

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2017 年 5 月 18 日 (18.05.2017)



(10) 国际公布号
WO 2017/080182 A1

- (51) 国际专利分类号:
H04L 29/06 (2006.01)
- (21) 国际申请号: PCT/CN2016/083374
- (22) 国际申请日: 2016 年 5 月 25 日 (25.05.2016)
- (25) 申请语言: 中文
- (26) 公布语言: 中文
- (30) 优先权:
201510766262.3 2015 年 11 月 11 日 (11.11.2015) CN
- (71) 申请人: 乐视控股(北京)有限公司 (LE HOLDINGS (BEIJING) CO., LTD.) [CN/CN]; 中国北京市朝阳区姚家园路 105 号 3 号楼 10 层 1102, Beijing 100025 (CN)。乐卡汽车智能科技(北京)有限公司 (LEAUTO INTELLIGENT TECHNOLOGY (BEIJING) CO. LTD) [CN/CN]; 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。
- (72) 发明人: 徐勇 (XU, Yong); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。李丹 (LI, Dan); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。

李文锐 (LI, Wenrui); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。林伟 (LIN, Wei); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。邹禹 (ZOU, Yu); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。勾晓菲 (GOU, Xiaofei); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。刘鹏 (LIU, Peng); 中国北京市朝阳区姚家园路 105 号观湖国际大厦 11 层, Beijing 100025 (CN)。

(74) 代理人: 北京市惠诚律师事务所 (BEIJING HUICHENG LAW FIRM); 中国北京市新中街 68 号聚龙花园 8 号楼 4 层 403, Beijing 100027 (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST,

[见续页]

(54) Title: DATA TRANSMISSION AND RECEIVING METHOD, TRANSMITTER, RECEIVER, AND CAN BUS NETWORK

(54) 发明名称: 数据发送、接收方法、发送端、接收端和 CAN 总线网络

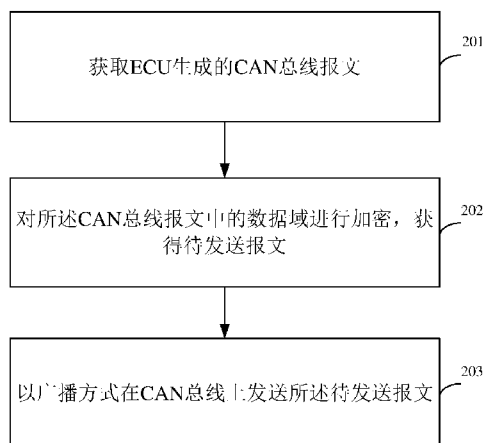


图 2

(57) Abstract: The invention provides a data transmission and receiving method, transmitter, receiver, and controller area network (CAN) bus network, encrypting a data field in a CAN bus message, thereby transmitting, in a transmission procedure, the data field in a form of an encrypted message, increasing security of the CAN bus message, and resolving a technical problem of information leakage resulting from a CAN bus being vulnerable to a network attack. This is because a CAN bus message in the prior art is transmitted in a cleartext form that could be easily monitored, decoded, and forged. In particular, when a forged message is present on a CAN bus, it would result in losing control of a brake, gearbox, and engine, threatening driving safety. Adopting the scheme provided by the embodiment can prevent such incidents from happening.

(57) 摘要: 本发明提供了数据发送、接收方法、发送端、接收端和 CAN 总线网络, 通过对 CAN 总线报文中的数据域进行加密, 从而在传输过程中, 数据域以密文形式传递, 增强了 CAN 总线报文的安全性, 解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于, 现有技术中 CAN 总线报文以明文形式传递, 导致容易被侦听、破解和伪造, 特别是伪造的报文出现在 CAN 总线上后, 将可能导致刹车、变速箱和发动机失控, 威胁行车安全, 采用本实施例中的方案后, 则可避免此类事故发生。

201 Obtain a CAN bus message generated by an electronic control unit (ECU)
202 Encrypt a data field in the CAN bus message to obtain a message to be transmitted
203 Broadcast the message to be transmitted on a CAN bus

WO 2017/080182 A1



SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ,
VC, VN, ZA, ZM, ZW。

CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE,
SN, TD, TG)。

- (84) **指定国** (除另有指明, 要求每一种可提供的地区
保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ,
NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚
(AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT,
BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR,
HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO,
PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ,

根据细则 4.17 的声明:

- 关于申请人有权要求在先申请的优先权(细则
4.17(iii))

本国际公布:

- 包括国际检索报告(条约第 21 条(3))。

数据发送、接收方法、发送端、接收端和 CAN 总线网络

本专利申请要求申请日为 2015 年 11 月 11 日、申请号为 2015107662623 的中国专利申请的优先权，并将上述专利申请以引用的方式全文引入本文中。

技术领域

本发明涉及通信技术，尤其涉及一种数据发送、接收方法、发送端、接收端和 CAN 总线网络。

10 背景技术

控制器局域网网络（Controller Area Network，CAN）总线协议是 ISO 国际标准化的串行通信协议。CAN 总线属于工业现场总线的范畴。与一般的通信总线相比，CAN 总线的数据通信具有突出的实时性和灵活性。由于其良好的性能及独特的设计，CAN 总线越来越受到人们的重视，尤其在汽车领域上被广泛应用。

汽车由四个系统组成，发动机、底盘、车身和电器。每个系统都包含多个电子控制单元（Electronic Control Unit，ECU）。这些 ECU 之间需要通信，而通信依赖于各种不同的总线协议，其中便包括 CAN 总线。

