(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 106034111 B
(45)授权公告日 2020.10.16

(21)申请号 201510109017.5

(22)申请日 2015.03.12

(65)同一申请的已公布的文献号
申请公布号 CN 106034111 A

(43)申请公布日 2016.10.19

(30)优先权数据
10-2014-0133321 2014.10.02 KR

(73)专利权人 现代自动车株式会社
地址 韩国首尔
专利权人 起亚自动车株式会社
朝鲜大学校产学协力团
首尔大学校产学协力团

(72)发明人 郑浩镇 李正熙 柳浩 李炳旭
安玹秀 金浩渊 文永植 禹俊永
金荣植 李冈石 卢宗善

(74)专利代理机构 北京尚诚知识产权代理有限公司 11322
代理人 龙淳

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

(56)对比文件
US 2008222414 A1,2008.09.11
CN 103457922 A,2013.12.18
US 2012284523 A1,2012.11.08
CN 101272379 A,2008.09.24
CN 101166167 A,2008.04.23

审查员 王莉

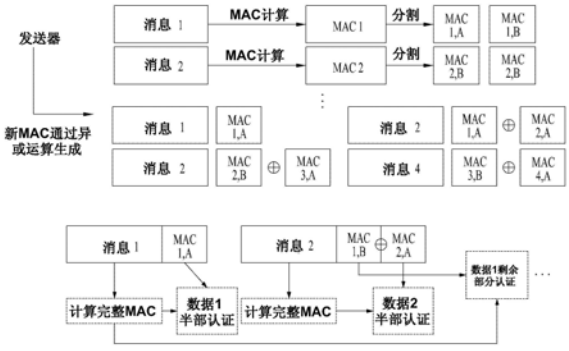
权利要求书4页 说明书6页 附图4页

(54)发明名称

使用混合的MAC认证CAN包的方法和实现其的设备

(57)摘要

本发明提供一种用于在控制器局域网(CAN)中认证数据包的方法和设备。该方法包括在控制器局域网(CAN)中使用混合的消息认证码(MAC)传输消息。另外,使用第一消息生成第一MAC,并且第一消息分割成第一MAC部分和第二MAC部分。使用第二消息生成第二MAC,并且第二MAC分割成第三MAC部分和第四MAC部分。在第二MAC部分和第三MAC部分之间执行线性运算以生成第一认证MAC。第一消息与第一MAC部分一起传输,并且第二消息与第一认证MAC一起传输。



CN 106034111 B

1.一种在车辆控制器局域网(CAN)中使用混合的消息认证码(MACs)发送消息的方法，所述车辆控制器局域网包括配置在车辆中的多个CAN控制器，所述方法包括如下步骤：

由所述多个CAN控制器中的发送控制器使用第一消息生成第一MAC；

由所述发送控制器将所述第一MAC分割成第一MAC部分和第二MAC部分；

由所述发送控制器使用第二消息生成第二MAC；

由所述发送控制器将所述第二MAC分割成第三MAC部分和第四MAC部分；

由所述发送控制器在所述第二MAC部分和所述第三MAC部分之间执行线性运算以生成第一认证MAC；

由所述发送控制器将所述第一消息与所述第一MAC部分一起发送至所述多个CAN控制器中的接收控制器，而不将所述第二MAC部分发送至所述多个CAN控制器中的接收控制器；以及

由所述发送控制器将所述第二消息与所述第一认证MAC一起传输至所述接收控制器；

由所述接收控制器基于所述第一MAC部分和第一认证MAC认证所述第一和第二消息；以及

响应于认证所述第一和第二消息，由所述接收控制器根据所述第一和第二消息执行所述车辆中的操作。

2.根据权利要求1所述的方法，其中分割所述第一MAC的步骤包括：由所述发送控制器将所述第一MAC分割成具有约相同大小的MAC部分的步骤，并且分割所述第二MAC的步骤包括由所述发送控制器将所述第二MAC分割成具有约相同大小的MAC部分的步骤。

3.根据权利要求2所述的方法，其中所述第一MAC部分对应于所述第一MAC的第一半部，并且所述第二MAC部分对应于所述第一MAC的第二半部。

4.根据权利要求2所述的方法，其中所述第三MAC部分对应于所述第二MAC的第一半部，并且所述第四MAC部分对应于所述第二MAC的第二半部。

5.根据权利要求1所述的方法，其中所述线性运算是异或(XOR)运算。

6.一种在车辆控制器局域网(CAN)中使用混合的消息认证码(MACs)接收消息的方法，所述车辆控制器局域网包括配置在车辆中的多个CAN控制器，所述方法包括如下步骤：

由所述多个CAN控制器中的接收控制器从所述多个CAN控制器中的发送控制器接收包括第一消息和第一认证MAC的第一帧；

由所述接收控制器使用所述第一消息计算第一MAC；

由所述接收控制器将所述第一MAC分割成第一MAC部分和第二MAC部分；

由所述接收控制器将所述第一认证MAC与所述第一MAC部分比较以部分地认证所述第一消息；

由所述接收控制器从所述发送控制器接收包括第二消息和第二认证MAC的第二帧；

由所述接收控制器使用所述第二消息计算第二MAC；

由所述接收控制器将所述第二MAC分割成第三MAC部分和第四MAC部分；

由所接收述控制器在所述第二MAC部分和所述第二认证MAC之间执行线性运算以计算所述第三MAC部分；以及

由所述接收控制器将被分割的第三MAC部分与计算出的第三MAC部分比较以部分地认证所述第二消息；以及

响应于认证所述第一和第二消息，由所述接收控制器根据所述第一和第二消息执行所述车辆中的操作。

7.根据权利要求6所述的方法，还包括如下步骤：

由所述接收控制器在所述第二认证MAC和所述被分割的第三MAC部分之间执行线性运算以计算所述第二MAC部分；以及

由所述接收控制器将计算出的第二MAC部分与被分割的第二MAC部分比较以认证所述第一消息。

8.根据权利要求6所述的方法，还包括如下步骤：

当所述被分割的第三部分和所述计算出的第三MAC部分相同时，由所述接收控制器确定出所述第一消息被认证。

9.根据权利要求6所述的方法，其中分割所述第一MAC的步骤包括由所述接收控制器将所述第一MAC分割成具有约相同大小的MAC部分，并且分割所述第二MAC的步骤包括由所述接收控制器将所述第二MAC分割成具有约相同大小的MAC部分。

