(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 109286500 B
(45)授权公告日 2023.04.11

(21)申请号 201811155806.2

(22)申请日 2018.09.30

(65)同一申请的已公布的文献号
申请公布号 CN 109286500 A

(43)申请公布日 2019.01.29

(73)专利权人 阿波罗智联(北京)科技有限公司
地址 100176 北京市大兴区北京经济技术开发区瑞合西二路7号院1号楼1层101

(72)发明人 吴兴茹

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
专利代理师 孙静 刘芳

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

(56)对比文件
CN 107026823 A,2017.08.08
CN 107277059 A,2017.10.20
CN 103763356 A,2014.04.30

审查员 陈君

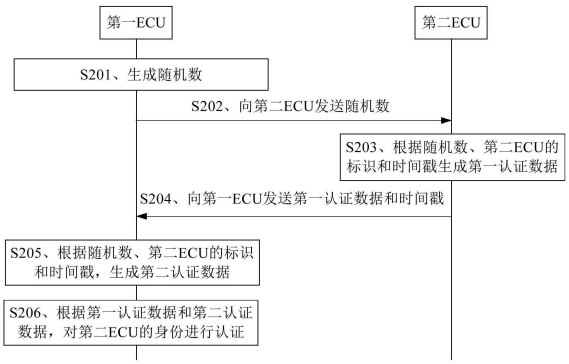
权利要求书3页 说明书12页 附图6页

(54)发明名称

车辆电子控制单元ECU认证方法、装置及设备

(57)摘要

本发明实施例提供一种车辆电子控制单元ECU认证方法、装置及设备，该方法包括：第一ECU生成随机数，并向第二ECU发送所述随机数；所述第一ECU接收所述第二ECU发送的第一认证数据，所述第一认证数据为所述第二ECU根据所述随机数、所述第二ECU的标识和时间戳生成的；所述第一ECU获取所述第二ECU的标识和所述时间戳，并根据所述随机数、所述第二ECU的标识和所述时间戳，生成第二认证数据；所述第一ECU根据所述第一认证数据和所述第二认证数据，对所述第二ECU的身份进行认证。提高了车辆ECU身份认证的安全性。



CN 109286500 B

1.一种车辆电子控制单元ECU认证方法,其特征在于,包括:

第一ECU接收第二ECU在需要与所述第一ECU进行数据通信时发送的认证请求消息;

所述第一ECU根据所述认证请求消息生成随机数,并向第二ECU发送所述随机数;

所述第一ECU接收所述第二ECU发送的第一认证数据,所述第一认证数据为所述第二ECU根据所述随机数、所述第二ECU的标识、时间戳和所述认证请求消息生成的;所述第一认证数据具体是所述第二ECU将所述第二ECU的标识作为预设算法的秘钥,将所述随机数、所述时间戳和所述认证请求消息作为预设算法中的数据,利用所述预设算法进行加密生成的;

所述第一ECU获取所述第二ECU的标识和所述时间戳,并根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息,生成第二认证数据;

所述第一ECU根据所述第一认证数据和所述第二认证数据,对所述第二ECU的身份进行认证,以在对所述第二ECU身份认证通过之后,进行与所述第二ECU之间的数据通信;

所述时间戳为所述第二ECU在接收到所述随机数之后生成的;

所述第一ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息,生成第二认证数据,包括:

所述第一ECU将所述第二ECU的标识作为预设算法的秘钥,将所述随机数、所述时间戳和所述认证请求消息作为预设算法中的数据,利用所述预设算法进行加密,生成所述第二认证数据。

2.根据权利要求1所述的方法,其特征在于,所述第一ECU获取所述时间戳,包括:

所述第一ECU接收所述第二ECU发送的第一消息,所述第一消息包括所述时间戳;

所述第一ECU从所述第一消息中获取所述时间戳。

3.根据权利要求2所述的方法,其特征在于,所述第一消息还包括所述第二ECU的标识;

所述第一ECU获取所述第二ECU的标识,包括:

所述第一ECU从所述第一消息中获取所述第二ECU的标识。

4.根据权利要求1所述的方法,其特征在于,所述第一ECU获取所述第二ECU的标识,包括:

所述第一ECU从所述认证请求消息中获取所述第二ECU的标识。

5.根据权利要求1所述的方法,其特征在于,所述第一ECU根据所述第一认证数据和所述第二认证数据,对所述第二ECU的身份进行认证,包括:

所述第一ECU判断所述第一认证数据和所述第二认证数据是否相同;

若是,则对所述第二ECU的身份认证成功;

若否,则对所述第二ECU的身份认证失败。

6.一种车辆电子控制单元ECU认证方法,其特征在于,包括:

当第二ECU需要与第一ECU进行数据通信时,所述第二ECU向所述第一ECU发送认证请求消息;

所述第二ECU接收所述第一ECU发送的根据认证请求消息生成的随机数;

所述第二ECU生成时间戳,并根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息生成第一认证数据;

所述第二ECU向所述第一ECU发送所述第一认证数据;

所述第二ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息生成第一认证数据，包括：

所述第二ECU将所述第二ECU的标识作为预设算法的秘钥，将所述随机数、所述时间戳和所述认证请求消息作为预设算法中的数据，利用所述预设算法进行加密，生成所述第一认证数据。

7.根据权利要求6所述的方法，其特征在于，所述认证请求消息中包括所述第二ECU的标识。

8.根据权利要求6所述的方法，其特征在于，所述第二ECU生成时间戳之后，还包括：

所述第二ECU向所述第一ECU发送所述时间戳。

9.一种车辆电子控制单元ECU认证装置，其特征在于，包括生成模块、发送模块、接收模块、获取模块和认证模块，其中，

所述接收模块用于，接收第二ECU在需要与第一ECU进行数据通信时发送的认证请求消息；

所述生成模块用于，根据所述认证请求消息生成随机数；

所述发送模块用于，向第二ECU发送所述随机数；

所述接收模块用于，接收所述第二ECU发送的第一认证数据，所述第一认证数据为所述第二ECU根据所述随机数、所述第二ECU的标识、时间戳和所述认证请求消息生成的；所述第一认证数据具体是所述第二ECU将所述第二ECU的标识作为预设算法的秘钥，将所述随机数、所述时间戳和所述认证请求消息作为预设算法中的数据，利用所述预设算法进行加密生成的；

所述获取模块用于，获取所述第二ECU的标识和所述时间戳；

所述生成模块还用于，根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息，生成第二认证数据；

所述认证模块用于，根据所述第一认证数据和所述第二认证数据，对所述第二ECU的身份进行认证，以在对所述第二ECU身份认证通过之后，进行与所述第二ECU之间的数据通信；

所述时间戳为所述第二ECU在接收到所述随机数之后生成的；

所述生成模块具体用于：将所述第二ECU的标识作为预设算法的秘钥，将所述随机数、所述时间戳和所述认证请求消息作为预设算法中的数据，利用所述预设算法进行加密，生成所述第二认证数据。

10.根据权利要求9所述的装置，其特征在于，所述接收模块还用于，接收所述第二ECU发送的第一消息，所述第一消息包括所述时间戳；

所述获取模块具体用于，从所述第一消息中获取所述时间戳。

11.根据权利要求10所述的装置，其特征在于，所述第一消息还包括所述第二ECU的标识；所述获取模块具体用于：

从所述第一消息中获取所述第二ECU的标识。

12.根据权利要求9所述的装置，其特征在于，所述获取模块具体用于：

从所述认证请求消息中获取所述第二ECU的标识。

13.根据权利要求9所述的装置，其特征在于，所述认证模块具体用于：

判断所述第一认证数据和所述第二认证数据是否相同；

若是,则对所述第二ECU的身份认证成功;

若否,则对所述第二ECU的身份认证失败。

14.一种车辆电子控制单元ECU认证装置,其特征在于,包括接收模块、生成模块和发送模块,其中,

所述发送模块用于,当第二ECU需要与第一ECU进行数据通信时,向所述第一ECU发送认证请求消息;