CAN 总线是车身内部最重要的总线，是目前汽车内部的主干网络。它连接了诸如发动机控制系统、变速箱控制系统、自动巡航控制、仪表盘和车身控制模块等模块。但发明人发现，目前 CAN 总线越来越多地受到攻击导致信息泄露，从而对行车安全造成威胁。

发明内容

本发明实施例提供了一种数据发送、接收方法、发送端、接收端和 CAN 总线网络，用于解决 CAN 总线容易受到攻击导致信息泄漏的技术问题。

为达到上述目的，本发明的实施例采用如下技术方案：

第一方面，提供了一种数据发送方法，包括：

获取 ECU 生成的 CAN 总线报文；

30 对所述 CAN 总线报文中的数据域进行加密，获得待发送报文；

以广播方式在 CAN 总线上发送所述待发送报文。

第二方面，提供了一种数据接收方法，包括：

对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文；

对所述加密 CAN 总线报文中的数据域进行解密，获得待接收报文；

5 向所述 ECU 发送所述待接收报文。

第三方面，提供了一种发送端，包括：

ECU 接口，用于获取 ECU 生成的 CAN 总线报文；

加密模块，用于对所述 CAN 总线报文中的数据域进行加密，获得待发送报文；

10 总线接口，用于以广播方式在 CAN 总线上发送所述待发送报文。

第四方面，提供了一种接收端，包括：

侦听模块，用于对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文；

解密模块，用于对所述加密 CAN 总线报文中的数据域进行解密，获得待接收报文；

15 发送模块，用于向所述 ECU 发送所述待接收报文。

第五方面，提供了一种 CAN 总线网络，包括：如上所述的发送端、如上所述的接收端、ECU 和 CAN 总线；

所述发送端分别与所述 ECU 和 CAN 总线连接；

20 所述接收端分别与所述 ECU 和 CAN 总线连接。

本发明实施例提供的数据发送、接收方法、发送端、接收端和 CAN 总线网络，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的
25 报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免此类事故发生。

上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其它目的、特征和优点能够更明显易懂，以下特举本发明的具体实施方式。
30

附图说明

通过阅读下文优选实施方式的详细描述，各种其他的优点和益处对于本领域普通技术人员将变得清楚明了。附图仅用于示出优选实施方式的目的，而并不认为是对本发明的限制。而且在整个附图中，用相同的参考符号表示相同的部件。在附图中：

图 1 为一种典型的 CAN 报文的格式；

图 2 为本发明实施例一提供的一种数据发送方法的流程示意图；

图 3 为本发明实施例二提供的一种数据接收方法的流程示意图；

10 图 4 为本发明实施例三提供的一种发送端 40 的结构示意图；

图 5 为本发明实施例四提供的另一种发送端 40 的结构示意图；

图 6 为本发明实施例五提供的一种接收端 60 的结构示意图；

图 7 为本发明实施例六提供的另一种接收端 60 的结构示意图；

图 8 为本发明实施例七提供的一种 CAN 总线网络的结构示意图。

15 具体实施方式

下面将参照附图更详细地描述本公开的示例性实施例。虽然附图中显示了本公开的示例性实施例，然而应当理解，可以以各种形式实现本公开而不应被这里阐述的实施例所限制。相反，提供这些实施例是为了能够更透彻地理解本公开，并且能够将本公开的范围完整的传达给本领域的技术人员。

通常，CAN 报文由七种不同的位域(Bit Field)组成：帧起始(Start of, SOF)、仲裁域(Arbitration Field)、控制域(Control Field)、数据域(Data Field)、循环冗余校验(cyclic Redundancy Check, CRC)域、应答(ACK)域和帧结束(End of , EOF)。图 1 为一种典型的 CAN 报文的格式，如图 1 所示：

帧起始，其长度可以为 1 位。

仲裁域，由 11 位身份标识 (Identity, ID) 和远程发送请求 (Remote Transmission Request, RTR) 位组成，长度可以为 12 位。

控制域，由 6 位组成，包括 2 个保留位 r，其中，第一个保留位可以 30 作为身份标识符扩展 (Identifier Extension, IDE) 和以及 4 位数据长

度码（Data length code，DLC）。

数据域，其长度可以为 0-64 位。

CRC 域，由 15 位 CRC 校验码域及一个隐性位 CRC 界定符（Delimiter，DEL），其组成长度可以为 0-64 位。

5 应答域，由发送端发出的 ACK 间隙及应答 DEL 隐性位组成。

EOF，每一个报文均由一串七个隐性位的帧结束域结尾。这样，接收端可以正确检测到一帧报文的传输结束。

然而，CAN 总线越来越多地受到攻击导致信息泄露，从而对行车安全造成威胁，这是因为现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，针对这种情况给出了解决方案，采用本实施例中的方案后，则可避免此类事故发生。

下面结合附图对本发明实施例对数据发送、接收方法、发送端、接收端和 CAN 总线网络进行详细描述。

15 实施例一

图 2 为本发明实施例一提供的一种数据发送方法的流程示意图，本实施例中的方法，可以由 CAN 总线网络中的节点执行，在该 CAN 总线网络中每一个节点存在至少一个 ECU，如图 2 所示，包括：

步骤 201、获取 ECU 生成的 CAN 总线报文。

20 具体的，CAN 总线报文的结构如图 1 所示，包括数据域，现有技术中数据域以明文传递，造成 CAN 总线越来越多地受到攻击导致信息泄露，从而对行车安全造成威胁。

步骤 202、对所述 CAN 总线报文中的数据域进行加密，获得待发送报文。

25 具体的，可以采用对称加密算法，对 CAN 总线报文中的数据域进行加密，例如高级加密标准（Advanced Encryption Standard，AES）。