10.根据权利要求7所述的方法，其中所述第一MAC部分对应于所述第一MAC的第一半部，并且所述第二MAC部分对应于所述第一MAC的第二半部。

11.根据权利要求7所述的方法，其中所述第三MAC部分对应于所述第二MAC的第一半部，并且所述第四MAC部分对应于所述第二MAC的第二半部。

12.根据权利要求6所述的方法，其中所述线性运算是异或(XOR)运算。

13.根据权利要求6所述的方法，还包括如下步骤：

由所述接收控制器将部分地认证所述第一消息和所述第二消息的结果与预定的确定规则比较，以确定发生错误的帧。

14.一种用于在车辆控制器局域网(CAN)中使用混合的消息认证码(MACs)发送消息的控制器，所述车辆控制器局域网(CAN)包括配置在车辆中的多个CAN控制器，所述控制器包括：

配置成存储程序指令的存储器；以及

配置成执行所述程序指令的处理器，当执行所述所述程序指令时使得所述处理器：

生成第一消息和第二消息；

使用所述第一消息生成第一MAC；

将所述第一MAC分割成第一MAC部分和第二MAC部分；

使用所述第二消息生成第二MAC；

将所述第二MAC分割成第三MAC部分和第四MAC部分；

在所述第二MAC部分和所述第三MAC部分之间执行线性运算以生成第一认证MAC；

将所述第一消息与所述第一MAC部分一起发送至所述多个CAN控制器中的接收控制器，而不将所述第二MAC部分发送至所述多个CAN控制器中的接收控制器；以及

将所述第二消息与所述第一认证MAC一起发送至所述接收控制器；

其中所述接收控制器基于所述第一MAC部分和第一认证MAC认证所述第一和第二消息；以及响应于认证所述第一和第二消息，由所述接收控制器根据所述第一和第二消息执行所述车辆中的操作。

15.根据权利要求14所述的发送消息的控制器，其中所述程序指令在执行时还配置成

将所述第一MAC分割成具有约相同大小的MAC部分，并且将所述第二MAC分割成具有约相同大小的MAC部分。

16.根据权利要求15所述的发送消息的控制器，其中所述第一MAC部分对应于所述第一MAC的第一半部，并且所述第二MAC部分对应于所述第一MAC的第二半部。

17.根据权利要求15所述的发送消息的控制器，其中所述第三MAC部分对应于所述第二MAC的第一半部，并且所述第四MAC部分对应于所述第二MAC的第二半部。

18.根据权利要求14所述的发送消息的控制器，其中所述线性运算是异或(XOR)运算。

19.一种用于在车辆控制器局域网(CAN)中使用混合的消息认证码(MACs)接收消息的控制器，所述车辆控制器局域网(CAN)包括配置在车辆中的多个CAN控制器，所述控制器包括：

配置成存储程序指令的存储器；以及

配置成执行所述程序指令的处理器，当执行所述所述程序指令时使得所述处理器：

从所述多个CAN控制器中的发送控制器接收包括第一消息和第一认证MAC的第一帧与包括第二消息和第二认证MAC的第二帧；

使用所述第一消息计算第一MAC；

将所述第一MAC分割成第一MAC部分和第二MAC部分，以将所述第一认证MAC与所述第一MAC部分比较，从而部分地认证所述第一消息；

使用所述第二消息计算第二MAC；

将所述第二MAC分割成第三MAC部分和第四MAC部分；

在所述第二MAC部分和所述第二认证MAC之间执行线性运算以计算所述第三MAC部分；

将被分割的第三MAC部分与计算出的第三MAC部分比较以部分地认证所述第二消息；以及

响应于认证所述第一和第二消息，根据所述第一和第二消息执行所述车辆中的操作。

20.根据权利要求19所述的控制器，其中当执行所述程序指令时还使得所述处理器：在所述第二认证MAC和所述被分割的第三MAC部分之间执行线性运算，以计算所述第二MAC部分，并将计算出的第二MAC部分与被分割的第二MAC部分比较以认证所述第一消息。

21.根据权利要求19所述的接收消息的控制器，其中当执行所述程序指令时还使得所述处理器：当所述被分割的第三部分和所述计算出的第三MAC部分相同时，确定出所述第一消息被认证。

22.根据权利要求19所述的接收消息的控制器，其中所述程序指令在执行时还配置成将所述第一MAC分割成具有约相同大小的MAC部分，并将所述第二MAC分割成具有约相同大小的MAC部分。

23.根据权利要求20所述的接收消息的控制器，其中所述第一MAC部分对应于所述第一MAC的第一半部，并且所述第二MAC部分对应于所述第一MAC的第二半部。

24.根据权利要求20所述的接收消息的控制器，其中所述第三MAC部分对应于所述第二MAC的第一半部，并且所述第四MAC部分对应于所述第二MAC的第二半部。

25.根据权利要求19所述的接收消息的控制器，其中所述线性运算是异或(XOR)运算。

26.根据权利要求19所述的接收消息的控制器，其中当执行所述程序指令时还使得所述处理器：将部分地认证所述第一消息和所述第二消息的结果与预定的确定规则比较，以

确定发生错误的帧。

27.一种在车辆控制器局域网(CAN)中使用用于认证消息的混合的消息认证码(MACs)来接收消息的方法,所述车辆控制器局域网(CAN)包括配置在车辆中的多个CAN控制器,所述方法包括如下步骤:

由多个CAN控制器中的接收控制器接收包括消息和认证MAC的帧;

由所述接收控制器使用所述消息计算MAC;

