAN报文；若生成的第一随机数与解析得到的第一随机数不同，则根据计算得到的第一随机数利用预定校验准则生成校验信息，判断生成的校验信息与解析得到的校验信息是否相同，若生成的校验信息与解析得到的校验信息相同，则响应CAN报文。

[0013] 本申请另一实施例中，基于伪随机数的CAN总线通信方法，包括：

[0014] CAN报文发送端用于生成随机种子；根据随机种子利用第一随机函数生成第一随

机数，根据第一随机数利用第二随机函数生成第二随机数；将第一随机数及第二随机数存入CAN报文中以更新CAN报文，将更新后的CAN报文发送至CAN报文接收端。

[0015] CAN报文接收端用于接收CAN报文发送端发送的CAN报文；解析CAN报文得到第一随机数及第二随机数，根据第一随机数利用第二随机函数生成第二随机数；判断生成的第二随机数与解析得到的第二随机数是否相同，若生成的第二随机数与解析得到的第二随机数相同，则响应CAN报文。

[0016] 本申请通过在CAN报文中存入随机种子及第一随机数，或在CAN报文中存入第一随机数或第二随机数的方式，能够保证每个CAN报文都不同，因随机种子、第一随机数、第二随机数是随机生成的，从而使得CAN报文不具有预见性和可推到性，能够防止伪造攻击，具有安全性高的特点。

附图说明

[0017] 为了更清楚地说明本申请实施例中的技术方案，下面将对实施例描述中所需要使用的附图作简单地介绍，显而易见地，下面描述中的附图仅仅是本申请的一些实施例，对于本领域普通技术人员来讲，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。

[0018] 图1A为本申请实施例的从CAN报文发送端描述的基于伪随机数的CAN总线通信方法流程图；

[0019] 图1B为本申请实施例的从CAN报文接收端描述的基于伪随机数的CAN总线通信方法流程图；

[0020] 图2为本申请实施例的随机种子生成过程流程图；

[0021] 图3A为本申请另一实施例的从CAN报文发送端描述的基于伪随机数的CAN总线通信方法流程图；

[0022] 图3B为本申请另一实施例的从CAN报文接收端描述的基于伪随机数的CAN总线通信方法流程图；

[0023] 图4为本申请实施例的基于伪随机数的CAN总线通信系统的结构图。

具体实施方式

[0024] 为了使本申请的技术特点及效果更加明显，下面结合附图对本申请的技术方案做进一步说明，本申请也可有其他不同的具体实例来加以说明或实施，任何本领域技术人员在权利要求范围内做的等同变换均属于本申请的保护范畴。

[0025] 在本说明书的描述中，参考术语“一实施例”、“一具体实施例”、“一实施方式”或“例如”等的描述意指结合该实施例或示例描述的具体特征、结构或者特点包含于本申请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一定指的是相同的实施例或示例。而且，描述的具体特征、结构或者特点可以在任何的一个或多个实施例或示例中以合适的方式结合。各实施例中涉及的步骤顺序用于示意性说明本申请的实施，其中的步骤顺序不作限定，可根据需要作适当调整。

[0026] 如图1A所示，图1A为本申请实施例的从CAN报文发送端描述的基于伪随机数的CAN总线通信方法流程图。具体的，CAN报文发送端的处理流程包括：

[0027] 步骤101,生成随机种子;

[0028] 步骤102,根据随机种子利用第一随机函数生成第一随机数;

[0029] 步骤103,将随机种子及第一随机数存入CAN报文中以更新CAN报文,将更新后的CAN报文发送至CAN报文接收端。

[0030] 详细的说,第一随机函数可以为现有技术中任意生成随机数的函数,本申请对第一随机函数具体为何不做限定。

[0031] 如图1B所示,图1B为本申请实施例的从CAN报文接收端描述的基于伪随机数的CAN总线通信方法流程图。具体的,CAN报文接收端的处理流程包括:

[0032] 步骤104,接收CAN报文发送端发送的CAN报文;

[0033] 步骤105,解析CAN报文得到随机种子及第一随机数,根据随机种子利用第一随机函数生成第一随机数;

[0034] 步骤106,判断生成的第一随机数与解析得到的第一随机数是否相同,若生成的第一随机数与解析得到的第一随机数相同,则响应CAN报文,如果不同,则上报异常信息。