进一步，CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密，其中，数据位，用于携带数据。从而在步骤 202 之前，还包括根据所述 CAN 总线报文中数据域的加密指示位的指示，确认所述 CAN 总线报文加密。作为一种可能的实

现方式，加密指示位为所述数据域中的第一比特位，例如：若加密指示位的取值为 0，则说明报文未加密，则不需要执行步骤 202；若加密指示为的取值为 1，则说明报文加密，则执行步骤 202，在步骤 202 中，对报文中的数据域中的数据位进行加密。

5 步骤 203、以广播方式在 CAN 总线上发送所述待发送报文。

具体的，当 CAN 总线上一个节点发送数据时，它以报文形式广播给网络中所有节点。对每个节点来说，无论该报文是否是发给自身都对其进行侦听，然后对侦听获得的报文，比对自身身份标识与报文仲裁域取值的异同，若相同则侦听获得的报文是发给自身，否则，不是发给自
10 身。

进一步，步骤 203 之前，还包括：

根据所述待发送报文中的仲裁域和 CRC 域，对所述待发送报文进行合法性校验。

具体的，根据帧的起始域、仲裁域、控制域、数据域计算获得 CRC
15 序列，将报文中的 CRC 域取值与计算获得的 CRC 序列进行比较获得比较结果。另外，仲裁域中的 RTR 位在数据帧里必须为“显性”，而在远程帧里必须为“隐性”。它是区别数据帧和远程帧的标志。经过校验，确认待发送报文无误后，进行发送。

本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在
20 传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免
25 此类事故发生。

实施例二

图 3 为本发明实施例二提供的一种数据接收方法的流程示意图，本
实施例中的方法，是与实施例一所提供的数据发送方法相对应的数据接
30 收方法，该数据接收方法可以由 CAN 总线网络中的节点执行，在该 CAN

总线网络中每一个节点存在至少一个 ECU，如图 3 所示，包括：

步骤 301、对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文。

具体的，对所述 CAN 总线侦听，获得仲裁域的取值与所述 ECU 的身份识别码相同的加密 CAN 总线报文。这是由于当 CAN 总线上一个节点发送数据时，它以报文形式广播给网络中所有节点。对每个节点来说，无论该报文是否是发给自身都对其进行侦听，然后对侦听获得的报文，比对自身身份标识与报文仲裁域取值的异同，若相同则侦听获得的报文是发给自身，否则，不是发给自身。

步骤 302、对所述加密 CAN 总线报文中的数据域进行解密，获得待接收报文。

具体的，可以采用与加密步骤所提供的相同的对称加密算法，例如 AES 加密法，对所述加密 CAN 总线报文中的数据位进行解密。

需要说明的是，本发明各实施例所提及的加密，除采用对称算法外，还可以采用非对称算法，本发明各实施例中对此不做限定。

进一步，加密 CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密，其中，数据位，用于携带数据。则在步骤 302 之前，还包括根据所述加密 CAN 总线报文中数据域的加密指示位的指示，确认所述加密 CAN 总线报文加密。作为一种可能的实现方式加密指示位为所述数据域中的第一比特位，例如：若加密指示位的取值为 0，则说明报文未加密，则不需要执行步骤 302；若加密指示为的取值为 1，则说明报文加密，则执行步骤 302，在步骤 302 中，对报文中的数据域中的数据位进行解密。

步骤 303、向所述 ECU 发送所述待接收报文。

具体的，ECU 从而获得待接收报文，进而根据该待接收报文中的数据域进行相应的操作。

本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变

速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免此类事故发生。同时，仅对 CAN 总线网络中涉及到行车安全的 ECU 的 CAN 总线报文进行加密，从而不仅在保证安全性的同时提高了 CAN 总线报文的传输效率，而且节约了 CAN 总线的成本。

5

实施例三

图 4 为本发明实施例三提供的一种发送端 40 的结构示意图，如图 4 所示，该发送端 40 包括：ECU 接口 41、加密模块 42 和总线接口 43。

ECU 接口 41，用于获取 ECU 生成的 CAN 总线报文。

10 具体的，当 ECU 生成需要发送 CAN 总线报文时，ECU 将该 CAN 总线报文发送至本实施例中发送端 40 的 ECU 接口 41，从而本实施例中的发送端 40 接收到 CAN 总线报文。

加密模块 42，用于对 ECU 接口 41 所获取的 CAN 总线报文中的数据域进行加密，获得待发送报文。

15 具体的，加密模块 42 可以采用对称加密算法，对 CAN 总线报文中的数据域进行加密，例如 AES。

总线接口 43，用于以广播方式在 CAN 总线上发送加密模块 42 所获得的待发送报文。

20 具体的，当 CAN 总线上一个节点发送数据时，总线接口 43 以报文形式广播给网络中所有节点。对每个节点来说，无论该报文是否是发给自身都对其进行侦听，然后对侦听获得的报文，比对自身身份标识与报文仲裁域取值的异同，若相同则侦听获得的报文是发给自身，否则，不是发给自身。

25 本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免此类事故发生。

30

实施例四

图 5 为本发明实施例四提供的另一种发送端 40 的结构示意图，如图 5 所示，该发送端 40 在上一实施例的基础上，进一步包括：校验模块 44。

校验模块 44，用于根据加密模块 42 所获得的待发送报文中的仲裁域和 CRC 域，对所述待发送报文进行合法性校验。

进一步，CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密；所述数据位，用于携带数据。

作为一种可能的实现方式，加密指示位为所述数据域中的第一比特位，例如：若加密指示位的取值为 0，则说明报文未加密，则不需要加密模块 42 加密；若加密指示为的取值为 1，则说明报文加密，则需要加密模块 42 加密，在加密模块 42 中，对报文中的数据域中的数据位进行加密。