由所述接收控制器在使用包括在先前接收的帧中的消息计算出的MAC的第二半部与所述认证MAC之间执行线性运算;

由所述接收控制器将执行所述线性运算的结果与使用所述消息计算出的所述MAC的第一半部比较,以部分地认证所述消息;

由所述接收控制器从所述多个CAN控制器中的发送控制器接收下一帧;

由所述接收控制器使用包括在所述下一帧中的消息计算下一MAC;

由所述接收控制器在使用所述消息计算出的所述MAC的第二半部与包括在所述下一帧中的认证MAC之间执行线性运算;

由所述接收控制器将执行所述线性运算的结果与所述下一MAC的第一半部比较以认证所述消息;以及

响应于认证所述消息,由所述接收控制器根据所述消息执行所述车辆中的操作。

28.根据权利要求27所述的方法,还包括如下步骤:

当包括在所述先前接收的帧中的所述消息是第一消息时,由所述接收控制器将包括在所述先前接收的帧中的认证MAC与使用包括在所述先前接收的帧中的所述消息计算出的所述MAC的第一半部比较,以部分地认证包括在所述先前接收的帧中的所述消息。

29.根据权利要求27所述的方法,其中所述线性运算是异或(XOR)运算。

使用混合的MAC认证CAN包的方法和实现其的设备

技术领域

[0001] 本发明涉及用于在控制器局域网(CAN:controller area network)中认证数据包(packet)的方法,并且更具体地涉及使用混合的被分割的消息认证码(MAC:message authentication code)的更高效的认证方法和用于该方法的设备。

背景技术

[0002] 在车辆中,控制器之间的数据包交换在控制器局域网(CAN)上执行。在目前发布的车辆中,直到近来,由于车辆的内部网络独立于外部网络操作,因此还没有提供车辆的内部网络信息的保护措施(例如认证)。因此,由于使用广播方法的车辆CAN的性质,因此还没有提供安全技术,该安全技术用于防止关于行驶中的车辆的信息经由用于车辆诊断的连接端口被窃取,或用于防止插入恶意CAN数据包。

[0003] 为了CAN数据包中的消息的安全性,可考虑消息认证码(MAC)方法。MAC指代用于消息认证的最少量的信息。MAC方法参考图1描述。图1示出根据现有技术的示例性MAC方法。

[0004] 图1在消息131从发送器110传输到接收器120的假设下示出。发送器和接收器预先共享私有密钥(private key)(K)141和MAC生成算法(例如MAC算法151)。在发送器110中,私有密钥141和消息131输入到MAC算法151以生成MAC 161,并且该MAC与消息131一起传输到接收器120。在接收器120中,所接收的消息和共享的私有密钥输入到MAC算法151'以计算MAC 161',并且将计算出的MAC 161'与所接收的MAC 161比较以检验消息的完整性。

[0005] 而且,在CAN中,当MAC方法用于安全性时,缺乏CAN帧中的空间,其中用于认证的MAC数据插入到该空间中。更具体地,尽管可用于CAN帧的数据具有64个比特位的最大值,但当一般MAC数据插入到帧中时,插入到帧中的CAN数据的大小减至小于64个比特位的一半。另外,可能难以将MAC方法应用到对延时敏感的电子设备,诸如车辆制动器或气囊。

发明内容

[0006] 因此,本发明提供用于在控制器局域网(CAN)中认证数据包的方法和用于该方法的设备,该方法和设备基本上消除由现有技术的局限和缺点引起的一个或多个问题。本发明的一个目标是提供车辆中更有效的MAC认证方法和用于该方法的设备。本发明的另一目标是提供使用最少量的MAC数据执行认证的方法和用于该方法的设备。

[0007] 本发明的另外优点、目标和特征在以下描述中部分地阐述,并且对本领域技术人员在考察以下内容时部分地变得显而易见,或可从本发明的实践来学习。本发明的目标和其他优点可通过在书面描述和关于该书面描述的权利要求以及附图中特别地指出的结构实现和获得。

[0008] 为实现这些目标和其他优点并根据本发明的目的,如在本文中实施和概括地描述,在控制器局域网(CAN)中使用混合的消息认证码(MAC)传输消息的方法可包括如下步骤:使用第一消息生成第一MAC;将第一MAC分割成第一MAC部分和第二MAC部分;使用第二消息生成第二MAC;将第二MAC分割成第三MAC部分和第四MAC部分;在第二MAC部分和第三MAC

部分之间执行线性运算以生成第一认证MAC;将第一消息与第一MAC部分一起传输;以及将第二消息与第一认证MAC一起传输。

[0009] 在本发明的另一方面,用于在控制器局域网(CAN)中使用混合的消息认证码(MAC)传输消息的控制器可包括消息管理模块、认证模块、收发器模块,该消息管理模块配置成生成第一消息和第二消息,该认证模块配置成使用第一消息生成第一MAC;将第一MAC分割成第一MAC部分和第二MAC部分;使用第二消息生成第二MAC;将第二MAC分割成第三MAC部分和第四MAC部分;在第二MAC部分和第三MAC部分之间执行线性运算以生成第一认证MAC,该收发器模块配置成将第一消息与第一MAC部分一起传输,并将第二消息与第一认证MAC一起传输。

[0010] 在本发明的另一方面,在控制器局域网(CAN)中使用混合的消息认证码(MAC)接收消息的方法可包括如下步骤:接收包括第一消息和第一认证MAC的第一帧;使用第一消息计算第一MAC;将第一MAC分割成第一MAC部分和第二MAC部分;将第一认证MAC与第一MAC部分比较以部分地认证第一消息;接收包括第二消息和第二认证MAC的第二帧;使用第二消息计算第二MAC;将第二MAC分割成第三MAC部分和第四MAC部分;在第二MAC部分和第二认证MAC之间执行线性运算以计算第三MAC部分,以及将被分割的第三MAC部分与计算出的第三MAC部分比较以部分地认证第二消息。