[0035] 详细的说,步骤105中的第一随机函数与步骤102中的第一随机函数相同,由CAN报文发送端与CAN报文接收端预先约定。

[0036] 图1A所示流程与图1B所示流程配合使用,在CAN报文中加入随机生成的随机种子及第一随机函数,能够保证每个CAN报文都不同,使CAN报文不具有预见性和可推到性,能够防止伪造攻击,具有安全性高的特点。另外,通过步骤101～步骤103生成CAN报文、步骤104～步骤106验证CAN报文的方式不会出现因丢包、延迟导致误判的问题。

[0037] 本申请一实施例中,为了避免CAN报文传输过程中因第一随机数发生错误而无法正常响应CAN报文,上述步骤102中还包括根据第一随机数按预定校验准则(如CRC校验准则)生成校验信息,上述步骤103进一步为将随机种子、第一随机数及校验信息存入CAN报文中以更新CAN报文,将更新后的CAN报文发送至CAN报文接收端。

[0038] CAN报文接收端接收到包含校验信息的CAN报文后进行如下处理:解析CAN报文得到随机种子、第一随机数及校验信息;根据随机种子利用第一随机函数生成第一随机数;判断生成的第一随机数与解析得到的第一随机数是否相同,若生成的第一随机数与解析得到的第一随机数相同,则响应CAN报文;若生成的第一随机数与解析得到的第一随机数不同(有可能因第一随机数传输过程中产生错误而不同),则根据计算得到的第一随机数利用预定校验准则生成校验信息,判断生成的校验信息与解析得到的校验信息是否相同,若生成的校验信息与解析得到的校验信息相同,则响应CAN报文。

[0039] 本申请一具体实施例中,如图2所示,上述步骤101生成随机种子的过程包括:

[0040] 步骤201,随机生成一随机数;

[0041] 步骤202,获取CAN报文发送端所在设备的模拟量参数;

[0042] 步骤203,组合所述随机数与所述模拟量参数得到随机种子。

[0043] 详细的说,模拟量参数包括车辆VIN,CAN报文发送端设备的实时电压、实时温度及实时湿度中的一个或多个。因CAN报文发送端设备的实时电压、实时温度或实时湿度是不断变化的,且无规律可循,所以通过将随机数与设备模拟量参数组合在一起得到随机种子的方式能够提高随机种子的随机性,有效防止伪造攻击。攻击者即使截获CAN报文也无法通过学习得到随机种子的产生规律。

[0044] 本申请其它实施例中，还可采用如下方式生成随机种子：获取系统时间戳；获取CAN报文发送端所在设备的模拟量参数；组合所述时间戳与所述模拟量参数得到随机种子。

[0045] 本申请另一实施例中，为了防止随机种子暴露，可采用根据随机种子生成的随机数来替代随机种子的方式来隐藏随机种子。具体的，如图3A及图3B所示。

[0046] 图3A为本申请另一实施例的从CAN报文发送端描述的基于伪随机数的CAN总线通信方法流程图。具体的，CAN报文发送端的处理流程包括：

[0047] 步骤301，生成随机种子；

[0048] 步骤302，根据随机种子利用第一随机函数生成第一随机数，根据第一随机数利用第二随机函数生成第二随机数；

[0049] 步骤303，将第一随机数及第二随机数存入CAN报文中以更新CAN报文，将更新后的CAN报文发送至CAN报文接收端。

[0050] 详细的说，第一随机函数及第二随机函数可以为现有技术中任一生成随机数的函数，本申请对第一随机函数及第二随机函数为何不做限定。具体实施时，第一随机函数与第二随机函数可以相同，也可以不同。

[0051] 图3B为本申请另一实施例的从CAN报文接收端描述的基于伪随机数的CAN总线通信方法流程图。具体的，CAN报文发送端的处理流程包括：

[0052] 步骤304，接收CAN报文发送端发送的CAN报文；

[0053] 步骤305，解析CAN报文得到第一随机数及第二随机数，根据第一随机数利用第二随机函数生成第二随机数；

[0054] 步骤306，判断生成的第二随机数与解析得到的第二随机数是否相同，若生成的第二随机数与解析得到的第二随机数相同，则响应CAN报文。

[0055] 详细的说，步骤305中的第二随机函数与步骤102中的第二随机函数相同，由CAN报文发送端与CAN报文接收端预先约定。

[0056] 图3A所示流程与图3B所示流程配合使用，在CAN报文中加入随机生成的第一随机数及第二随机函数，能够保证每个CAN报文都不同，使CAN报文不具有预见性和可推到性，能够防止伪造攻击，具有安全性高的特点。另外，通过步骤301～步骤303生成CAN报文、步骤304～步骤306验证CAN报文的方式不会出现因丢包、延迟导致误判的问题。