所述接收模块用于,接收所述第一ECU发送的根据认证请求消息生成的随机数;

所述生成模块用于,生成时间戳,并根据所述随机数、第二ECU的标识、所述时间戳和所述认证请求消息生成第一认证数据;

所述发送模块用于,向所述第一ECU发送所述第一认证数据;

所述生成模块具体用于,将所述第二ECU的标识作为预设算法的秘钥,将所述随机数、所述时间戳和所述认证请求消息作为预设算法中的数据,利用所述预设算法进行加密,生成所述第一认证数据。

15.根据权利要求14所述的装置,其特征在于,所述认证请求消息中包括所述第二ECU的标识。

16.根据权利要求14所述的装置,其特征在于,

所述发送模块还用于,在所述生成模块生成时间戳之后,向所述第一ECU发送所述时间戳。

17.一种车辆电子控制单元ECU认证装置,其特征在于,包括:处理器,所述处理器与存储器耦合,其中,

所述存储器用于,存储计算机程序;

所述处理器用于,执行所述存储器中存储的计算机程序,用于实现权利要求1-5任一项所述的车辆ECU认证方法。

18.一种车辆电子控制单元ECU认证装置,其特征在于,包括:处理器,所述处理器与存储器耦合,其中,

所述存储器用于,存储计算机程序;

所述处理器用于,执行所述存储器中存储的计算机程序,用于实现权利要求6-8任一项所述的车辆ECU认证方法。

19.一种可读存储介质,其特征在于,包括程序或指令,当所述程序或指令在计算机上运行时,如所述权利要求1-5任一项所述的车辆ECU认证方法被执行。

20.一种可读存储介质,其特征在于,包括程序或指令,当所述程序或指令在计算机上运行时,如所述权利要求6-8任一项所述的车辆ECU认证方法被执行。

车辆电子控制单元ECU认证方法、装置及设备

技术领域

[0001] 本发明实施例涉及通信技术领域，尤其涉及一种车辆ECU认证方法、装置及设备。

背景技术

[0002] 目前，车辆(例如小汽车、公交车等)中通常包括多个电子控制单元(Electronic Control Unit，简称ECU)，多个ECU之间可以通过数据总线相互通信，以实现对车辆进行控制。

[0003] 为了避免黑客通过伪造的ECU在数据总线中窃取消息或者发送攻击指令，两个ECU在进行通信之前可以进行身份认证。在现有技术中，两个ECU之间通常采用seed/key的安全认证方式进行身份认证，具体的，第一ECU向第二ECU发送认证请求消息，第二ECU根据认证请求消息向第一ECU发送seed值，第一ECU根据seed生成key，并向第二ECU发送key，第二ECU根据seed值生成一个key，并根据生成的key和接收到的key对第一ECU进行身份认证。

[0004] 然而，在上述过程中，seed值通常为固定值或者长度为2-3个字节的数据，导致seed值容易被破解出现，使得黑客可以根据破解得到的seed进行身份认证，导致现有技术中的车辆ECU的身份认证的安全性较低。

发明内容

[0005] 本发明实施例提供一种车辆ECU认证方法、装置及设备，提高了车辆ECU身份认证的安全性。

[0006] 第一方面，本发明实施例提供一种车辆电子控制单元ECU认证方法，包括：

[0007] 第一ECU生成随机数，并向第二ECU发送所述随机数；

[0008] 所述第一ECU接收所述第二ECU发送的第一认证数据，所述第一认证数据为所述第二ECU根据所述随机数、所述第二ECU的标识和时间戳生成的；

[0009] 所述第一ECU获取所述第二ECU的标识和所述时间戳，并根据所述随机数、所述第二ECU的标识和所述时间戳，生成第二认证数据；

[0010] 所述第一ECU根据所述第一认证数据和所述第二认证数据，对所述第二ECU的身份进行认证。

[0011] 在一种可能的实施方式中，在第一ECU生成随机数之前，还包括：所述第一ECU接收所述第二ECU发送的认证请求消息；相应的，所述第一认证数据具体为所述第二ECU根据所述随机数、所述第二ECU的标识、时间戳和所述认证请求消息生成的；

[0012] 相应的，所述第一ECU根据所述随机数、所述第二ECU的标识和所述时间戳，生成第二认证数据，包括：

[0013] 所述第一ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息，生成第二认证数据。

[0014] 在另一种可能的实施方式中，所述时间戳为所述第二ECU在接收到所述随机数之后生成的；所述第一ECU获取所述时间戳，包括：

[0015] 所述第一ECU接收所述第二ECU发送的第一消息，所述第一消息包括所述时间戳；

[0016] 所述第一ECU从所述第一消息中获取所述时间戳。

[0017] 在另一种可能的实施方式中，所述第一消息还包括所述第二ECU的标识；

[0018] 所述第一ECU获取所述第二ECU的标识，包括：

[0019] 所述第一ECU从所述第一消息中获取所述第二ECU的标识。

[0020] 在另一种可能的实施方式中，所述第一ECU获取所述第二ECU的标识，包括：

[0021] 所述第一ECU从所述认证请求消息中获取所述第二ECU的标识。

[0022] 在另一种可能的实施方式中，所述第一ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息，生成第二认证数据，包括：

[0023] 所述第一ECU通过预设算法，并根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息进行运算，得到所述第二认证数据。

[0024] 在另一种可能的实施方式中，所述第一ECU根据所述第一认证数据和所述第二认证数据，对所述第二ECU的身份进行认证，包括：

[0025] 所述第一ECU判断所述第一认证数据和所述第二认证数据是否相同；

[0026] 若是，则对所述第二ECU的身份认证成功；

[0027] 若否，则对所述第二ECU的身份认证失败。

[0028] 第二方面，本发明实施例提供一种车辆电子控制单元ECU认证方法，包括：

[0029] 第二ECU接收第一ECU发送的随机数；

[0030] 所述第二ECU生成时间戳，并根据所述随机数、所述第二ECU的标识和所述时间戳生成第一认证数据；

[0031] 所述第二ECU向所述第一ECU发送所述第一认证数据。

[0032] 在一种可能的实施方式中，所述第二ECU接收第一ECU发送的随机数之前，还包括：

[0033] 所述第二ECU向所述第一ECU发送认证请求消息。

[0034] 在另一种可能的实施方式中，所述第二ECU根据所述随机数、所述第二ECU的标识和所述时间戳生成第一认证数据，包括：

[0035] 所述第二ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息生成第一认证数据。

[0036] 在另一种可能的实施方式中，所述认证请求消息中包括所述第二ECU的标识。

[0037] 在另一种可能的实施方式中，所述第二ECU生成时间戳之后，还包括：

[0038] 所述第二ECU向所述第一ECU发送所述时间戳。

[0039] 第三方面，本发明实施例提供一种车辆电子控制单元ECU认证装置，包括生成模块、发送模块、接收模块、获取模块和认证模块，其中，

[0040] 所述生成模块用于，生成随机数；

[0041] 所述发送模块用于，向第二ECU发送所述随机数；

[0042] 所述接收模块用于，接收所述第二ECU发送的第一认证数据，所述第一认证数据为所述第二ECU根据所述随机数、所述第二ECU的标识和时间戳生成的；

[0043] 所述获取模块用于，获取所述第二ECU的标识和所述时间戳；

[0044] 所述生成模块还用于，根据所述随机数、所述第二ECU的标识和所述时间戳，生成第二认证数据；

[0045] 所述认证模块用于，根据所述第一认证数据和所述第二认证数据，对所述第二ECU的身份进行认证。

[0046] 在一种可能的实施方式中，所述接收模块还用于，在所述生成模块生成随机数之前，接收所述第二ECU发送的认证请求消息；相应的，所述第一认证数据具体为所述第二ECU根据所述随机数、所述第二ECU的标识、时间戳和所述认证请求消息生成的；

