(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 115242410 B
(45)授权公告日 2022.11.29

(21)申请号 202211154415.5
(22)申请日 2022.09.22
(65)同一申请的已公布的文献号
申请公布号 CN 115242410 A
(43)申请公布日 2022.10.25
(73)专利权人 合肥工业大学
地址 230009 安徽省合肥市包河区屯溪路193号
(72)发明人 程腾 刘强 吴泽旭 石琴
(74)专利代理机构 合肥和瑞知识产权代理事务所(普通合伙) 34118
专利代理师 王挺
(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
(56)对比文件
CN 105245406 A,2016.01.13
WO 2022025321 A1,2022.02.03
CN 113114699 A,2021.07.13
CN 106533655 A,2017.03.22
CN 112994898 A,2021.06.18
CN 111880444 A,2020.11.03
CN 113141344 A,2021.07.20
CN 111740825 A,2020.10.02
CN 109728909 A,2019.05.07
CN 107273152 A,2017.10.20
CN 107104791 A,2017.08.29
CN 107426187 A,2017.12.01
CN 103856939 A,2014.06.11
万爱兰,韩牟,马世典,王运文,华蕾 ,冯晓林.基于一次性密码本的车内网身份认证协议.《计算机工程》.2018,第44卷(第6期),第141-146及161页.
石润华,石泽.基于区块链技术的物联网密钥管理方案.《信息网络安全》.2020,第20卷(第8期),第1-8页.
(续)
审查员 王丹

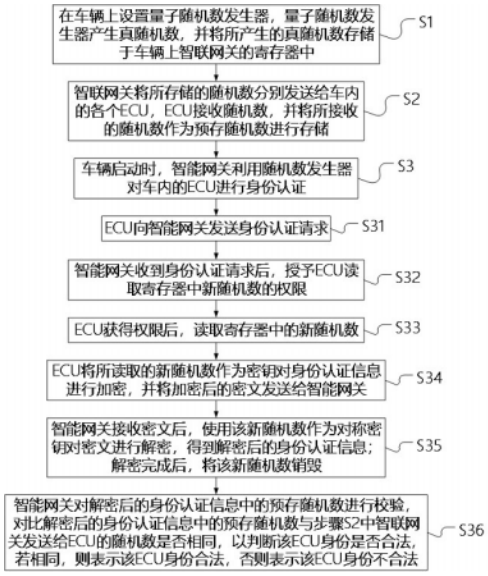
权利要求书1页 说明书5页 附图3页

(54)发明名称

一种基于量子随机数发生器的车内网身份认证方法

(57)摘要

本发明公开了一种基于量子随机数发生器的车内网身份认证方法,涉及车内网技术领域,在车辆上设置量子随机数发生器用于产生真随机数,并将真随机数存储于车辆智联网关的寄存器中;首先,智联网关将随机数发送给各个ECU作为ECU的预存随机数;然后车辆每启动时,智能网关再利用随机数发生器对车内的ECU进行身份认证,认证过程中ECU利用随机数发生器产生的新随机数作为密钥,对包含有该ECU预存随机数的身份认证信息进行加密,智能网关利用新随机数对密文进行解密,解密后将新随机数销毁,并对解密后的身份认证信息中的预存随机数进行校验,判断该ECU身份是否合法,解决了目前车内网中缺少ECU身份认证的问题。



CN 115242410 B

[转续页]

[接上页]

(56)对比文件

Huixian Gao;Jiapeng Xiu;Zhengqiu Yang;Chaoyu Tian.A key generation algorithm supporting SecOC framework for secure onboard communication.《 2021 6th International Symposium on Computer and Information Processing Technology (ISCIPT)》.2021,

Basker Palaniswamy,Seyit Camtepe, Ernest Foo,Josef Pieprzyk.An Efficient Authentication Scheme for Intra-Vehicular Controller Area Network.《 IEEE Transactions on Information Forensics and Security》.2020,第15卷第3107-3122页.