[0011] 在本发明的另一方面,用于在控制器局域网(CAN)中使用混合的消息认证码(MAC)接收消息的控制器可包括收发器模块和认证模块,该收发器模块配置成接收包括第一消息和第一认证MAC的第一帧与包括第二消息和第二认证MAC的第二帧,该认证模块配置成使用第一消息计算第一MAC;将第一MAC分割成第一MAC部分和第二MAC部分并将第一认证MAC与第一MAC部分比较以部分地认证第一消息;使用第二消息计算第二MAC;将第二MAC分割成第三MAC部分和第四MAC部分;在第二MAC部分和第二认证MAC之间执行线性运算以计算第三MAC部分;并且将被分割的第三MAC部分与计算出的第三MAC部分比较以部分地认证第二消息。

[0012] 应理解本发明的以上一般描述和以下详细描述都是示例性和解释性的,并且旨在提供如所要求的本发明的进一步解释。

附图说明

[0013] 附图示出本发明的示例性实施例并与本说明一起用来解释本发明的原理,该附图被包括以提供本描述的进一步理解并被结合在本申请中且构成本申请的一部分。在附图中:

[0014] 图1是示出根据现有技术的MAC方法的示例图;

[0015] 图2是示出根据现有技术的当应用一般MAC方法时延时何时发生的示例图;

[0016] 图3是示出根据本发明的一个示例性实施例的使用混合的被分割的MAC数据的顺序认证法的示例图;

[0017] 图4是示出根据本发明的示例性实施例的由接收器接收的两个消息的认证成功的示例图;以及

[0018] 图5是示出根据本发明的一个示例性实施例的用于使用混合的MAC执行认证的设备的结构的示例性框图。

具体实施方式

[0019] 可以理解的是，本文所使用的术语“车辆”或“车辆的”或者其他相似术语包括一般的机动车辆，例如客运汽车，包括运动型多用车(SUV)、公共汽车、卡车、各种商用车辆、包括各种船和艇在内的水运工具、航空器，等等，并且包括混合动力交通车辆、电动车辆、插电式混合电动车辆、氢动力车辆和其他替代燃料车辆(例如，从石油以外的资源取得的燃料)。

[0020] 虽然示例性实施例被描述为使用多个单元来执行示例性处理，但是可以理解，也可由一个或多个模块来执行示例性处理，另外，可以理解，数据控制器/控制单元是指包括存储器和处理器的硬件设备。存储器配置为模块存储器，且处理器具体配置为执行所述模块从而执行以下进一步说明的一个或多个处理过程。

[0021] 此外，本发明的控制逻辑可体现为包括由处理器、控制器/控制单元等执行的可执行程序指令的计算机可读介质上的非暂时性计算机可读介质。计算机可读介质的示例包括但不限于ROM、RAM、光盘(CD)-ROM、磁带、软盘、闪存盘、智能卡和光数据存储设备。计算机可读记录介质也可分布在网络连接的计算机系统中，使得计算机可读介质例如远程信息处理服务器或控制局域网(CAN:Controller Area Network)以分布式方式存储和执行。

[0022] 在此使用的术语仅是为描述特定实施例的目的，而并非旨在限制本公开。如本文所用，除非上下文另外清楚表明，否则单数形式“一”、“一个”和“该”旨在也包括复数形式。应当进一步理解，术语“包括”和/或“包含”当在本说明书中使用时，其指所述特征、整体、步骤、操作、元件和/或部件的存在，而不排除一个或多个其他特征、整体、步骤、操作、元件、部件和/或其群组的存在或添加。如本文所用，术语“和/或”包括一个或多个相关联的所列项目的任何或所有组合。

[0023] 除具体陈述或从上下文显然的之外，如在本文中使用，术语“约”理解为在本领域中正常公差的范围内，例如在平均值的2个标准差内。“约(大约)”可理解为在陈述值的10％、9％、8％、7％、6％、5％、4％、3％、2％、1％、0.5％、0.1％、0.05％或0.01％内。除非以其他方式从上下文清楚的，否则在本文中提供的全部数值都由术语“约”修饰。

[0024] 根据本发明的认证CAN的方法参考附图更详细描述。本文中的要素的后缀“模块”或“单元”用于描述方便，并因此可互换使用并且没有任何可区别的意义或功能。通常，当MAC方法应用于车辆CAN时，CAN数据可首先传输并然后CAN数据的MAC数据可传输。特别地，由于接收器不可认证CAN数据直到首先接收的CAN数据的MAC数据被接收，因此可能发生延时(例如，延迟可在认证过程中发生)。这参考图2更详细描述。

[0025] 图2是示出根据现有技术的当应用一般MAC方法时发生延时的示例图。参考图2，当消息(例如，有效负载(payload)231和232)从发送器210传输到接收器220时，消息可经由不同的CAN帧传输。此后，已传输消息231和232的MAC数据可分割成两个数据241和242，并且该两个数据可在不同的帧中传输。尽管接收器120可经由首先接收的两个CAN帧接收消息，但由于消息不可验证直到接收包括被分割的MAC的剩余CAN帧，因此对应于三个帧的延时可从消息经由第一帧接收时发生。

[0026] 总之，用于认证的MAC数据不可与消息同时传输。因此，由于认证不可立即执行，所以可能难以将MAC数据用于对延时敏感的关键数据的认证。另外，当被分割MAC数据中的任一个损坏或丢失时，所有MAC数据可使用。

[0027] 为解决上述问题，在本发明的一个示例性实施例中，提出了这样一种方法：分割

MAC以减小CAN帧中用于MAC的空间，在被分割的MAC之间执行线性运算，并将被分割的MAC混合以在发送器生成新MAC。在接收器中，认证可根据由发送器所用的线性运算的性质使用在被分割的MAC之间的关系更有效执行。