[0047] 所述生成模块具体用于，根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息，生成第二认证数据。

[0048] 在另一种可能的实施方式中，所述时间戳为所述第二ECU在接收到所述随机数之后生成的；

[0049] 所述接收模块还用于，接收所述第二ECU发送的第一消息，所述第一消息包括所述时间戳；

[0050] 所述获取模块具体用于，从所述第一消息中获取所述时间戳。

[0051] 在另一种可能的实施方式中，所述第一消息还包括所述第二ECU的标识；所述获取模块具体用于：

[0052] 从所述第一消息中获取所述第二ECU的标识。

[0053] 在另一种可能的实施方式中，所述获取模块具体用于：

[0054] 从所述认证请求消息中获取所述第二ECU的标识。

[0055] 在另一种可能的实施方式中，所述生成模块具体用于：

[0056] 通过预设算法，并根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息进行运算，得到所述第二认证数据。

[0057] 在另一种可能的实施方式中，所述认证模块具体用于：

[0058] 判断所述第一认证数据和所述第二认证数据是否相同；

[0059] 若是，则对所述第二ECU的身份认证成功；

[0060] 若否，则对所述第二ECU的身份认证失败。

[0061] 第四方面，本发明实施例提供一种车辆电子控制单元ECU认证装置，包括接收模块、生成模块和发送模块，其中，

[0062] 所述接收模块用于，接收第一ECU发送的随机数；

[0063] 所述生成模块用于，生成时间戳，并根据所述随机数、第二ECU的标识和所述时间戳生成第一认证数据；

[0064] 所述发送模块用于，向所述第一ECU发送所述第一认证数据。

[0065] 在一种可能的实施方式中，所述发送模块还用于，在所述接收模块接收所述第一ECU发送的随机数之前，向所述第一ECU发送认证请求消息。

[0066] 在另一种可能的实施方式中，所述生成模块具体用于：

[0067] 所述第二ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息生成第一认证数据。

[0068] 在另一种可能的实施方式中，所述认证请求消息中包括所述第二ECU的标识。

[0069] 在另一种可能的实施方式中，所述发送模块还用于，在所述生成模块生成时间戳之后，向所述第一ECU发送所述时间戳。

[0070] 第五方面，本发明实施例提供一种车辆电子控制单元ECU认证装置，包括：处理器，

所述处理器与存储器耦合，其中，

[0071] 所述存储器用于，存储计算机程序；

[0072] 所述处理器用于，执行所述存储器中存储的计算机程序，用于实现上述第一方面任一项所述的车辆ECU认证方法。

[0073] 第六方面，本发明实施例提供一种车辆电子控制单元ECU认证装置，包括：处理器，所述处理器与存储器耦合，其中，

[0074] 所述存储器用于，存储计算机程序；

[0075] 所述处理器用于，执行所述存储器中存储的计算机程序，用于实现上述第二方面任一项所述的车辆ECU认证方法。

[0076] 第七方面，本发明实施例提供一种可读存储介质，包括程序或指令，当所述程序或指令在计算机上运行时，如上述第一方面任一项所述的车辆ECU认证方法被执行。

[0077] 第八方面，本发明实施例提供一种可读存储介质，包括程序或指令，当所述程序或指令在计算机上运行时，如上述第二方面任一项所述的车辆ECU认证方法被执行。

[0078] 本申请提供的车辆ECU认证方法、装置及设备，第一ECU生成随机数，并向第二ECU发送随机数，第二ECU根据随机数、第二ECU的标识和时间戳生成第一认证数据，第二ECU向第一ECU发送第一认证数据和时间戳。第一ECU根据随机数、第二ECU的标识和时间戳，生成第二认证数据，并根据第一认证数据和第二认证数据，对第二ECU的身份进行认证。在上述过程中，认证数据是依据随机数、第二ECU的标识和时间戳生成的，由于随机数是随机生成的，且不同身份认证过程中的随机数不同，不同身份认证过程中的时间戳也不同，因此，即使一次身份认证中的随机数和时间戳被破解，也无法应用于下次的身份认证过程中，进而提高身份认证的安全性。进一步的，若第二ECU向第一ECU发送的随机数、时间戳、第二ECU的标识和第一认证数据中的任意一个被篡改，则第一ECU对第二ECU的身份认证失败，进而提高了车辆ECU身份认证的安全性。

附图说明

[0079] 为了更清楚地说明本发明实施例或现有技术中的技术方案，下面将对实施例或现有技术描述中所需要使用的附图作一简单地介绍，显而易见地，下面描述中的附图是本发明的一些实施例，对于本领域普通技术人员来讲，在不付出创造性劳动性的前提下，还可以根据这些附图获得其他的附图。

[0080] 图1为本申请提供的车辆中ECU的示意图；

[0081] 图2为本申请提供的车辆ECU认证方法的流程示意图一；

[0082] 图3为本申请提供的车辆ECU认证方法的流程示意图二；

[0083] 图4为本发明实施例提供的车辆ECU认证方法的流程示意图三；

[0084] 图5为本发明实施例提供的一种车辆ECU认证装置的结构示意图；

[0085] 图6为本发明实施例提供的另一种车辆ECU认证装置的结构示意图；

[0086] 图7为本发明实施例提供的车辆ECU认证装置的硬件结构示意图。

具体实施方式

[0087] 为使本发明实施例的目的、技术方案和优点更加清楚，下面将结合本发明实施例

中的附图，对本发明实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例是本发明一部分实施例，而不是全部的实施例。基于本发明中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本发明保护的范围。

[0088] 图1为本申请提供的车辆中ECU的示意图。请参见图1，在车辆中包括多个ECU和控制器局域网络(Controller Area Network，简称CAN)。

[0089] 可选的，ECU可以根据车辆的运行状态，生成对车辆的控制信息。控制信息通过CAN总线传输至车辆的机械部件或者其它ECU。为了保证通信的安全性，在一个ECU与另一个ECU进行通信之前，该两个ECU之间需要进行身份认证。

[0090] 需要说明的是，图1只是以示例的形式示意车辆中的ECU，并非对车辆中ECU的限定。

[0091] 在本申请中，在不同的ECU进行身份认证时，依据随机数、ECU的标识和时间戳，由于随机数是随机生成的，且不同身份认证过程中的随机数不同，不同身份认证过程中的时间戳也不同，因此，即使一次身份认证中的随机数和时间戳被破解，也无法应用于下次的身份认证过程中，进而提高身份认证的安全性。

[0092] 下面，通过具体实施例对本申请所示的技术方案进行详细说明。需要说明的是，下面几个具体实施例可以相互结合，对于相同或相似的内容，在不同的实施例中不再进行重复说明。

[0093] 图2为本申请提供的车辆ECU认证方法的流程示意图一。请参见图2，该方法可以包括：

[0094] S201、第一ECU生成随机数。

[0095] 可选的，第一ECU可以为车辆中任意一个ECU。

[0096] 可选的，车辆可以为汽车、火车、地铁等。

[0097] 当然，在实际应用过程中，可以根据实际需要设置车辆的类型，本发明实施例对此不作具体限定。

[0098] 可选的，随机数可以为任意的字符序列。

[0099] 例如，随机数可以包括数字、字母以及符号中的任意一种或多种。

[0100] S202、第一ECU向第二ECU发送随机数。

[0101] 可选的，第二ECU可以为车辆中任意一个ECU。

[0102] 可选的，第二ECU可以与第一ECU进行通信。

[0103] S203、第二ECU根据随机数、第二ECU的标识和时间戳生成第一认证数据。

[0104] 可选的，可以通过字符序列标识时间戳，通过时间戳可以唯一的标识某一时刻的时间。

[0105] 可选的，第二ECU可以通过哈希消息认证码(Hash-based Message Authentication Code，简称HMAC)算法，对随机数、第二ECU的标识和时间戳进行运算，以生成第一认证数据。