[0057] 本申请其它实施例中，CAN报文发送端还可根据随机种子利用N个随机函数迭代生成N个随机数，将第N-1个及第N个随机数加入至CAN报文中；CAN报文接收端存储有第N个随机函数。例如，CAN报文发送端根据随机种子利用第一随机函数生成第一随机数，根据第一随机数利用第二随机函数生成第二随机数，根据第二随机数利用第三随机函数生成第三随机数，…，根据第N-1个随机数利用第N个随机函数生成第N个随机数，将第N个随机数及第N-1个随机数加入至CAN报文中；CAN报文接收端根据解析得到的第N-1个随机数利用第N个随机函数生成第N个随机数，判断生成的第N个随机数与解析得到的第N个随机数是否相同，如果相同，则响应CAN报文。

[0058] 如图4所示，图4为本申请实施例的基于伪随机数的CAN总线通信系统的结构图。具体的，基于伪随机数的CAN总线通信系统包括CAN报文发送端及CAN报文接收端。

[0059] 一具体实施方式中，CAN报文发送端用于生成随机种子；根据随机种子利用第一随机函数生成第一随机数；将随机种子及第一随机数存入CAN报文中以更新CAN报文，将更新

后的CAN报文发送至CAN报文接收端。CAN报文接收端用于接收CAN报文发送端发送的CAN报文;解析CAN报文得到随机种子及第一随机数,根据随机种子利用第一随机函数生成第一随机数;判断生成的第一随机数与解析得到的第一随机数是否相同,若生成的第一随机数与解析得到的第一随机数相同,则响应CAN报文。

[0060] 另一具体实施方式中,CAN报文发送端用于生成随机种子;根据随机种子利用第一随机函数生成第一随机数;根据第一随机数按预定校验准则生成校验信息;将随机种子、第一随机数及校验信息存入CAN报文中以更新CAN报文,将更新后的CAN报文发送至CAN报文接收端;

[0061] CAN报文接收端用于接收CAN报文发送端发送的CAN报文;解析CAN报文得到随机种子、第一随机数及校验信息;根据随机种子利用第一随机函数生成第一随机数;判断生成的第一随机数与解析得到的第一随机数是否相同,若生成的第一随机数与解析得到的第一随机数相同,则响应CAN报文;若生成的第一随机数与解析得到的第一随机数不同,则根据计算得到的第一随机数利用预定校验准则生成校验信息,判断生成的校验信息与解析得到的校验信息是否相同,若生成的校验信息与解析得到的校验信息相同,则响应CAN报文。

[0062] 再一具体实施方式中,CAN报文发送端用于生成随机种子;根据随机种子利用第一随机函数生成第一随机数,根据第一随机数利用第二随机函数生成第二随机数;将第一随机数及第二随机数存入CAN报文中以更新CAN报文,将更新后的CAN报文发送至CAN报文接收端。CAN报文接收端用于接收CAN报文发送端发送的CAN报文;解析CAN报文得到第一随机数及第二随机数,根据第一随机数利用第二随机函数生成第二随机数;判断生成的第二随机数与解析得到的第二随机数是否相同,若生成的第二随机数与解析得到的第二随机数相同,则响应CAN报文。

[0063] 本申请基于伪随机数的CAN总线通信系统通过在CAN报文中存入随机种子及第一随机数,或在CAN报文中存入第一随机数或第二随机数的方式,能够保证每个CAN报文都不同,因随机种子、第一随机数、第二随机数是随机生成的,从而使得CAN报文不具有预见性和可推到性,能够防止伪造攻击,具有安全性高的特点。

[0064] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0065] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器,使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0066] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中,使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品,该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或

多个方框中指定的功能。

[0067] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0068] 以上所述仅用于说明本申请的技术方案，任何本领域普通技术人员均可在不违背本申请的精神及范畴下，对上述实施例进行修饰与改变。因此，本申请的权利保护范围应视权利要求范围为准。