[0028] 图3是示出根据本发明的一个示例性实施例的使用混合的被分割MAC数据的顺序认证法的示例图。参考图3，发送器可配置成使用消息1和消息2生成MAC 1和MAC 2。MAC 1可分割成MAC(1,A)和MAC(1,B)，并且MAC 2可分割成MAC(2,A)和MAC(2,B)。被分割的MAC的大小可以是大约相同的(例如，使用消息生成的MAC的半部)。在第一帧中，MAC(1,A)可作为消息1及其认证MAC数据被包括。在第二帧和此后的帧中，在被分割的MAC(例如，第二被分割MAC)和第一被分割MAC之间执行线性运算(例如异或)的结果可作为MAC数据被包括，该被分割的MAC未包括在使用包括在先前帧中的消息生成的MAC的被分割的MAC之间的先前帧中，该第一被分割MAC处于使用包括在当前帧中的消息生成的MAC的被分割MAC之间。例如，在第二帧中，在MAC(1,B)和MAC(2,A)之间执行线性运算的结果(例如，$\mathrm{MAC}(1,\mathrm{B})\oplus\mathrm{MAC}(2,\mathrm{A})$)可作为用于消息2的MAC数据被包括。

[0029] 当接收器接收第一帧时，可使用消息1生成MAC 1，并且可基于MAC 1的第一半部是否约等于MAC(1,A)来认证消息1的半部。对于第二帧的认证MAC数据(例如，$\mathrm{MAC}(1,\mathrm{B})\oplus\mathrm{MAC}(2,\mathrm{A})$)的认证，可使用下面公式1和公式2计算MAC(1,B)和MAC(2,A)。

[0030] 公式1

[0031] $$\mathrm{MAC}(1,\mathrm{A})\oplus\mathrm{MAC}(1,\mathrm{B})\oplus\mathrm{MAC}(1,\mathrm{A})=\mathrm{MAC}(1,\mathrm{B})$$

[0032] 公式2

[0033] $$\mathrm{MAC}(1,\mathrm{B})\oplus\mathrm{MAC}(2,\mathrm{A})\oplus\mathrm{MAC}(1,\mathrm{B})=\mathrm{MAC}(2,\mathrm{A})$$

[0034] 即，可使用公式1计算作为MAC 1的第二半部的MAC(1,B)，并且可经由在第二帧的认证MAC数据($\mathrm{MAC}(1,\mathrm{B})\oplus\mathrm{MAC}(2,\mathrm{A})$)和MAC(1,B)之间的异或运算获得MAC(2,A)。MAC(2,A)可与经由消息2计算的MAC 2第一半部比较以执行认证。此外，在被计算的MAC 2第一半部和被计算的MAC 1第二半部之间执行线性运算的结果可与包括在第二帧中的认证MAC数据比较。可替换地，MAC(1,B)可通过修改公式2并包括在第二帧中的认证MAC数据和第二消息的第一半部之间执行异或运算来获得。

[0035] 因此，消息1的半部(例如，消息1的第一半部)可经由第一帧认证，并且消息1的剩余半部(例如，消息1的第二半部)和消息2的半部(例如，消息2的第一半部)可经由第二帧认证。由于第三帧和此后的帧相似于第二帧，因此为描述简化，省略重复描述。当认证成功时，包括在帧中的认证MAC数据的长度可减半，并且MAC的长度实质上可增加(例如，可加倍)。即，可使用认证MAC数据的半部来增加(例如，加倍)安全性(例如，MAC的长度)。另外，根据本发明的一个示例性实施例描述当两个帧中至少部分认证失败时的错误确定法，在这两个帧中已分割MAC被混合并传输。

[0036] 图4是示出由接收器接收的两个消息的认证成功的示例图。当认证失败时，可应用基于概率的确定规则以确定认证成功或认证失败。例如，图4在第一帧的认证成功但第二帧的MAC认证失败的假设下示出。特别地，错误可在是MAC 1的组成部分的MAC(1,B)或在是MAC 2的组成部分的MAC(2,A)中发生。因此，当MAC 1的半部，即MAC(1,A)的认证成功时，错误在

是第一MAC的剩余半部(例如,第一MAC的第二半部)的MAC(1,B)中发生的概率可降低。因此,可确定错误在MAC(2,A)中发生。

[0037] 确定规则可基于MAC算法的性质。MAC算法可基于输入生成随机MAC。当MAC的第一半部正确(例如,被认证)并且MAC的第二半部错误(例如,不被认证)时,可发生在MAC算法安全性方面的问题。在此类状况下,确定规则可考虑MAC算法的性质来定义。

[0038] 在下文中,更详细描述根据本示例性实施例的确定规则。如上所述,MAC算法可关于输入数据生成随机输出。特别地,即使当输入数据的一个比特位改变时,与输入数据的半部对应并且位于随机位置的比特位的值可改变。因此,当MAC的大小是b个比特位并且错误在输入数据的一个或多个比特位中发生时,错误可在平均b/2个比特位中发生。然而,根据本发明,当错误在一个帧中发生时,该帧可影响此后传输的其他帧的认证MAC数据。

[0039] 当0表示认证成功并且1表示认证失败时,以下错误可以一般在前四个连续帧中发生。首先,“0000…”可为认证成功而获得。当认证失败在两个或更多个连续帧中发生时可以是如下的。

[0040] 1100…:第一帧认证失败

[0041] 0110…:第二帧认证失败

[0042] 0011…:第三帧认证失败

[0043] 1110…:第一帧和第二帧认证失败

[0044] 0111…:第二帧和第三帧认证失败

[0045] 1111…:第一帧、第二帧和第三帧认证失败

[0046] 如在上面的结果中,当任一个帧的认证失败时,可确定认证失败。因此,认证失败可表明在车辆的内部通信网络中发生的错误,或可表明未认证的访问。因此,当认证错误无关于错误模式而发生时,接收器的控制器可配置成传输警告到内部系统。以下认证失败可以充分低概率1/2b发生。

[0047] 0100:第一帧或第二帧的认证失败(概率1/2b)

[0048] 0010:第二帧或第三帧的认证失败(概率1/2b)

[0049] 1011:在第一帧的认证失败后第三帧的认证失败(概率1/2b)