[0106] 可选的，可以将第二ECU的标识作为HMAC算法的秘钥，随机数和时间戳作为HMAC加密算法中的数据(data)，利用HMAC算法进行加密，接人得到第一认证数据。

[0107] 需要说明的是，在实际应用过程中，可以根据实际需要通过其它算法对随机数、第二ECU的标识和时间戳进行运算，以生成第一认证数据。

[0108] 需要说明的是，在第二ECU生成第一认证数据时，还可以基于其它参数，本发明实施例对此不作具体限定。

[0109] S204、第二ECU向第一ECU发送第一认证数据和时间戳。

[0110] 可选的，第二ECU可以分别向第一ECU发送第一认证数据和时间戳。即，第二ECU以两条消息的形式，向第一ECU发送第一认证数据和时间戳，其中，第一认证数据和时间戳位于相同不同的消息中。

[0111] 可选的，第二ECU还可以以一条消息的形式向第一ECU发送第一认证数据和时间戳。

[0112] 例如，第二ECU还可以向第一ECU发送第二消息，并在第二消息中携带认证数据和时间戳。

[0113] 当第二ECU通过一条消息的形式向第一ECU发送第一认证数据和时间戳时，由于减少了发送消息的次数，进而可以节省信令开销。

[0114] S205、第一ECU根据随机数、第二ECU的标识和时间戳，生成第二认证数据。

[0115] 可选的，第一ECU可以先获取第二ECU的标识和时间戳。

[0116] 可选的，第二ECU可以向第一ECU发送第一消息，第一消息中携带第二ECU的标识和时间戳。相应的，第二ECU可以在第一消息中获取第二ECU的标识和时间戳。

[0117] 可选的，第一ECU可以通过HMAC算法，对随机数、第二ECU的标识和时间戳进行运算，以生成第二认证数据。

[0118] 可选的，可以将第二ECU的标识作为HMAC算法的秘钥，随机数和时间戳作为HMAC加密算法中的数据(data)，利用HMAC算法进行加密，进而得到第二认证数据。

[0119] 可选的，第一ECU生成第二认证数据所采用的算法，与第二ECU生成第一认证数据所采用的算法相同。

[0120] 可选的，第一ECU和第二ECU可以预先约定生成认证数据所采用的算法。

[0121] 需要说明的是，在第一ECU生成第二认证数据时，还可以基于其它参数，本发明实施例对此不作具体限定。

[0122] S206、第一ECU根据第一认证数据和第二认证数据，对第二ECU的身份进行认证。

[0123] 可选的，第一ECU可以判断第一认证数据和第二认证数据是否相同；若是，则对第二ECU的身份认证成功；若否，则对第二ECU的身份认证失败。

[0124] 可选的，在第一ECU对第二ECU的身份认证成功时，第一ECU可以向第二ECU发送认证成功响应消息。在第一ECU对第二ECU的身份认证失败时，第一ECU可以向第二ECU发送认证失败响应消息。

[0125] 需要说明的是，在第一ECU对第二ECU身份认证通过之后，第二ECU可以向第一ECU发送接入请求，进而实现第一ECU和第二ECU之间的数据通信。

[0126] 需要说明的是，第二ECU采用预设算法，根据随机数、时间戳和第二ECU的标识，生成第一认证数据，并向第一ECU发送第一认证数据和时间戳，以使第一ECU可以采用预设算法，根据随机数、时间戳和第二ECU的标识，生成第二认证数据，第一ECU根据第一认证数据和第二认证数据对第二ECU的身份进行认证。在受到网络攻击时，当通过网络传输的随机数、时间戳、第二ECU的标识和第一认证数据中的任意一个被篡改时，则导致第一认证数据和第二认证数据不同，使得第一ECU对第二ECU的身份认证失败，进而无法建立第一ECU和第

二ECU之间的通信。

[0127] 本申请提供的车辆ECU认证方法，第一ECU生成随机数，并向第二ECU发送随机数，第二ECU根据随机数、第二ECU的标识和时间戳生成第一认证数据，第二ECU向第一ECU发送第一认证数据和时间戳。第一ECU根据随机数、第二ECU的标识和时间戳，生成第二认证数据，并根据第一认证数据和第二认证数据，对第二ECU的身份进行认证。在上述过程中，认证数据是依据随机数、第二ECU的标识和时间戳生成的，由于随机数是随机生成的，且不同身份认证过程中的随机数不同，不同身份认证过程中的时间戳也不同，因此，即使一次身份认证中的随机数和时间戳被破解，也无法应用于下次的身份认证过程中，进而提高身份认证的安全性。进一步的，若第二ECU向第一ECU发送的随机数、时间戳、第二ECU的标识和第一认证数据中的任意一个被篡改，则第一ECU对第二ECU的身份认证失败，进而提高了车辆ECU身份认证的安全性。

[0128] 在实际应用过程中，可选的，当第二ECU需要与第一ECU进行通信时，第二ECU向第一ECU发送认证请求，以请求第一ECU对第二ECU进行身份认证，具体的，请参见图3所示的实施例。

[0129] 图3为本申请提供的车辆ECU认证方法的流程示意图二。在图2所示实施例的基础上，请参见图3，该方法可以包括：

[0130] S301、第二ECU向第一ECU发送认证请求消息。

[0131] 可选的，第一ECU和第二ECU可以为车辆中任意两个可以进行通信的ECU。

[0132] 其中，第二ECU向第一ECU发送的认证请求消息用于请求第一ECU对第二ECU的身份进行认证。

[0133] 可选的，当第二ECU需要与第一ECU进行通信时，第二ECU向第一ECU发送认证请求。

[0134] 例如，当第二ECU需要向第一ECU发送控制指令时，第二ECU可以向第一ECU发送的认证请求。

[0135] S302、第一ECU根据认证请求消息，生成随机数。

[0136] S303、第一ECU向第二ECU发送随机数。

[0137] S304、第二ECU生成时间戳，并根据随机数、第二ECU的标识和时间戳生成第一认证数据。

[0138] 需要说明的是，S302-S304的执行过程可以参见S201-S203的执行过程，此处不再进行赘述。

[0139] S305、第二ECU向第一ECU发送第一认证数据、时间戳和第二ECU的标识。

[0140] 可选的，第二ECU可以向第一ECU发送第一认证数据和第一消息，其中，第一消息中包括时间戳和第二ECU的标识。

[0141] 可选的，第二ECU可以向第一ECU发送第三消息，第三消息中包括第一认证数据、时间戳和第二ECU的标识。

[0142] S306、第一ECU根据随机数、第二ECU的标识和时间戳，生成第二认证数据。

[0143] S307、第一ECU根据第一认证数据和第二认证数据，对第二ECU的身份进行认证。

[0144] 需要说明的是，S306-S307的执行过程可以参见S205-S206的执行过程，此处不再进行赘述。

[0145] 在图3所示的实施例中，在第二ECU需要与第一ECU建立通信之前，第二ECU先向第

一ECU发送认证请求消息，以请求第一ECU对第二ECU的身份进行认证。由于认证数据是根据随机数、第二ECU的标识和时间戳生成的，由于随机数是随机生成的，且不同身份认证过程中的随机数不同，不同身份认证过程中的时间戳也不同，因此，即使一次身份认证中的随机数和时间戳被破解，也无法应用于下次的身份认证过程中，进而提高身份认证的安全性。进一步的，若第二ECU向第一ECU发送的随机数、时间戳、第二ECU的标识和第一认证数据中的任意一个被篡改，则第一ECU对第二ECU的身份认证失败，进而提高了车辆ECU身份认证的安全性。