则所述发送端 40，还包括：判断模块 45。

判断模块 45，用于根据 ECU 接口 41 所获得的 CAN 总线报文中数据域的加密指示位的指示，确认所述 CAN 总线报文是否需要加密。

具体的，判断模块 45 若根据所述 CAN 总线报文中数据域的加密指示位的指示，确认所述 CAN 总线报文加密，则向加密模块 42 发送所述 CAN 总线报文；否则，通过校验模块 44 向总线接口 43 发送所述 CAN 总线报文。

作为一种可能的实现方式，若加密指示位的取值为 0，则说明 CAN 总线报文未加密，判断模块 45 向总线接口 43 发送所述 CAN 总线报文；若加密指示为的取值为 1，则说明 CAN 总线报文加密，判断模块 45 向加密模块 42 发送所述 CAN 总线报文，在加密模块 42 中，对 CAN 总线报文中的数据域中的数据位进行加密。

相应的，加密模块 42，具体用于采用 AES 加密法，对所述 CAN 总线报文中的数据位进行加密。

本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，

解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免此类事故发生。同时，仅对 CAN 总线网络中涉及到行车安全的 ECU 的 CAN 总线报文进行加密，从而不仅在保证安全性的同时提高了 CAN 总线报文的传输效率，而且节约了 CAN 总线的成本。

实施例五

图 6 为本发明实施例五提供的一种接收端 60 的结构示意图，如图 6 所示，包括：侦听模块 61、解密模块 62 和发送模块 63。

侦听模块 61，用于对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文。

具体的，侦听模块 61 对所述 CAN 总线侦听，获得仲裁域的取值与所述 ECU 的身份识别码相同的加密 CAN 总线报文。这是由于当 CAN 总线上一个节点发送数据时，它以报文形式广播给网络中所有节点。对每个节点来说，无论该报文是否是发给自身都对其进行侦听，然后对侦听获得的报文，比对自身身份标识与报文仲裁域取值的异同，若相同则侦听获得的报文是发给自身，否则，不是发给自身。

解密模块 62，用于对侦听模块 61 获得的加密 CAN 总线报文中的数据域进行解密，获得待接收报文。

具体的，可以采用与加密步骤所提供的相同的对称加密算法，例如 AES 加密法，对所述加密 CAN 总线报文中的数据位进行解密。

发送模块 63，用于向所述 ECU 发送解密模块 62 解密获得的待接收报文。

具体的，ECU 从而通过发送模块 63 获得待接收报文，进而根据该待接收报文中的数据域进行相应的操作。

本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，

现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免此类事故发生。

5

实施例六

图 7 为本发明实施例六提供的另一种接收端 60 的结构示意图，如图 6 所示，该接收端 60 在上一实施例的基础上，加密 CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报

10 文是否加密；所述数据位，用于携带数据。

作为一种可能的实现方式，加密指示位为所述数据域中的第一比特位，例如：若加密指示位的取值为 0，则说明报文未加密，则不需要解密模块 62 解密；若加密指示为的取值为 1，则说明报文加密，则需要解密模块 62 解密，在解密模块 62 中，对报文中的数据域中的数据位进行

15 解密。

相应的，该接收端 60 进一步包括：判断模块 64。

判断模块 64，用于根据侦听模块 61 获得的加密 CAN 总线报文中数据域的加密指示位的指示，判断所述加密 CAN 总线报文是否加密。

作为一种可能的实现方式，若加密指示位的取值为 0，则说明加密

20 CAN 总线报文未加密，判断模块 64 向发送模块 63 发送所述加密 CAN 总线报文；若加密指示为的取值为 1，则说明加密 CAN 总线报文加密，判断模块 64 向解密模块 62 发送所述加密 CAN 总线报文，在解密模块 62 中，对加密 CAN 总线报文中的数据域中的数据位进行解密。

相应的，解密模块 62，具体用于采用 AES 加密法，对所述加密 CAN

25 总线报文中的数据位进行解密。

本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和

30 伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变

速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避免此类事故发生。同时，仅对 CAN 总线网络中涉及到行车安全的 ECU 的 CAN 总线报文进行加密，从而不仅在保证安全性的同时提高了 CAN 总线报文的传输效率，而且节约了 CAN 总线的成本。

5

实施例七

图 8 为本发明实施例七提供的一种 CAN 总线网络的结构示意图，如图 8 所示，包括如前述实施例所述的发送端 40 和接收端 60，以及 ECU80 和 CAN 总线。其中，发送端 40 和接收端 60 集成在通信接口 81
10 中，为便于表示，图 8 中仅用一条粗线表示 CAN 总线。

其中，发送端 40 分别与所述 ECU80 和 CAN 总线连接。

接收端 60 分别与所述 ECU80 和 CAN 总线连接。

需要说明的是，图 8 仅作为一种可能的 CAN 总线网络的示意，CAN 总线网络中的 ECU80 可以通过发送端 40 和接收端 60 与 CAN 总线连接，
15 也可以直接与 CAN 总线连接，也就是说，并不是所有 ECU80 所发送的报文都需要进行加密传送。作为一种可能的情况，仅对涉及行车安全的 ECU80 所发送报文进行加密传送，从而这些 ECU80 通过发送端 40 和接收端 60 与 CAN 总线连接。

由于仅对 CAN 总线网络中涉及到行车安全的 ECU 的 CAN 总线报文进行加密，从而不仅在保证安全性的同时提高了 CAN 总线报文的传输效率，而且节约了 CAN 总线的成本。
20

另外，在本实施例中的发送端 40 和接收端 60 集成在一个处理单元中，也可以是单独物理存在。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