[0050] 0001:根据第五帧的认证结果改变。在00011的情况下第四帧的认证失败,以及在00010的情况下具有概率1/2b的第三帧或第四帧的认证失败

[0051] 1101:根据第一帧的认证失败后第五帧的认证结果改变。在11011的情况下第四帧的认证失败,以及在11010的情况下具有概率1/2b的第三帧或第四帧的认证失败

[0052] 使用上述认证方法,CAN帧的最小区域可用于认证,上述认证方法使用混合的被分割MAC。因此,包括在一个帧中的认证MAC数据的大小可以减小(例如,减小一半),并且当传输所有MAC时获得的效果可通过在接收器处经由运算执行认证来获得。另外,不同于图2所示的使用被分割MAC的方法,根据本发明的认证方法可提供与在传输所有帧时获得的那些效果相似的效果。进一步地,用于执行上述时间同步方法的设备参考图5描述。图5是示出根据本发明的一个示例性实施例的用于使用混合的被分割的MAC执行认证的设备的结构的示例性框图。

[0053] 使用混合的被分割的MAC执行认证的上述方法由CAN控制器500执行。该认证方法可用于网络上所有CAN控制器,或可仅用于处理敏感数据的一些CAN控制器。

[0054] CAN控制器500可包括并可配置成操作消息管理模块510、认证模块520和收发器模块530，该消息管理模块510配置成生成或处理消息，该认证模块520配置成生成和管理MAC数据并使用被分割的MAC执行认证，该收发器模块530配置成使用CAN方法执行通信。尽管控制器在图5中示为仅包括实施本发明所必需的部件，但如需要则控制器可包括更多部件。

[0055] 更具体地，当控制器500传输消息到网络(例如，控制器作为发送器操作)时，消息管理模块510可配置成生成将要传输到网络的消息。认证模块520可配置成通过第一消息生成MAC 1并通过第二消息生成MAC 2，该第一消息由消息管理模块510生成。认证模块520可配置成在MAC 1的第二半部和MAC 2的第一半部之间执行线性运算，并生成将要包括在第二帧中的认证MAC数据。

[0056] 收发器模块530可配置成将第一消息与MAC 1的第一半部一起经由第一CAN帧传输到网络。收发器模块530可进一步配置成将第二消息与执行线性运算的结果一起经由第二CAN帧传输到网络，该线性运算在MAC 1的第二半部和MAC 2的第一半部之间执行。由于第二帧后的传输过程相似于第二帧的传输过程，因此省略详细描述。

[0057] 当控制器500从网络接收消息(例如，控制器作为接收器操作)时，收发器模块530可配置成从网络接收CAN帧。认证模块520可配置成使用经由第一CAN帧接收的第一消息计算MAC 1，并将MAC 1的第一半部与包括在第一帧中的认证MAC数据比较，以认证第一消息的半部。此后，当接收第二帧时，可使用第二消息计算MAC 2，并且可在MAC 2的第一半部和MAC 1的第二半部之间执行线性运算以将认证MAC数据认证。可替换地，认证模块可配置成经由线性运算来计算MAC 1的第二半部以认证第一消息的剩余半部(例如，第二半部)，并且在第二帧的认证MAC数据和MAC 1的第二半部之间执行线性运算以认证MAC 2的第一半部，从而认证第二消息的半部。认证已完成的消息可由消息管理模块510解释和管理。

[0058] 上述CAN消息认证方法不限于上述示例性实施例的配置，并且可通过选择性地组合上述实施例中的全部或一些来做出各种修改。可以根据本发明的至少一个示例性实施例，通过上述认证方法在车辆CAN中更有效执行认证。特别地，由于传输混合的被分割MAC，因此可以使用最少量的MAC数据执行认证。由于可执行在被分割MAC之间的异或运算，并且认证可经由接收器中的运算来执行，因此可获得与传输所有MAC时获得的那些效果相似的效果。

[0059] 对于本领域技术人员，显然可在本发明中做出各种修改和变化而不背离本发明的实质或保护范围。因此，本发明旨在如果本发明的修改和变化落入附随权利要求及其等效的保护范围内，则本发明覆盖这些修改和变化。