[0146] 在上述任意一个实施例的基础上，可选的，为了进一步提高身份认证的安全性，在生成认证数据时，还可以基于认证请求消息，具体的，请参见图4所示的实施例。

[0147] 图4为本发明实施例提供的车辆ECU认证方法的流程示意图三。在上述任意一个实施例的基础上，请参见图4，该方法可以包括：

[0148] S401、第二ECU向第一ECU发送认证请求消息，认证请求消息中包括第二ECU的标识。

[0149] 需要说明的时，S401的执行过程可以参见S301，本发明实施例此处不再进行赘述。

[0150] S402、第一ECU根据认证请求消息，生成随机数。

[0151] S403、第一ECU向第二ECU发送随机数。

[0152] 需要说明的时，S302的执行过程可以参见S202，本发明实施例此处不再进行赘述。

[0153] S404、第二ECU生成时间戳，并根据随机数、第二ECU的标识、时间戳和认证请求消息，生成第一认证数据。

[0154] 可选的，第一ECU可以通过HMAC算法，对随机数、第二ECU的标识、时间戳和认证请求消息进行运算，以生成第一认证数据。

[0155] 可选的，可以将第二ECU的标识作为HMAC算法的秘钥，随机数、时间戳和认证请求消息作为HMAC加密算法中的数据(data)，利用HMAC算法进行加密，进而得到第一认证数据。

[0156] 需要说明的是，在实际应用过程中，可以根据实际需要通过其它算法对随机数、第二ECU的标识、时间戳和认证请求消息进行运算，以生成第一认证数据。

[0157] S405、第二ECU向第一ECU发送第一认证数据和时间戳。

[0158] 需要说明的时，S405的执行过程可以参见S204，本发明实施例此处不再进行赘述。

[0159] S406、第一ECU在认证请求消息中获取第二ECU的标识。

[0160] S407、第一ECU根据随机数、第二ECU的标识、时间戳和认证请求消息，生成第二认证数据。

[0161] 可选的，第一ECU可以通过HMAC算法，对随机数、第二ECU的标识、时间戳和认证请求消息进行运算，以生成第二认证数据。

[0162] 可选的，可以将第二ECU的标识作为HMAC算法的秘钥，随机数、时间戳和认证请求消息作为HMAC加密算法中的数据(data)，利用HMAC算法进行加密，进而得到第二认证数据。

[0163] 可选的，第一ECU生成第二认证数据所采用的算法，与第二ECU生成第一认证数据所采用的算法相同。

[0164] 可选的，第一ECU和第二ECU可以预先约定生成认证数据所采用的算法。

[0165] S408、第一ECU根据第一认证数据和第二认证数据，对第二ECU的身份进行认证。

[0166] 需要说明的时，S408的执行过程可以参见S206，本发明实施例此处不再进行赘述。

[0167] 需要说明的是，第二ECU采用预设算法，根据随机数、时间戳、第二ECU的标识和认证请求消息，生成第一认证数据，并向第一ECU发送第一认证数据和时间戳，以使第一ECU可以采用预设算法，根据随机数、时间戳、第二ECU的标识和认证请求消息，生成第二认证数据，第一ECU根据第一认证数据和第二认证数据对第二ECU的身份进行认证。在受到网络攻击时，当通过网络传输的随机数、时间戳、第二ECU的标识、认证请求消息和第一认证数据中的任意一个被篡改时，则导致第一认证数据和第二认证数据不同，进而使得第一ECU对第二ECU的身份认证失败，进而无法建立第一ECU和第二ECU之间的通信。

[0168] 在图4所示的实施例中，在第二ECU需要与第一ECU建立通信之前，第二ECU先向第一ECU发送认证请求消息，该认证请求消息中包括第二ECU的标识，第一ECU生成随机数，并向第二ECU发送随机数，第二ECU根据随机数、第二ECU的标识、时间戳和认证请求消息生成第一认证数据，第二ECU向第一ECU发送第一认证数据和时间戳。第一ECU在认证请求消息中获取第二ECU的标识，并根据随机数、第二ECU的标识、时间戳和认证请求消息，生成第二认证数据，并根据第一认证数据和第二认证数据，对第二ECU的身份进行认证。在上述过程中，认证数据是依据随机数、第二ECU的标识、时间戳和认证请求消息生成的，由于随机数是随机生成的，且不同身份认证过程中的随机数、时间戳以及认证请求消息均不同，因此，即使一次身份认证中的随机数、时间戳和认证请求消息被破解，也无法应用于下次的身份认证过程中，进而提高身份认证的安全性。进一步的，若第二ECU向第一ECU发送的随机数、时间戳、第二ECU的标识、第一认证数据和认证请求消息中的任意一个被篡改，则第一ECU对第二ECU的身份认证失败，进而提高了车辆ECU身份认证的安全性。

[0169] 图5为本发明实施例提供的一种车辆ECU认证装置的结构示意图。请参见图5，该车辆ECU认证装置10可以包括生成模块11、发送模块12、接收模块13、获取模块14和认证模块15，其中，

[0170] 所述生成模块11用于，生成随机数；

[0171] 所述发送模块12用于，向第二ECU发送所述随机数；

[0172] 所述接收模块13用于，接收所述第二ECU发送的第一认证数据，所述第一认证数据为所述第二ECU根据所述随机数、所述第二ECU的标识和时间戳生成的；

[0173] 所述获取模块14用于，获取所述第二ECU的标识和所述时间戳；

[0174] 所述生成模块11还用于，根据所述随机数、所述第二ECU的标识和所述时间戳，生成第二认证数据；

[0175] 所述认证模块15用于，根据所述第一认证数据和所述第二认证数据，对所述第二ECU的身份进行认证。

[0176] 本发明实施例提供的车辆ECU认证装置可以执行上述方法实施例所示的技术方案，其实现原理以及有益效果类似，此处不再进行赘述。

[0177] 在一种可能的实施方式中，所述接收模块13还用于，在所述生成模块11生成随机数之前，接收所述第二ECU发送的认证请求消息；相应的，所述第一认证数据具体为所述第二ECU根据所述随机数、所述第二ECU的标识、时间戳和所述认证请求消息生成的；

[0178] 所述生成模块11具体用于，根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息，生成第二认证数据。

[0179] 在另一种可能的实施方式中，所述时间戳为所述第二ECU在接收到所述随机数之

后生成的；

[0180] 所述接收模块13还用于，接收所述第二ECU发送的第一消息，所述第一消息包括所述时间戳；

[0181] 所述获取模块14具体用于，从所述第一消息中获取所述时间戳。

[0182] 在另一种可能的实施方式中，所述第一消息还包括所述第二ECU的标识；所述获取模块14具体用于：

[0183] 从所述第一消息中获取所述第二ECU的标识。

[0184] 在另一种可能的实施方式中，所述获取模块14具体用于：

[0185] 从所述认证请求消息中获取所述第二ECU的标识。

[0186] 在另一种可能的实施方式中，所述生成模块11具体用于：

[0187] 通过预设算法，并根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息进行运算，得到所述第二认证数据。

[0188] 在另一种可能的实施方式中，所述认证模块11具体用于：

[0189] 判断所述第一认证数据和所述第二认证数据是否相同；

[0190] 若是，则对所述第二ECU的身份认证成功；

[0191] 若否，则对所述第二ECU的身份认证失败。

[0192] 本发明实施例提供的车辆ECU认证装置可以执行上述方法实施例所示的技术方案，其实现原理以及有益效果类似，此处不再进行赘述。

[0193] 图6为本发明实施例提供的另一种车辆ECU认证装置的结构示意图。请参见图6，车辆ECU认证装置20可以包括接收模块21、生成模块22和发送模块23，其中，