25 本实施例中，通过对 CAN 总线报文中的数据域进行加密，从而在传输过程中，数据域以密文形式传递，增强了 CAN 总线报文的安全性，解决了 CAN 总线容易受到攻击导致信息泄漏的技术问题。这是由于，现有技术中 CAN 总线报文以明文形式传递，导致容易被侦听、破解和伪造，特别是伪造的报文出现在 CAN 总线上后，将可能导致刹车、变速箱和发动机失控，威胁行车安全，采用本实施例中的方案后，则可避
30

免此类事故发生。

本领域普通技术人员可以理解：实现上述各方法实施例的全部或部分步骤可以通过程序指令相关的硬件来完成。前述的程序可以存储于一计算机可读取存储介质中。该程序在执行时，执行包括上述各方法实施例的步骤；而前述的存储介质包括：ROM、RAM、磁碟或者光盘等各种可以存储程序代码的介质。

最后应说明的是：以上各实施例仅用以说明本发明的技术方案，而非对其限制；尽管参照前述各实施例对本发明进行了详细的说明，本领域的普通技术人员应当理解：其依然可以对前述各实施例所记载的技术方案进行修改，或者对其中部分或者全部技术特征进行等同替换；而这些修改或者替换，并不使相应技术方案的本质脱离本发明各实施例技术方案的范围。

权 利 要 求 书

1、一种数据发送方法，其特征在于，包括：

获取 ECU 生成的 CAN 总线报文；

对所述 CAN 总线报文中的数据域进行加密，获得待发送报文；

5 以广播方式在 CAN 总线上发送所述待发送报文。

2、根据权利要求 1 所述的数据发送方法，其特征在于，所述 CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密；所述数据位，用于携带数据；

则所述对所述 CAN 总线报文中的数据域进行加密，获得待发送报文
10 之前，还包括：

根据所述 CAN 总线报文中数据域的加密指示位的指示，确认所述 CAN 总线报文加密。

3、根据权利要求 2 所述的数据发送方法，其特征在于，所述加密指示位为所述数据域中的第一比特位。

15 4、根据权利要求 2 所述的数据发送方法，其特征在于，所述对所述 CAN 总线报文中的数据域进行加密，包括：

采用 AES 加密法，对所述 CAN 总线报文中的数据位进行加密。

5、根据权利要求 1-4 任一项所述的数据发送方法，其特征在于，所述对所述 CAN 总线报文中的数据域进行加密，获得待发送报文之后，还包
20 括：

根据所述待发送报文中的仲裁域和 CRC 域，对所述待发送报文进行合法性校验。

6、一种数据接收方法，其特征在于，包括：

对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文；

25 对所述加密 CAN 总线报文中的数据域进行解密，获得待接收报文；

向所述 ECU 发送所述待接收报文。

7、根据权利要求 6 所述的数据接收方法，其特征在于，所述加密 CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密；所述数据位，用于携带数据；

30 则对所述加密 CAN 总线报文中的数据域进行解密，获得待接收报文

之前，还包括：

根据所述加密 CAN 总线报文中数据域的加密指示位的指示，确认所述加密 CAN 总线报文加密。

8、根据权利要求 7 所述的数据接收方法，其特征在于，所述加密指示位为所述数据域中的第一比特位。

9、根据权利要求 7 所述的数据接收方法，其特征在于，所述对所述加密 CAN 总线报文中的数据域进行解密，包括：

采用 AES 加密法，对所述加密 CAN 总线报文中的数据位进行解密。

10、根据权利要求 6-8 任一项所述的数据接收方法，其特征在于，所述对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文，包括：

对所述 CAN 总线侦听，获得仲裁域的取值与所述 ECU 的身份识别码相同的加密 CAN 总线报文。

11、一种发送端，其特征在于，包括：

ECU 接口，用于获取 ECU 生成的 CAN 总线报文；

15 加密模块，用于对所述 CAN 总线报文中的数据域进行加密，获得待发送报文；

总线接口，用于以广播方式在 CAN 总线上发送所述待发送报文。

12、根据权利要求 11 所述的发送端，其特征在于，所述 CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密；所述数据位，用于携带数据；

则所述发送端，还包括：

判断模块，用于根据所述 CAN 总线报文中数据域的加密指示位的指示，判断所述 CAN 总线报文是否加密。

13、根据权利要求 12 所述的发送端，其特征在于，

25 所述加密模块，具体用于采用 AES 加密法，对所述 CAN 总线报文中的数据位进行加密。

14、根据权利要求 11-13 任一项所述的发送端，其特征在于，所述发送端，还包括：

30 校验模块，用于根据所述待发送报文中的仲裁域和 CRC 域，对所述待发送报文进行合法性校验。

15、一种接收端，其特征在于，包括：

侦听模块，用于对 CAN 总线进行侦听，获得 ECU 的加密 CAN 总线报文；

5 解密模块，用于对所述加密 CAN 总线报文中的数据域进行解密，获得待接收报文；

发送模块，用于向所述 ECU 发送所述待接收报文。

16、根据权利要求 15 所述的接收端，其特征在于，所述加密 CAN 总线报文中的数据域包括加密指示位和数据位，所述加密指示位，用于指示所述报文是否加密；所述数据位，用于携带数据；