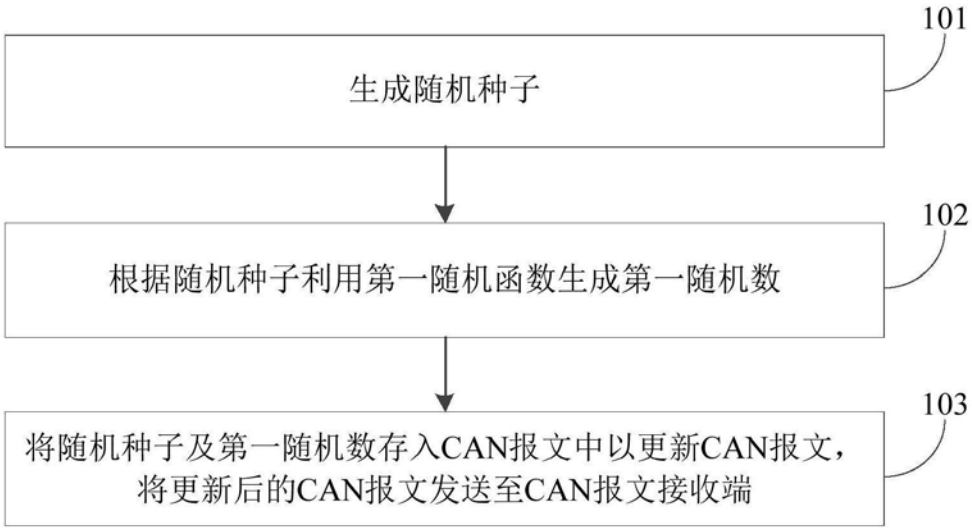

101
生成随机种子
102
根据随机种子利用第一随机函数生成第一随机数
103
将随机种子及第一随机数存入CAN报文中以更新CAN报文，
将更新后的CAN报文发送至CAN报文接收端

图1A

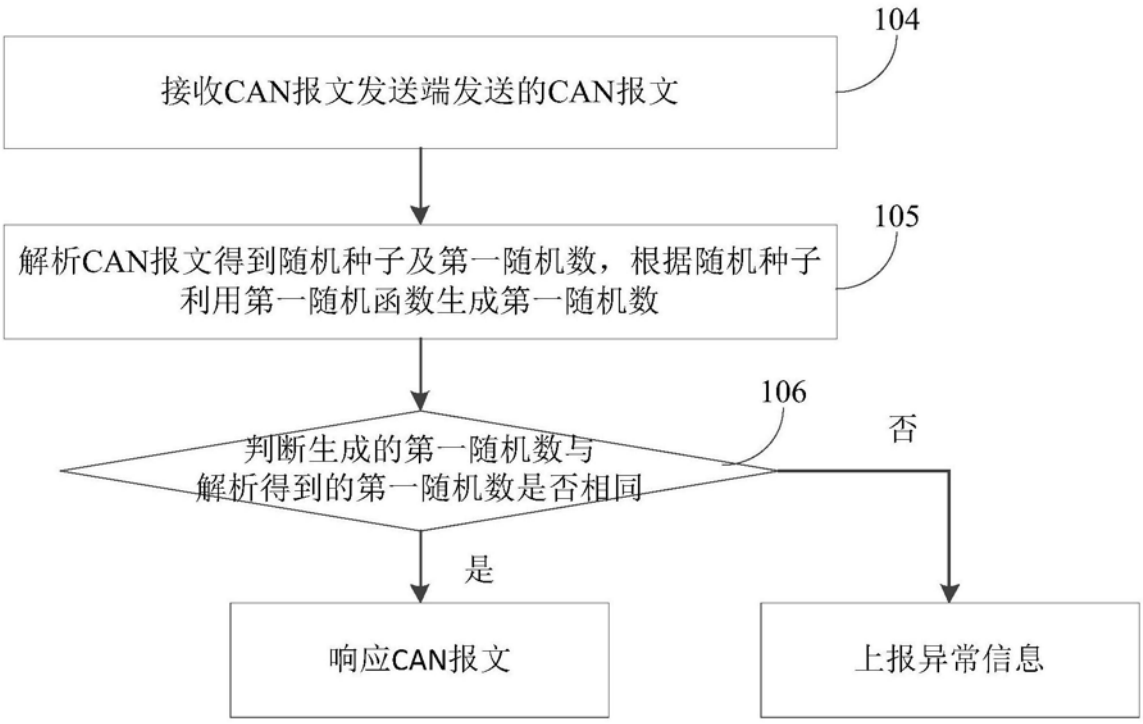

104
接收CAN报文发送端发送的CAN报文
105
解析CAN报文得到随机种子及第一随机数，根据随机种子
利用第一随机函数生成第一随机数
106
判断生成的第一随机数与
解析得到的第一随机数是否相同
否
是
响应CAN报文
上报异常信息