[0194] 所述接收模块21用于，接收第一ECU发送的随机数；

[0195] 所述生成模块22用于，生成时间戳，并根据所述随机数、第二ECU的标识和所述时间戳生成第一认证数据；

[0196] 所述发送模块23用于，向所述第一ECU发送所述第一认证数据。

[0197] 本发明实施例提供的车辆ECU认证装置可以执行上述方法实施例所示的技术方案，其实现原理以及有益效果类似，此处不再进行赘述。

[0198] 在另一种可能的实施方式中，所述发送模块23还用于，在所述接收模块21接收所述第一ECU发送的随机数之前，向所述第一ECU发送认证请求消息。

[0199] 在另一种可能的实施方式中，所述生成模块22具体用于：

[0200] 所述第二ECU根据所述随机数、所述第二ECU的标识、所述时间戳和所述认证请求消息生成第一认证数据。

[0201] 在另一种可能的实施方式中，所述认证请求消息中包括所述第二ECU的标识。

[0202] 在另一种可能的实施方式中，所述发送模块23还用于，在所述生成模块22生成时间戳之后，向所述第一ECU发送所述时间戳。

[0203] 本发明实施例提供的车辆ECU认证装置可以执行上述方法实施例所示的技术方案，其实现原理以及有益效果类似，此处不再进行赘述。

[0204] 图7为本发明实施例提供的车辆ECU认证装置的硬件结构示意图。如图7所示，该车辆ECU认证装置30包括：至少一个处理器31和存储器32。可选地，该车辆ECU认证装置30还包括通信部件33。其中，处理器31、存储器32以及通信部件33通过总线34连接。

[0205] 可选的，车辆ECU认证装置30可以设置在上述第一ECU中，也可以设置在上述第二ECU中。

[0206] 在具体实现过程中，至少一个处理器31执行所述存储器32存储的计算机执行指令，使得至少一个处理器31执行如上方法实施例所示的方法。可选的，处理器31可以执行上述方法实施例中第一ECU的执行步骤，以及第二ECU的执行步骤。

[0207] 通信部件33可以与其它部件(例如其它ECU)进行数据交互。

[0208] 处理器31的具体实现过程可参见上述方法实施例，其实现原理和技术效果类似，本实施例此处不再赘述。

[0209] 在上述的图7所示的实施例中，应理解，处理器可以是中央处理单元(英文：Central Processing Unit，简称:CPU)，还可以是其他通用处理器、数字信号处理器(英文：Digital Signal Processor，简称:DSP)、专用集成电路(英文:Application Specific Integrated Circuit，简称:ASIC)等。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。结合发明所公开的方法的步骤可以直接体现为硬件处理器执行完成，或者用处理器中的硬件及软件模块组合执行完成。

[0210] 存储器可能包含高速RAM存储器，也可能还包括非易失性存储NVM，例如至少一个磁盘存储器。

[0211] 总线可以是工业标准体系结构(Industry Standard Architecture，ISA)总线、外部设备互连(Peripheral Component，PCI)总线或扩展工业标准体系结构(Extended Industry Standard Architecture，EISA)总线等。总线可以分为地址总线、数据总线、控制总线等。为便于表示，本申请附图中的总线并不限定仅有一根总线或一种类型的总线。

[0212] 本申请还提供一种计算机可读存储介质，所述计算机可读存储介质中存储有计算机执行指令，当处理器执行所述计算机执行指令时，实现如上所述的方法实施例所示的方法。

[0213] 上述的计算机可读存储介质，上述可读存储介质可以是由任何类型的易失性或非易失性存储设备或者它们的组合实现，如静态随机存取存储器(SRAM)，电可擦除可编程只读存储器(EEPROM)，可擦除可编程只读存储器(EPROM)，可编程只读存储器(PROM)，只读存储器(ROM)，磁存储器，快闪存储器，磁盘或光盘。可读存储介质可以是通用或专用计算机能够存取的任何可用介质。

[0214] 一种示例性的可读存储介质耦合至处理器，从而使处理器能够从该可读存储介质读取信息，且可向该可读存储介质写入信息。当然，可读存储介质也可以是处理器的组成部分。处理器和可读存储介质可以位于专用集成电路(Application Specific Integrated Circuits，简称:ASIC)中。当然，处理器和可读存储介质也可以作为分立组件存在于设备中。

[0215] 所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

[0216] 所述作为分离部件说明的单元可以是或者也可以不是物理上分开的，作为单元显示的部件可以是或者也可以不是物理单元，即可以位于一个地方，或者也可以分布到多个

网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0217] 另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。

[0218] 所述功能如果以软件功能单元的形式实现并作为独立的产品销售或使用时，可以存储在一个计算机可读取存储介质中。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分或者该技术方案的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质中，包括若干指令用以使得一台计算机设备(可以是个人计算机，服务器，或者网络设备等)执行本发明各个实施例所述方法的全部或部分步骤。而前述的存储介质包括：U盘、移动硬盘、只读存储器(ROM，Read-Only Memory)、随机存取存储器(RAM，Random Access Memory)、磁碟或者光盘等各种可以存储程序代码的介质。

[0219] 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。

[0220] 最后应说明的是：以上各实施例仅用以说明本发明实施例的技术方案，而非对其限制；尽管参照前述各实施例对本发明实施例进行了详细的说明，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实施例方案的范围。