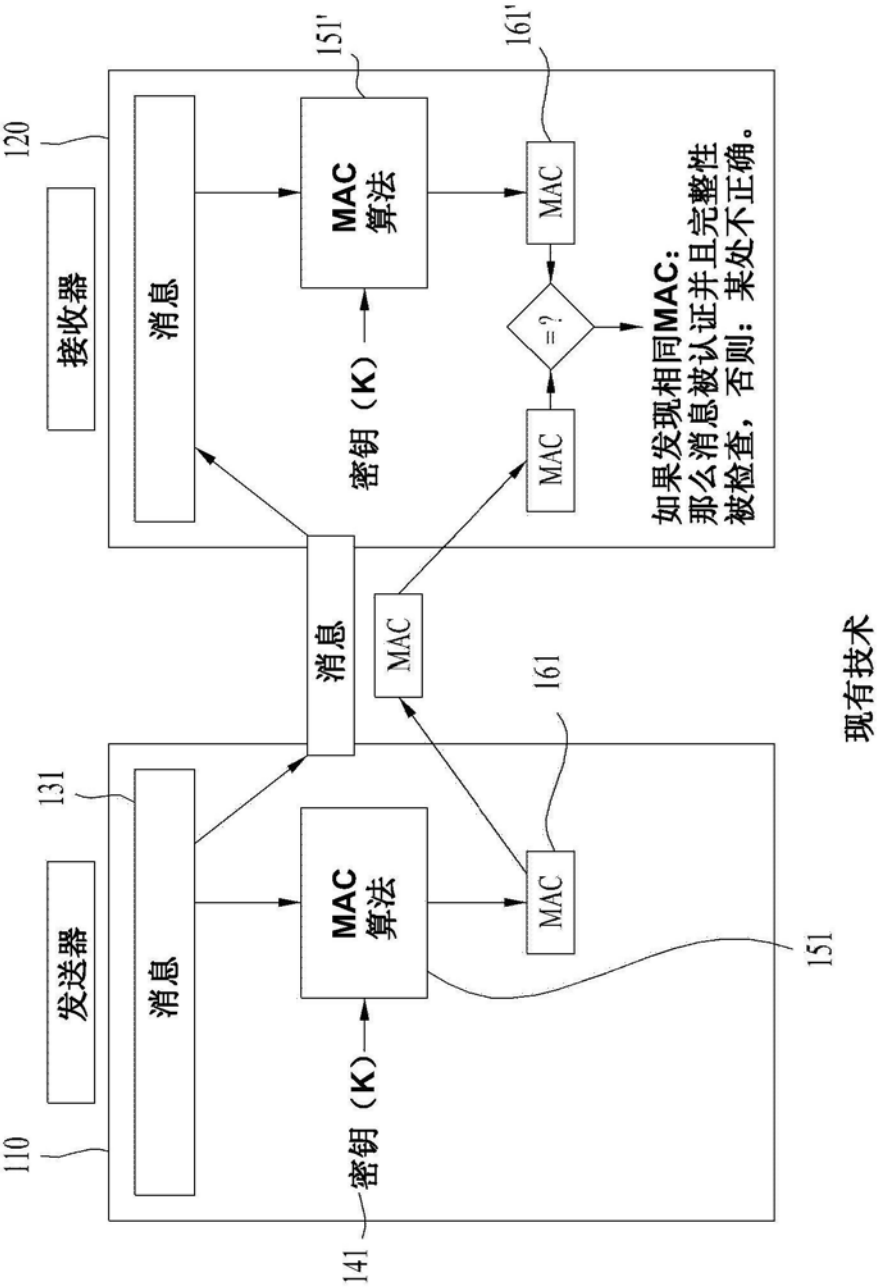

120
接收器
消息
151'
MAC
算法
161'
MAC
=?
MAC
密钥（K）
如果发现相同MAC:
那么消息被认证并且完整性
被检查，否则：某处不正确。
消息
MAC
161
131
发送器
消息
MAC
算法
MAC
151
110
密钥（K）
141
现有技术