1.一种基于量子随机数发生器的车内网身份认证方法,其特征在于,包括以下步骤:

S1,在车辆上设置随机数发生器,所述随机数发生器用于产生随机数,并将所产生的随机数存储于车辆上的智联网关的寄存器中;

S2,智联网关将所存储的随机数分别发送给车内的各个ECU即电子控制单元;所述ECU接收随机数,并将所接收的随机数作为预存随机数进行存储;

S3,车辆每启动时,智能网关利用随机数发生器对车内的ECU进行身份认证,认证过程为:

S31,ECU向智能网关发送身份认证请求;

S32,智能网关收到该ECU的身份认证请求后,授予该ECU读取寄存器中新随机数的权限;

S33,ECU获得权限后,读取寄存器中的新随机数;所述寄存器中的新随机数为随机数发生器新产生的随机数;

S34,ECU将所读取的新随机数作为密钥对身份认证信息进行加密,并将加密后的密文发送给智能网关;所述身份认证信息中包含ECU的MAC信息以及预存随机数;

S35,智能网关接收密文后,使用该新随机数作为对称密钥对密文进行解密,得到解密后的身份认证信息;解密完成后,智能网关对该新随机数进行销毁;

S36,智能网关对解密后的身份认证信息中的预存随机数进行校验,对比解密后的身份认证信息中的预存随机数与步骤S2中智联网关发送给ECU的随机数是否相同,以判断该ECU身份是否合法,若相同,则表示该ECU身份合法,否则表示该ECU身份不合法。

2.根据权利要求1所述的一种基于量子随机数发生器的车内网身份认证方法,其特征在于,所述随机数发生器为量子随机数发生器,用于产生真随机数。

3.根据权利要求1所述的一种基于量子随机数发生器的车内网身份认证方法,其特征在于,步骤S2中,智联网关向车内的各个ECU所发送的随机数均不相同,即车内的各个ECU的预存随机数均不相同。

一种基于量子随机数发生器的车内网身份认证方法

技术领域

[0001] 本发明涉及车内网技术领域,尤其是一种基于量子随机数发生器的车内网身份认证方法。

背景技术

[0002] 车内网是实现单车智能网联的基础技术。车内网是指基于成熟的CAN总线技术建立一个标准化整车网络(CAN网络),实现车内各电子控制单元(Electronic Control Unit,简称ECU)间的状态信息和控制信号在车内网上的传输,使车辆能够实现状态感知、故障诊断和智能控制等功能。

[0003] 车内网的技术核心是CAN总线技术。CAN总线通过遍布车身的传感器,将车辆的各种行驶数据发送到“总线”上,从而使需要这些数据的接收端都可以从“总线”上读取需要的信息,实现车辆发动机、自动变速箱、ABS、安全气囊等单元之间的通讯,做到全车信息及时共享,最终促进车辆安全行驶、舒适和可靠。

[0004] 目前车内网中缺少可行的身份认证机制与加密机制,由于在CAN总线上增加电子控制单元(ECU)对系统没有明显影响,且车内网的通信为明文通信,因此,外部随意接入的ECU都可以读取到车内网中的信息。

发明内容

[0005] 为了克服上述现有技术中的缺陷,本发明提供一种基于量子随机数发生器的车内网身份认证方法,解决了目前车内网中缺少ECU身份认证的问题,弥补了车内网明文通信所造成的缺陷。

[0006] 为实现上述目的,本发明采用以下技术方案,包括:

[0007] 一种基于量子随机数发生器的车内网身份认证方法,包括以下步骤:

[0008] S1,在车辆上设置随机数发生器,所述随机数发生器用于产生随机数,并将所产生的随机数存储于车辆上的智联网关的寄存器中;

[0009] S2,智联网关将所存储的随机数分别发送给车内的各个ECU即电子控制单元;所述ECU接收随机数,并将所接收的随机数作为预存随机数进行存储;

[0010] S3,车辆每启动时,智能网关利用随机数发生器对车内的ECU进行身份认证,认证过程为:

[0011] S31,ECU向智能网关发送身份认证请求;

[0012] S32,智能网关收到该ECU的身份认证请求后,授予该ECU读取寄存器中新随机数的权限;

[0013] S33,ECU获得权限后,读取寄存器中的新随机数;所述寄存器中的新随机数为随机数发生器新产生的随机数;

[0014] S34,ECU将所读取的新随机数作为密钥对身份认证信息进行加密,并将加密后的密文发送给智能网关;所述身份认证信息中包含ECU的MAC信息以及预存随机数;

[0015] S35,智能网关接收密文后,使用该新随机数作为对称密钥对密文进行解密,得到解密后的身份认证信息;解密完成后,智能网关对该新随机数进行销毁;

[0016] S36,智能网关对解密后的身份认证信息中的预存随机数进行校验,对比解密后的身份认证信息中的预存随机数与步骤S2中智联网关发送给ECU的随机数是否相同,以判断该ECU身份是否合法,若相同,则表示该ECU身份合法,否则表示该ECU身份不合法。

[0017] 优选的,所述随机数发生器为量子随机数发生器,用于产生真随机数。

[0018] 优选的,步骤S2中,智联网关向车内的各个ECU所发送的随机数均不相同,即车内的各个ECU的预存随机数均不相同。

[0019] 本发明的优点在于:

[0020] (1)本发明将随机数发生器置于车端,先将随机数发生器产生的随机数作为静态随机数用于车内网ECU的身份认证,然后在认证过程中再将随机数发生器产生的随机数作为密钥,对身份认证信息的信息进行对称加密,本发明解决了目前车内网中缺少ECU身份认证的问题,弥补了车内网明文通信所造成的缺陷。

[0021] (2)本发明中既有用于信息加密的动态随机数,也有用于提高MAC信息安全性的静态随机数,通过在安全环境中为各ECU添加静态随机数,保证了"MAC|预存随机数"不可被复制,并且智能网关使用量子随机数发生器所提供的动态随机数作为对称密钥对身份认证消息进行加密,动态随机数用后即销毁,保证了车内网信息通讯的安全性,为CAN网络通讯提供一种身份认证与加密的方案。

[0022] (3)现有技术中随机数的获取均为使用算法生成的伪随机数,伪随机数是根据特定的复杂算法产生的,从本质上讲仍然具有周期性。因此,只要黑客获得了伪随机数算法,并且得到用于伪随机数算法中的参数,就可能提前获得这个伪随机数。然而本发明将量子随机数发生器置于车端,量子随机数发生器通过物理方式产生真随机数,该真随机数是无法提前获知的。

[0023] (4)由于对称加密后的密文与明文长度相等,且加密速度快,能够满足车内网中身份认证及时的要求。

附图说明

[0024] 图1为本发明的一种基于量子随机数发生器的车内网身份认证方法流程图。

[0025] 图2为智能网关对ECU进行身份认证的过程示意图。

[0026] 图3为量子随机数发生器产生随机数的过程示意图。

[0027] 图4为车内网即CAN网络模型示意图。

具体实施方式

[0028] 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,所描述的实施例仅仅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。

[0029] 由图1所示,一种基于量子随机数发生器的车内网身份认证方法,包括以下步骤:

[0030] S1,在车辆上设置量子随机数发生器,量子随机数发生器用于产生真随机数,并将

所产生的真随机数存储于车辆上智联网关的寄存器中；

[0031] 量子随机数发生器为现有技术，由图3所示，量子随机数发生器产生随机数的过程包括随机源选择、数字化采样、数据后处理、随机性检验四个步骤。基于不同的随机源，需采取不同的随机数产生方案，本实施例选择一个物理系统作为随机源，经过测量装置后得到测量结果；该测量结果经过数字化采样转换成二进制随机比特串，作为原始随机数；由于原始随机序列中可能含有一些经典噪声，其统计分布仍然存在一些偏差，因此原始随机序列还需要经过随机性后处理即数据后处理，进一步转为一个更小的、更理想的无偏差随机序列；最后为了检验所生成随机数的质量，通常采用标准的随机性检测软件包对生成随机数进行随机性检验。

[0032] S2，在车辆组装完成后出厂时，智联网关将所存储的随机数分别发送给车内的各个ECU即电子控制单元；所述ECU接收随机数，并将所接收的随机数作为预存随机数进行存储。

[0033] 车辆在完成组装后，智能网关将所存储的随机数分发给各个ECU，为后续的身份认证提高保障。因为车载ECU数量有限，只要二进制随机数的位数够多，就能够保证每一个ECU所赋予的预存随机数不同，且每个ECU的预存随机数不会被更改替换，相对于是一个静态随机数。

[0034] S3，将车辆的启动与熄火视为一个周期，每一个周期内都需要重新认证。因此，车辆每启动时，智能网关对车内的ECU进行初始化身份认证，量子随机数发生器为智能网关对ECU的身份认证提供支持。结合图2，认证过程具体为：

[0035] S31，ECU向智能网关发送身份认证请求；

[0036] S32，智能网关收到身份认证请求后，授予ECU读取寄存器中新随机数的权限；

[0037] S33，ECU获得权限后，读取寄存器中的新随机数；

[0038] 所述寄存器为智能网关的寄存器，所述寄存器中的新随机数为量子随机数发生器所产生的新的真随机数；

[0039] S34，ECU将所读取的新随机数作为密钥对身份认证信息进行加密，并将加密后的密文发送给智能网关；所述身份认证信息中包含ECU的MAC信息以及预存随机数；

[0040] S35，智能网关接收密文后，使用该新随机数作为对称密钥对密文进行解密，得到解密后的身份认证信息；解密完成后，智能网关对该新随机数进行销毁，该新随机数即相当于一个动态随机数，用后即销毁；