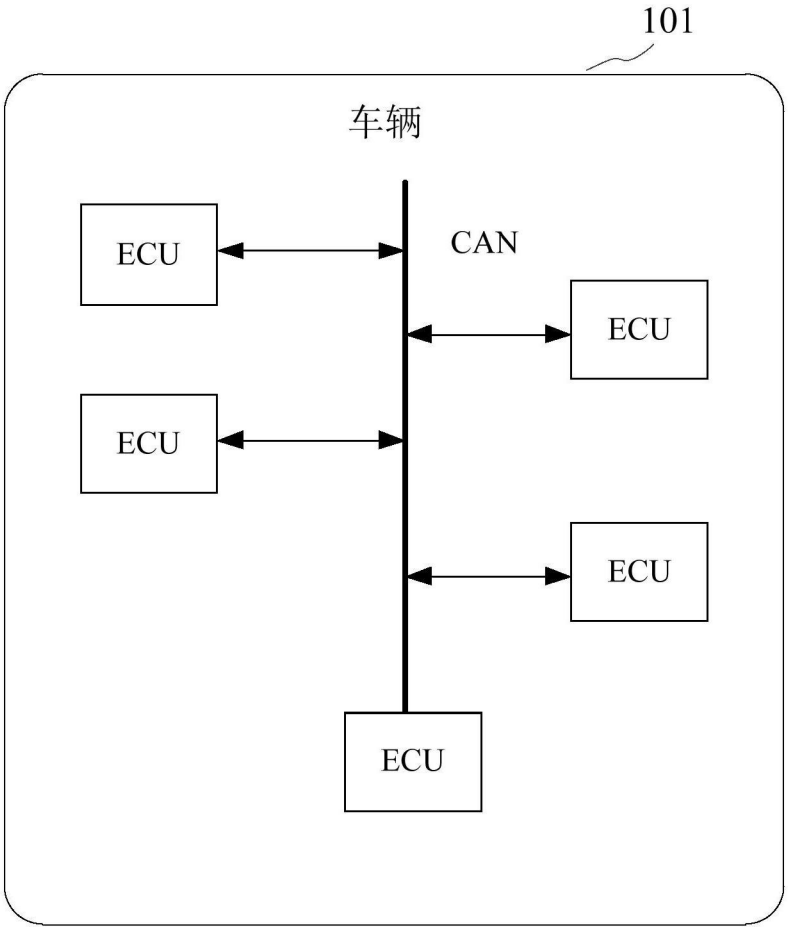


图1

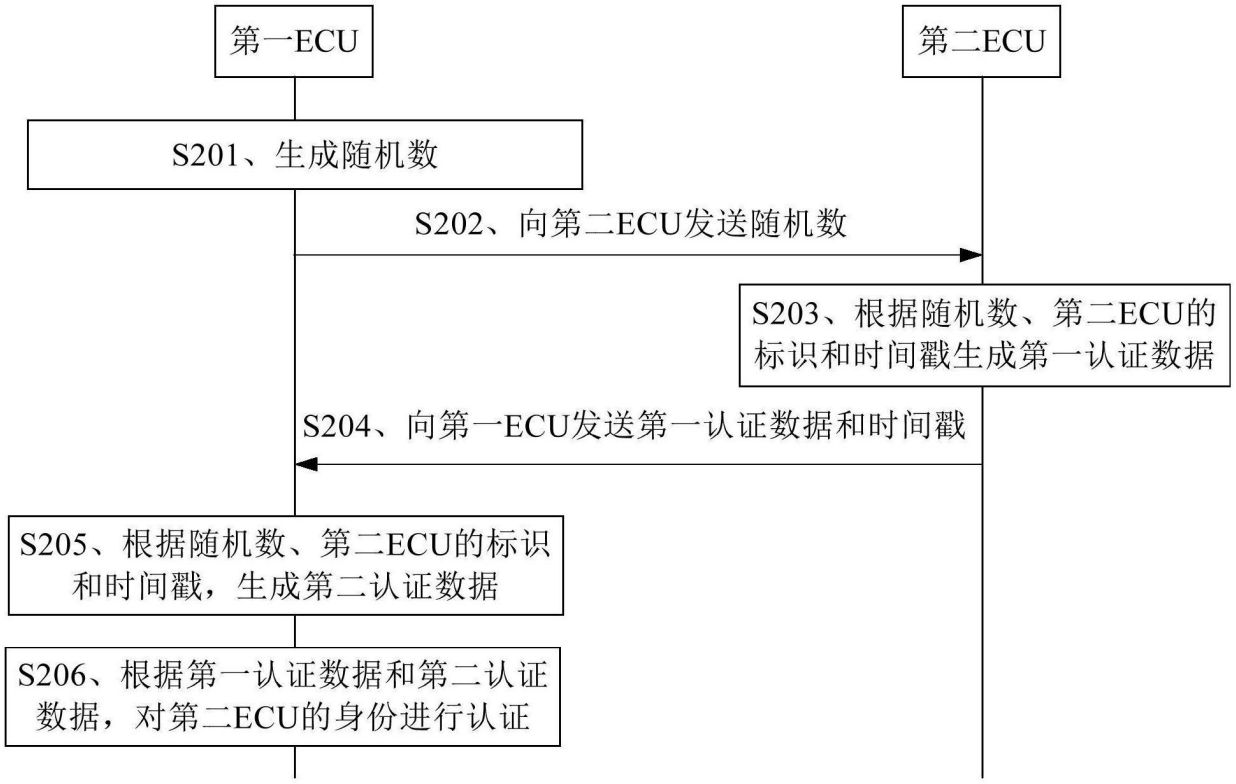

第一ECU
第二ECU
S201、生成随机数
S202、向第二ECU发送随机数
S203、根据随机数、第二ECU的标识和时间戳生成第一认证数据
S204、向第一ECU发送第一认证数据和时间戳
S205、根据随机数、第二ECU的标识和时间戳，生成第二认证数据
S206、根据第一认证数据和第二认证数据，对第二ECU的身份进行认证

图2

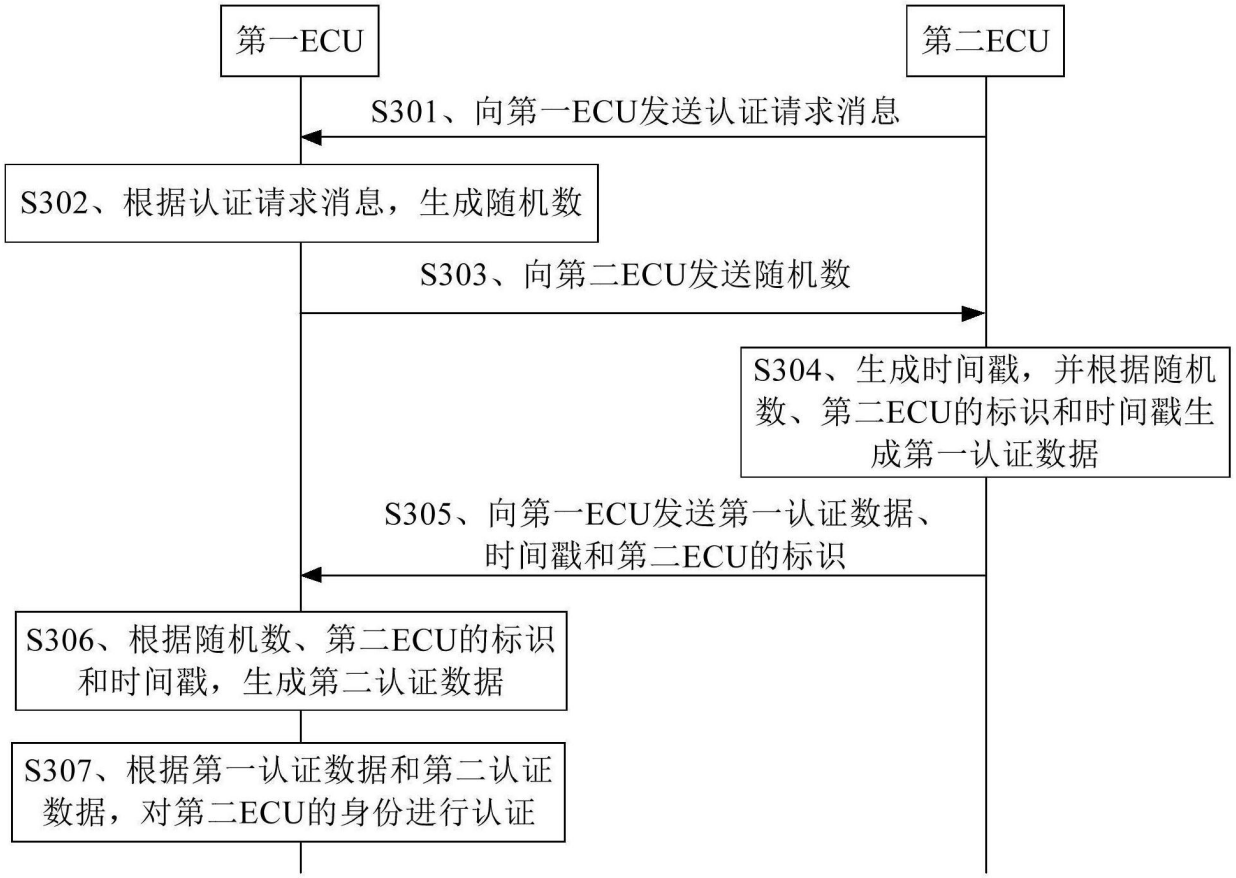

第一ECU
第二ECU
S301、向第一ECU发送认证请求消息
S302、根据认证请求消息，生成随机数
S303、向第二ECU发送随机数
S304、生成时间戳，并根据随机数、第二ECU的标识和时间戳生成第一认证数据
S305、向第一ECU发送第一认证数据、时间戳和第二ECU的标识
S306、根据随机数、第二ECU的标识和时间戳，生成第二认证数据
S307、根据第一认证数据和第二认证数据，对第二ECU的身份进行认证