图1B

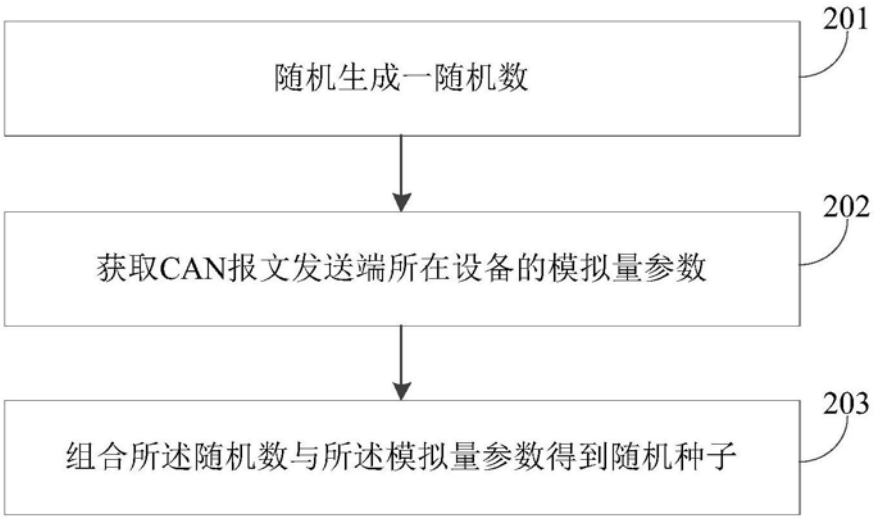

201
随机生成一随机数
202
获取CAN报文发送端所在设备的模拟量参数
203
组合所述随机数与所述模拟量参数得到随机种子

图2

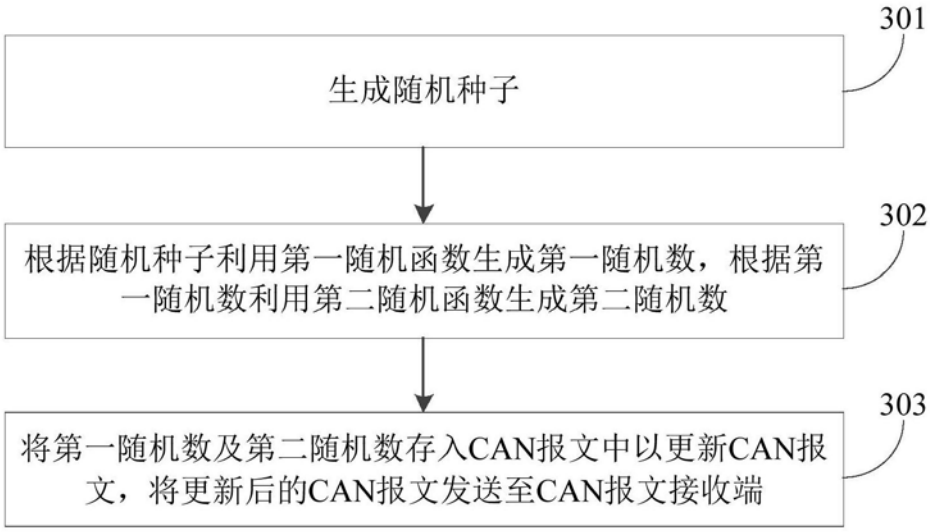

301
生成随机种子
302
根据随机种子利用第一随机函数生成第一随机数，根据第一随机数利用第二随机函数生成第二随机数
303
将第一随机数及第二随机数存入CAN报文中以更新CAN报文，将更新后的CAN报文发送至CAN报文接收端