图1

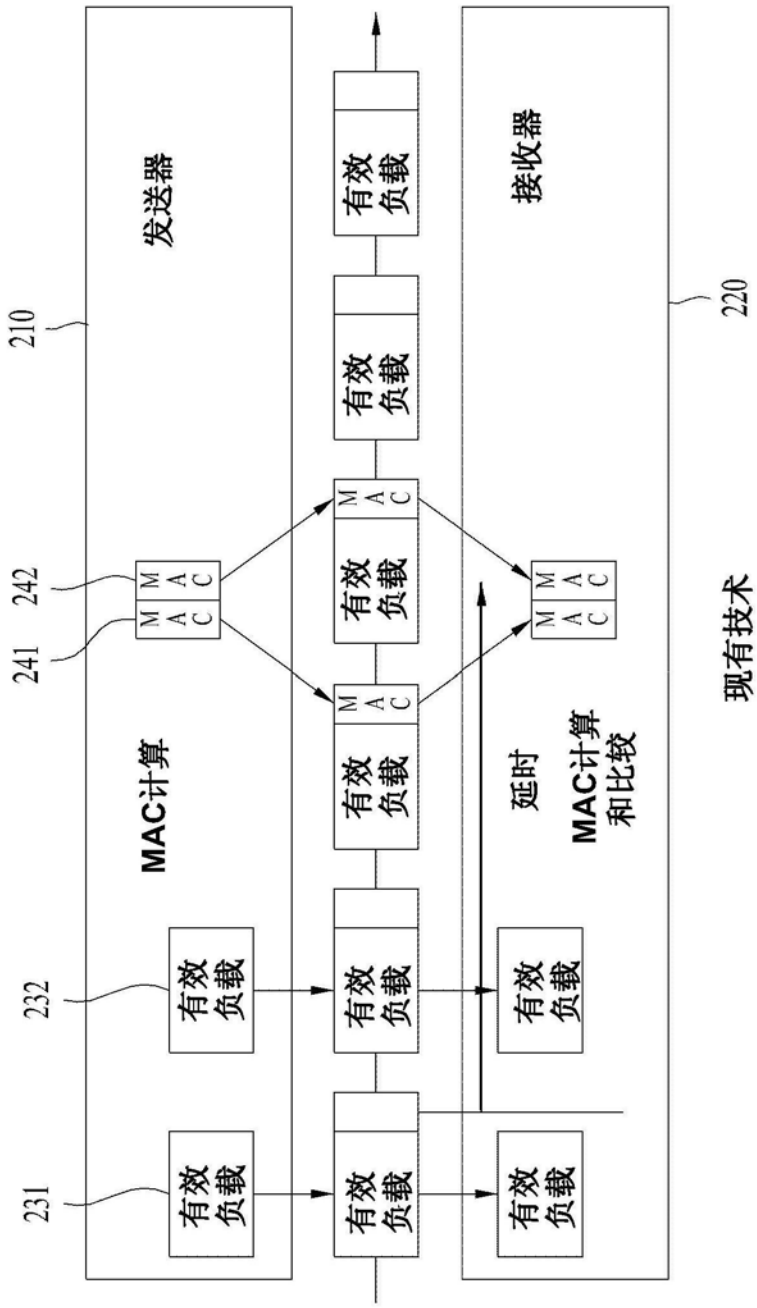

发送器
210
MAC计算
231
232
241
242
有效负载
MAC
接收器
220
延时
MAC计算和比较
现有技术

图2

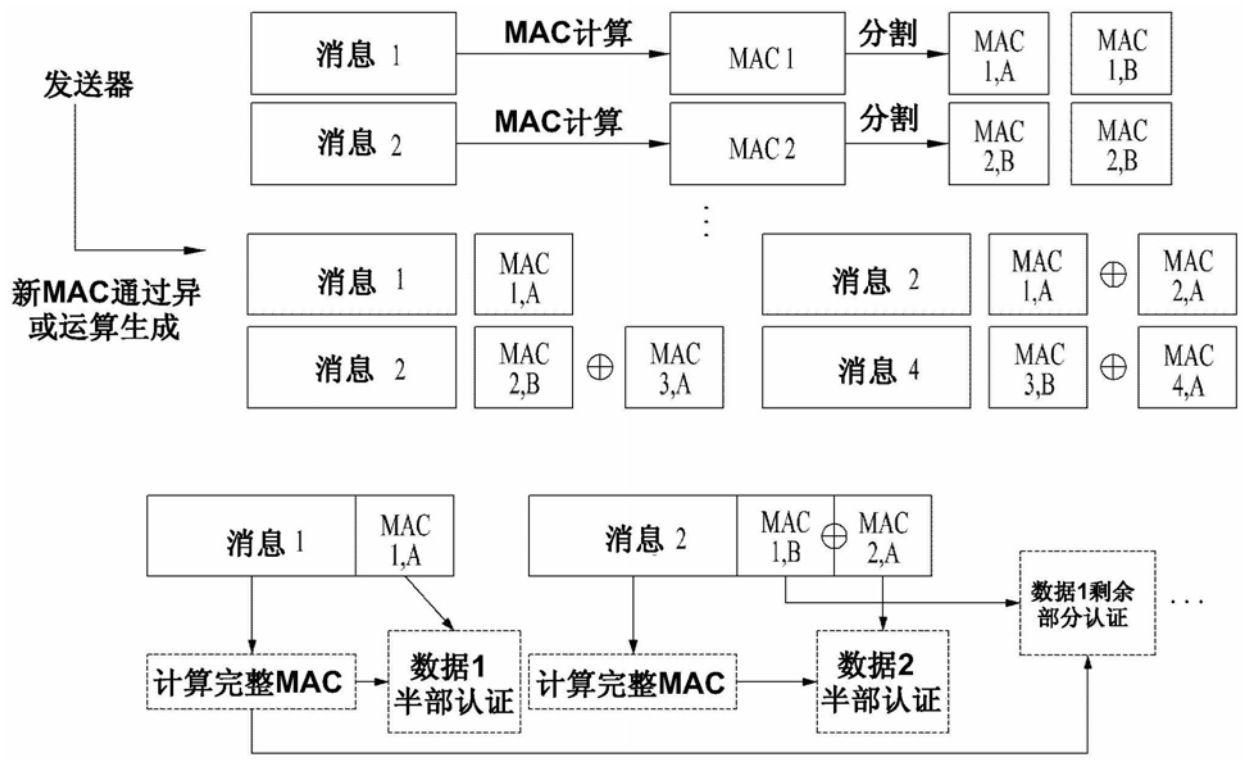

发送器
新MAC通过异或运算生成
消息 1
MAC计算
MAC 1
分割
MAC 1,A
MAC 1,B
消息 2
MAC计算
MAC 2
分割
MAC 2,B
MAC 2,B
消息 1
MAC 1,A
消息 2
MAC 2,B
MAC 3,A
消息 2
MAC 1,A
MAC 2,A
消息 4
MAC 3,B
MAC 4,A
消息 1
MAC 1,A
消息 2
MAC 1,B
MAC 2,A
计算完整MAC
数据1 半部认证
计算完整MAC
数据2 半部认证
数据1剩余部分认证

图3

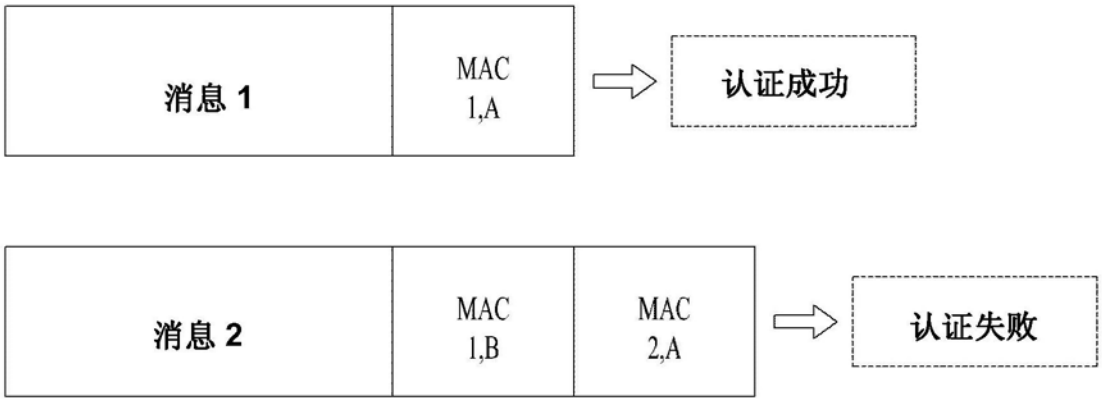

消息 1
MAC 1,A
认证成功
消息 2
MAC 1,B
MAC 2,A
认证失败

图4

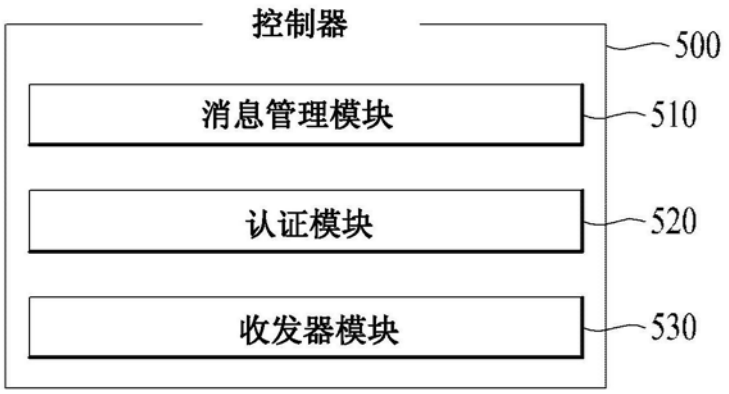


图5