10 则所述接收端，还包括：

判断模块，用于根据所述加密 CAN 总线报文中数据域的加密指示位的指示，判断所述加密 CAN 总线报文是否加密。

17、根据权利要求 16 所述的接收端，其特征在于，

15 所述解密模块，具体用于采用 AES 加密法，对所述加密 CAN 总线报文中的数据位进行解密。

18、根据权利要求 15-17 任一项所述的接收端，其特征在于，

所述侦听模块，具体用于对所述 CAN 总线侦听，获得仲裁域的取值与所述 ECU 的身份识别码相同的加密 CAN 总线报文。

20 19、一种 CAN 总线网络，包括：如权利要求 11-14 任一项所述的发送端、如权利要求 15-18 任一项所述的接收端、ECU 和 CAN 总线；

所述发送端分别与所述 ECU 和 CAN 总线连接；

所述接收端分别与所述 ECU 和 CAN 总线连接。

1/4

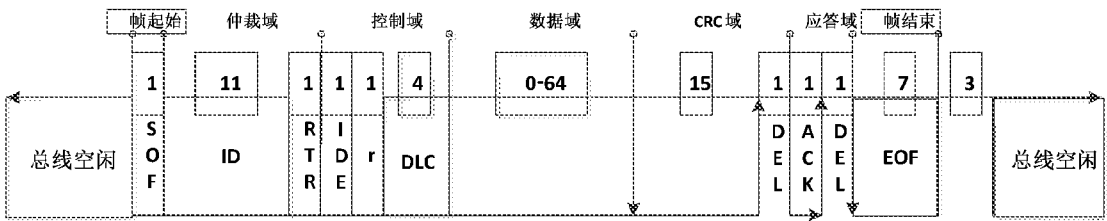


图 1

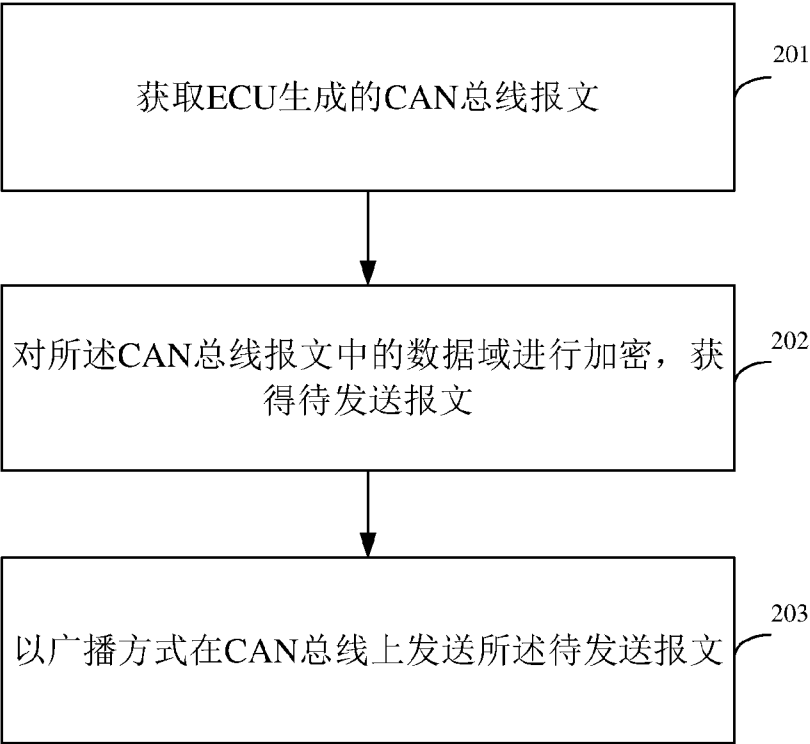


图 2

2/4

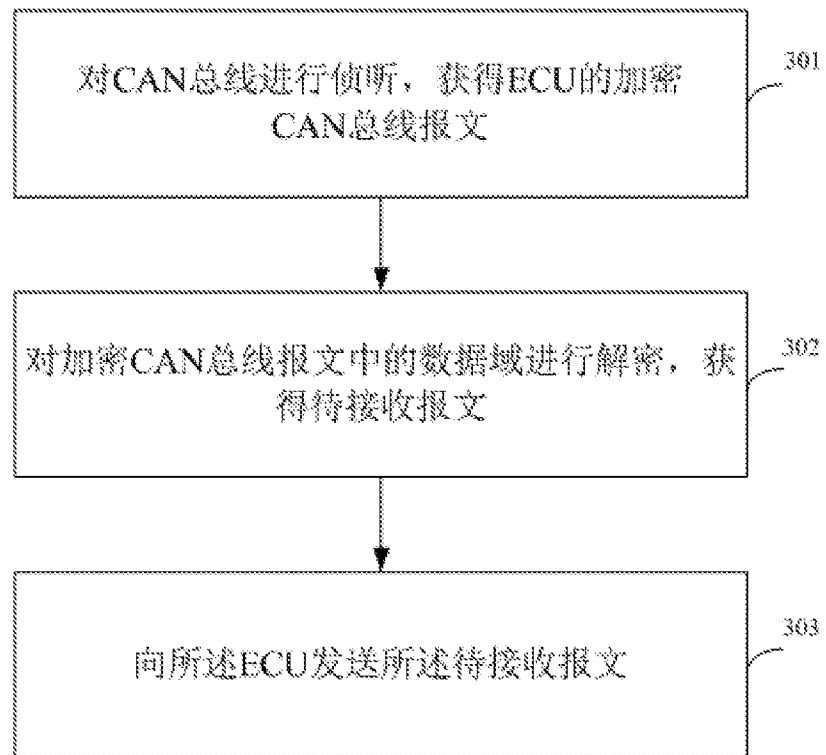


图 3

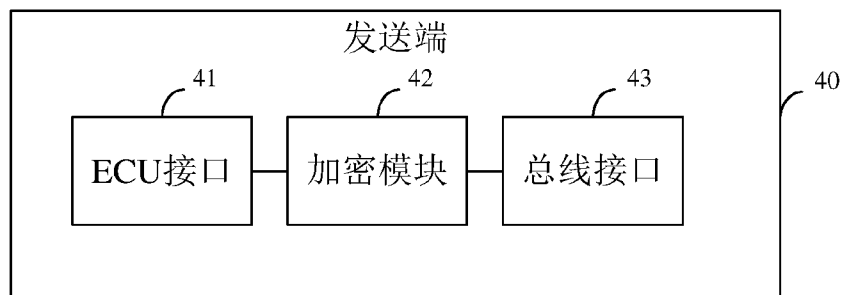


图 4

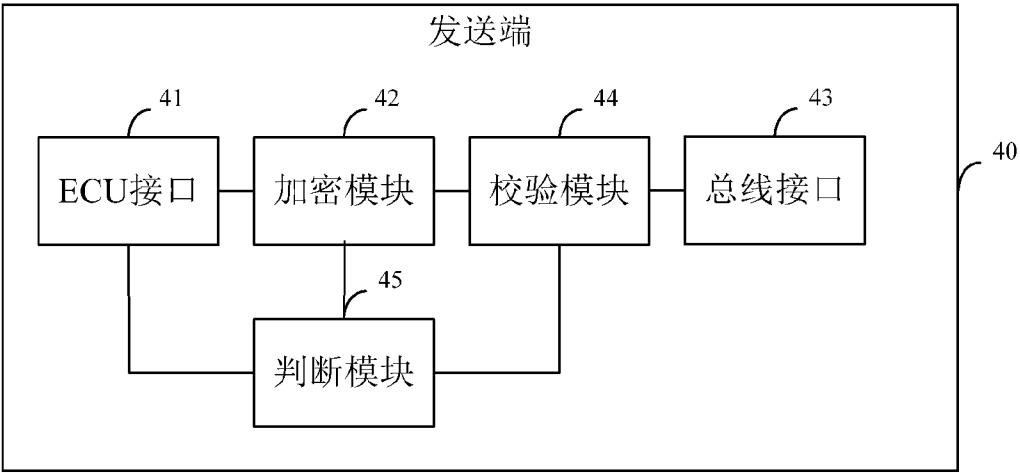


图 5

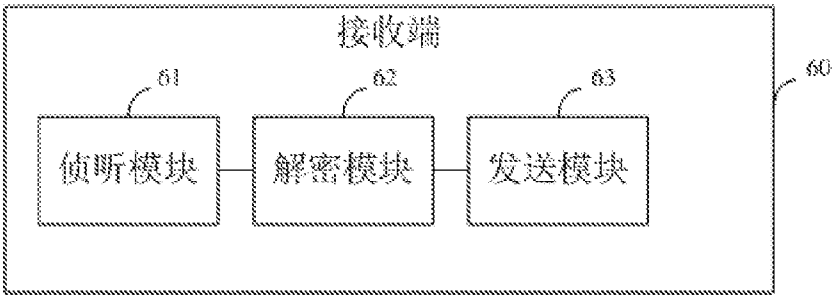


图 6

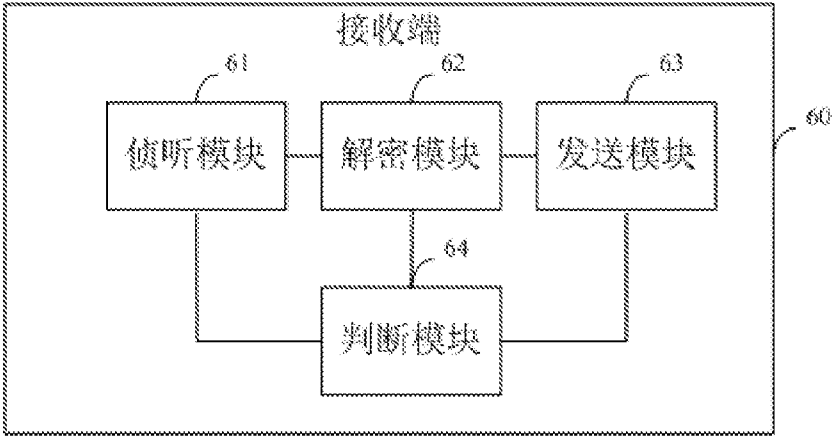


图 7

4/4

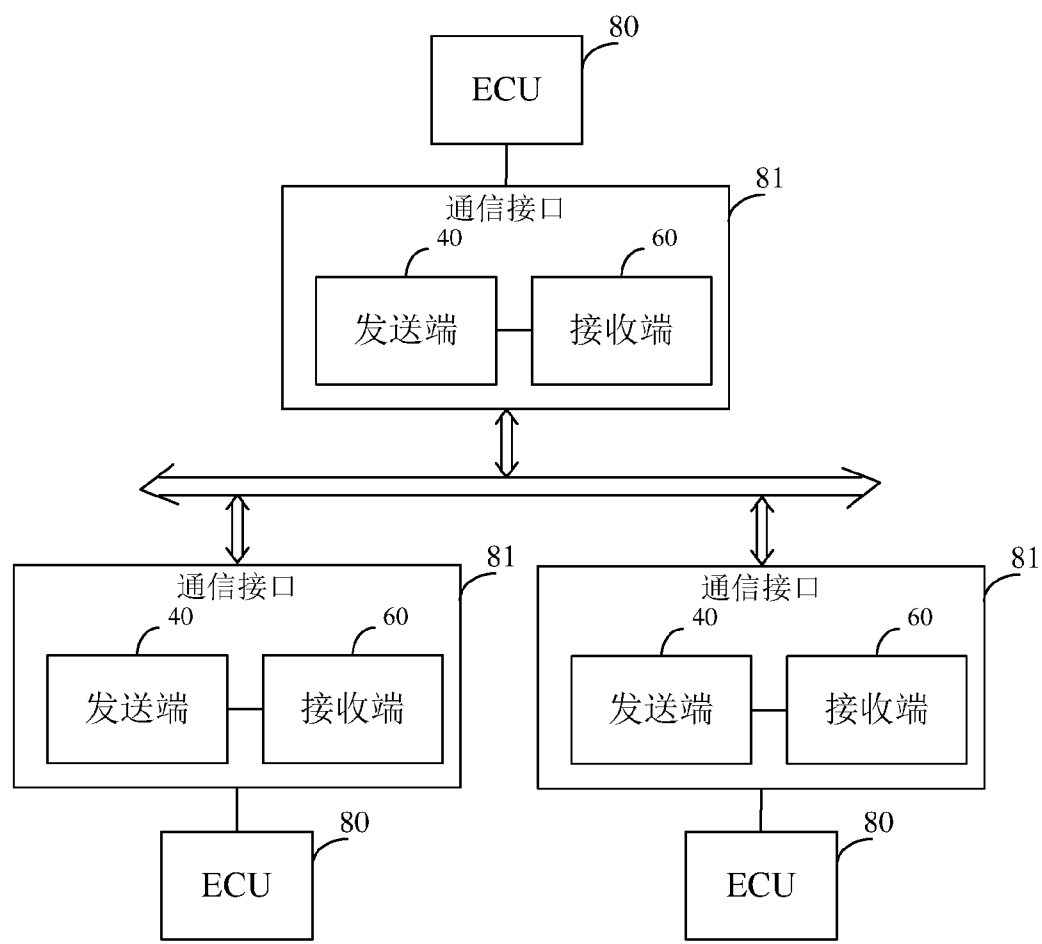


图 8

INTERNATIONAL SEARCH REPORT

International application No.

PCT/CN2016/083374**A. CLASSIFICATION OF SUBJECT MATTER**

H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CPRSABS; CNTXT; VEN; CNKI: controller area network, electronic control unit, CAN, bus, protocol, send, receive, ECU, message, encrypt, decrypt, broadcast, data, connect

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	CN 103166943 A (BEIQI FOTON MOTOR CO., LTD.), 19 June 2013 (19.06.2013), description, pages 1-4	1, 6, 11, 15, 19