图3A

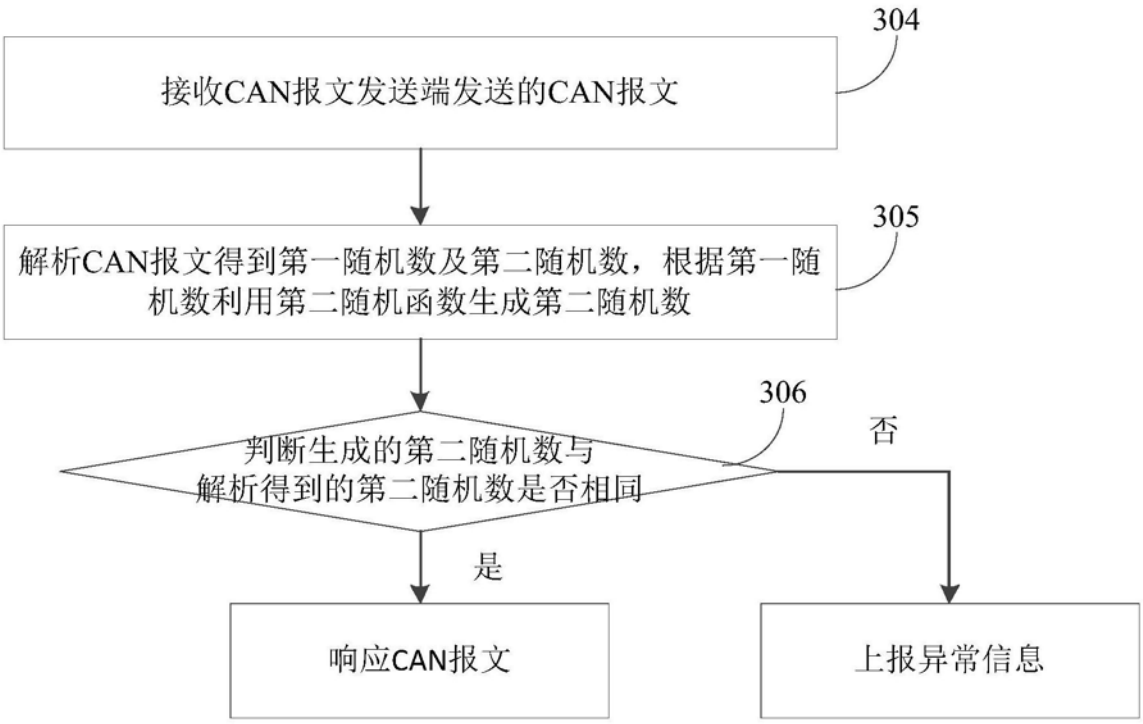

304
接收CAN报文发送端发送的CAN报文
305
解析CAN报文得到第一随机数及第二随机数，根据第一随机数利用第二随机函数生成第二随机数
306
判断生成的第二随机数与解析得到的第二随机数是否相同
否
是
响应CAN报文
上报异常信息

图3B

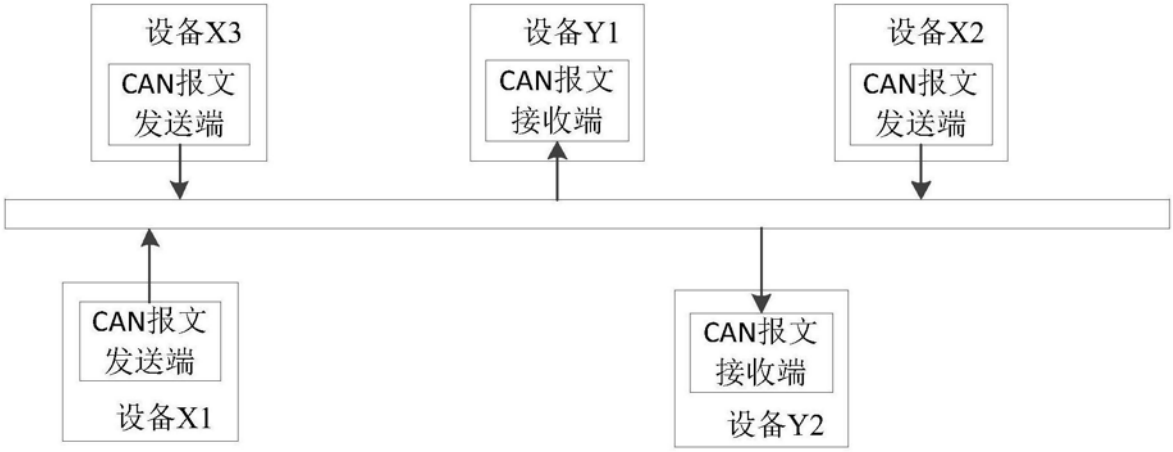

设备X3
CAN报文发送端
设备Y1
CAN报文接收端
设备X2
CAN报文发送端
CAN报文发送端
设备X1
CAN报文接收端
设备Y2

图4