图3

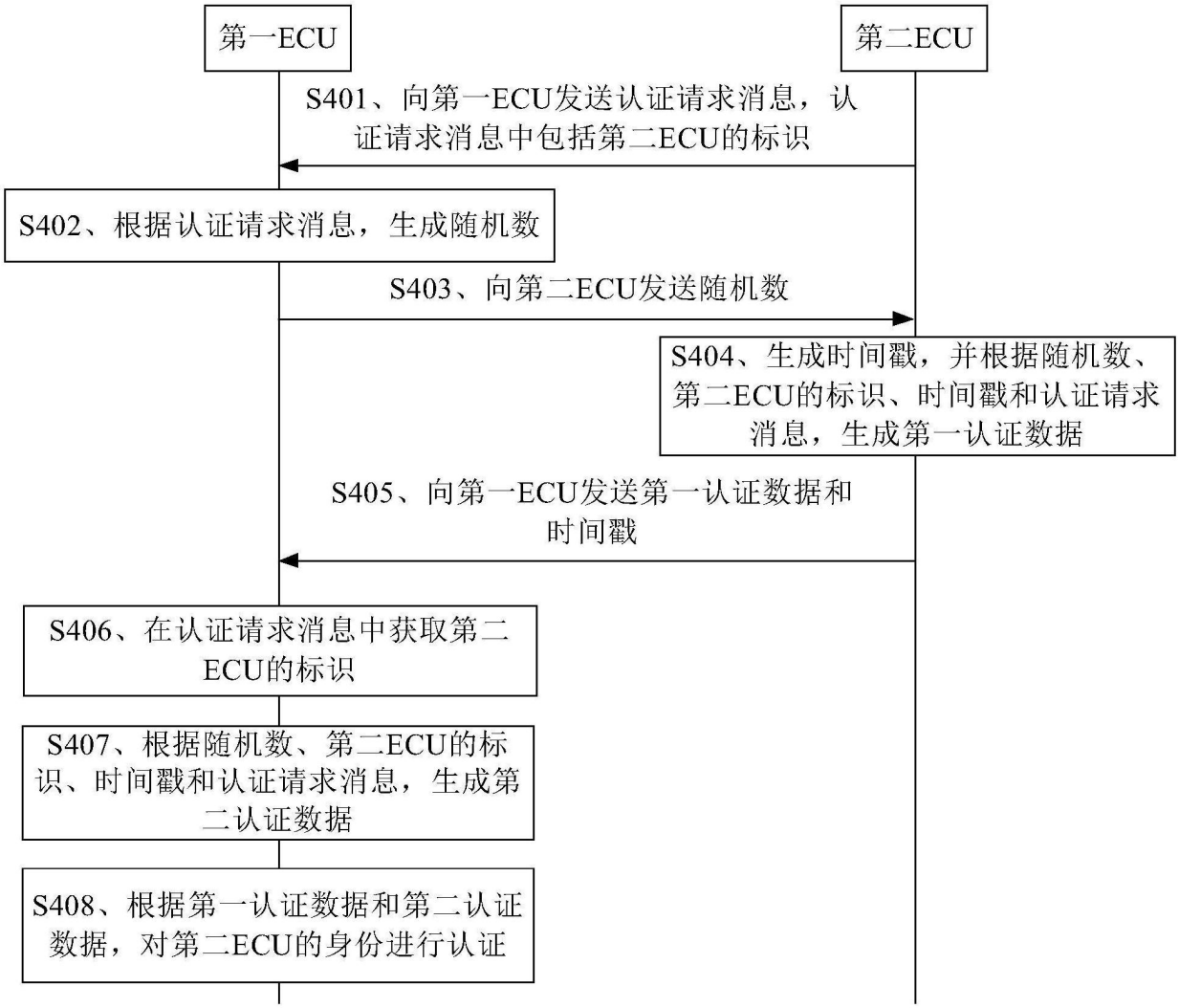

第一ECU
第二ECU
S401、向第一ECU发送认证请求消息，认证请求消息中包括第二ECU的标识
S402、根据认证请求消息，生成随机数
S403、向第二ECU发送随机数
S404、生成时间戳，并根据随机数、第二ECU的标识、时间戳和认证请求消息，生成第一认证数据
S405、向第一ECU发送第一认证数据和时间戳
S406、在认证请求消息中获取第二ECU的标识
S407、根据随机数、第二ECU的标识、时间戳和认证请求消息，生成第二认证数据
S408、根据第一认证数据和第二认证数据，对第二ECU的身份进行认证

图4

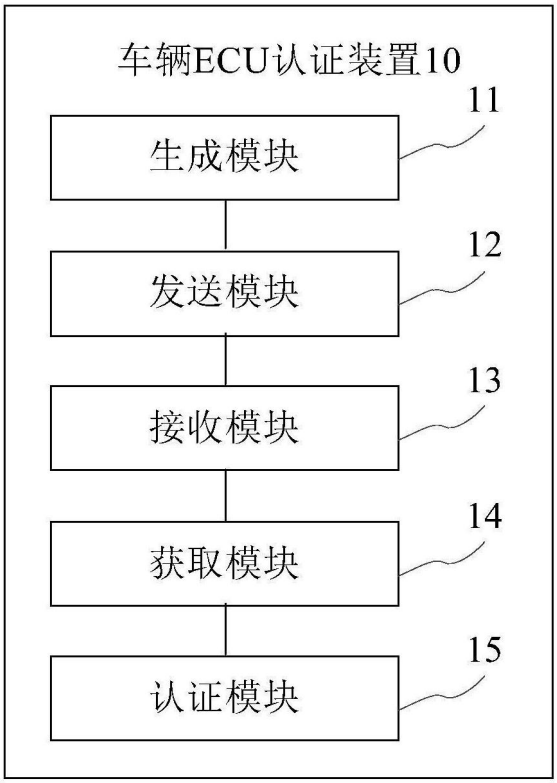

车辆ECU认证装置10
11
生成模块
12
发送模块
13
接收模块
14
获取模块
15
认证模块

图5

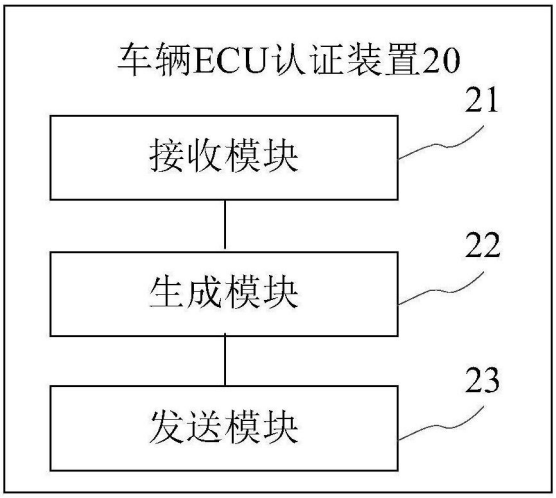

车辆ECU认证装置20
21
接收模块
22
生成模块
23
发送模块

图6

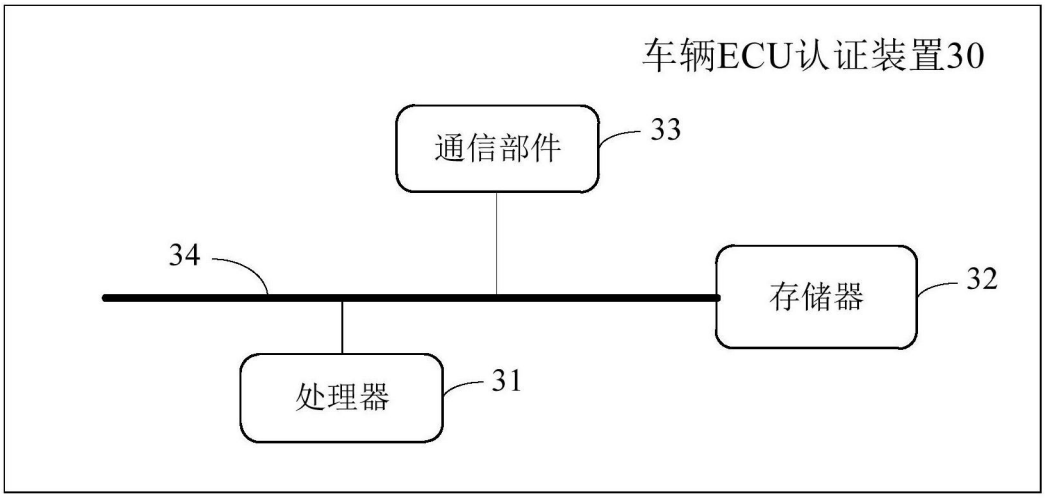


图7