Y	CN 104767618 A (TSINGHUA UNIVERSITY), 08 July 2015 (08.07.2015), description, pages 2-5	1, 6, 11, 15, 19
A	CN 104029652 A (CHERY AUTOMOBILE CO., LTD.), 10 September 2014 (10.09.2014), the whole document	1-19
A	CN 101911604 A (CLARK EQUIPMENT COMPANY), 08 December 2010 (08.12.2010), the whole document	1-19

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

05 August 2016 (05.08.2016)

Date of mailing of the international search report

22 August 2016 (22.08.2016)Name and mailing address of the ISA/CN:
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No.: (86-10) 62019451

Authorized officer

CHENG, DongTelephone No.: (86-10) **62411276**

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/CN2016/083374

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 103166943 A	19 June 2013	None	
CN 104767618 A	08 July 2015	None	
CN 104029652 A	10 September 2014	None	
CN 101911604 A	08 December 2010	US 2009169007 A1	02 July 2009
		CA 2711248 A1	16 July 2009
		EP 2227882 A2	15 September 2010
		WO 2009088469 A2	16 July 2009
		WO 2009088469 A3	24 September 2009

国际检索报告

国际申请号

PCT/CN2016/083374

A. 主题的分类

H04L 29/06(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04W

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称, 和使用的检索词(如使用))

CPRSABS;CNTXT;VEN;CNKI: 控制器局域网络, 总线, 协议, 发送, 接收, 电子控制单元, 报文, 加密, 解密, 广播, 数据, 连接, CAN, bus, protocol, send, receive, ECU, message, encrypt, decrypt, broadcast, data, connect

C. 相关文件

类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求
Y	CN 103166943 A (北汽福田汽车股份有限公司) 2013年 6月 19日 (2013 - 06 - 19) 说明书第1-4页	1, 6, 11, 15, 19
Y	CN 104767618 A (清华大学) 2015年 7月 8日 (2015 - 07 - 08) 说明书第2-5页	1, 6, 11, 15, 19
A	CN 104029652 A (奇瑞汽车股份有限公司) 2014年 9月 10日 (2014 - 09 - 10) 全文	1-19
A	CN 101911604 A (克拉克设备公司) 2010年 12月 8日 (2010 - 12 - 08) 全文	1-19

☐ 其余文件在C栏的续页中列出。☒ 见同族专利附件。

* 引用文件的具体类型:

“A” 认为不特别相关的表示了现有技术一般状态的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的)

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期

2016年 8月 5日

国际检索报告邮寄日期

2016年 8月 22日

ISA/CN的名称和邮寄地址

中华人民共和国国家知识产权局(ISA/CN)
中国北京市海淀区蓟门桥西土城路6号 100088

授权官员

程东

传真号 (86-10)62019451

电话号码 (86-10)62411276

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/083374

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	103166943	A	2013年 6月 19日	无			
CN	104767618	A	2015年 7月 8日	无			
CN	104029652	A	2014年 9月 10日	无			
CN	101911604	A	2010年 12月 8日	US	2009169007	A1	2009年 7月 2日
				CA	2711248	A1	2009年 7月 16日
				EP	2227882	A2	2010年 9月 15日
				WO	2009088469	A2	2009年 7月 16日
				WO	2009088469	A3	2009年 9月 24日

表 PCT/ISA/210 (同族专利附件) (2009年7月)