[0041] S36，智能网关对解密后的身份认证信息中的预存随机数进行校验，对比解密后的身份认证信息中的预存随机数与步骤S2中智联网关发送给ECU的预存随机数是否相同，以判断该ECU身份是否合法，若相同，则表示该ECU身份合法，否则表示该ECU身份不合法。

[0042] 本发明将量子随机数发生器置于车端，先将量子随机数发生器产生的真随机数作为静态随机数用于车内网ECU的身份认证，然后在认证过程中再将量子随机数发生器产生的真随机数作为密钥，对身份认证信息的信息进行对称加密，由于对称加密后的密文与明文长度相等，且加密速度快，能够满足车内网中身份认证及时的要求。同时解决了目前车内外缺少身份验证方式，明文通信的缺陷。

[0043] 本发明中既有用于信息加密的动态随机数，也有用于提高MAC信息安全性的静态随机数，通过在安全环境中为各ECU添加静态随机数，保证了“MAC|预存随机数”不可被复

制,并且智能网关使用量子随机数发生器所提供的动态随机数作为对称密钥对身份认证消息进行加密,为CAN网络通讯提供一种ECU初始化的身份认证方案。

[0044] 由图4所示,一般燃油车的CAN网络可以分成如下5条CAN总线:

[0045] 1、动力总成CAN总线即PT CAN总线(PowerTrain CAN)

[0046] PT CAN总线上一般有以下ECU:

[0047] 发动机控制模块ECM(Engine Control Module);

[0048] 电子安全气囊SRS(SupplementalRestraintSystem);

[0049] 电池管理系统BMS(Battery Management System);

[0050] 电子驻车系统EPB(Electronic Park Brake)。

[0051] 2、底盘控制CAN总线即CH CAN总线(Chassis CAN)

[0052] CH CAN总线上一般有以下ECU:

[0053] 防抱死制动系统ABS(Antilock Brake System);

[0054] 车身电子稳定系统ESP(Electronic Stability Program) ;

[0055] 电子转向助力EPS(Electric Power Steering)。

[0056] CH CAN总线还负责车辆底盘及各个车轮的制动/稳定/转向;

[0057] 3、车身控制总线即body CAN总线

[0058] Body CAN总线负责车身上的用于提高舒适性/安全性的智能硬件的管理与控制,由于用于提高舒适性/安全性的智能硬件为辅助设备,因此Body CAN总线的网络信号优先级较低。

[0059] 4、娱乐系统总线即info CAN总线(Infomercial CAN)

[0060] Info CAN总线负责车身上的用于提高娱乐性的智能硬件的管理与控制,由于用于提高娱乐性的智能硬件为辅助设备,因此Info CAN总线的网络信号优先级较低。

[0061] 5、诊断控制总线即diag CAN总线(Diagnose CAN)

[0062] Diag CAN总线主要提供远程诊断功能,只有一个ECU。

[0063] 本实施例中,以如下场景对本发明方法的有效性进行分析验证:

[0064] 黑客在CAN网络中新加入了一个伪ECU。

[0065] 由于每一次车辆启动时,智能网关都会对车内的各个ECU进行身份认证,由于这个新的ECU是伪造的,因此这个伪ECU内部的预存随机数也是伪造的,伪ECU申请进行身份认证时,被授予读取新随机数的权限,并将新随机数作为对称密钥,伪ECU对自己的MAC信息与伪预存随机数进行加密,智能网关收到密文后进行解密,对解密后的伪预存随机数进行检测对比,发现伪ECU的伪预存随机数在智能网关中无法查询,因此判断此伪ECU为伪造身份。

[0066] 另外,现有技术中随机数的获取均为使用算法生成的伪随机数。伪随机数是根据特定的复杂算法产生的,从本质上讲仍然具有周期性。如c++语言中的rand函数,其本质就是线性同余法,其基本思想是通过对前一个数进行线性运算并取模从而得到下一个数,通过合理设置参数,就可以实现最大循环周期,且在一个循环计算中所产生的随机数序列近似是随机的。随机数序列是对一个均匀分布随机变量的一组抽样,其结果应是不可预测的,序列中的每个数都是独立的,且服从均匀分布。

[0067] 现有技术所得到的伪随机数是通过算法得到的,因此,只要黑客获得了随机数算法,并且得到用于随机数算法中的形参,就可能提前获得这个随机数。然而,本发明将量子

随机数发生器置于车端，量子随机数发生器通过物理方式产生真随机数，该真随机数是无法提前获知的。

[0068] 以上仅为本发明创造的较佳实施例而已，并不用以限制本发明创造，凡在本发明创造的精神和原则之内所作的任何修改、等同替换和改进等，均应包含在本发明创造的保护范围之内。

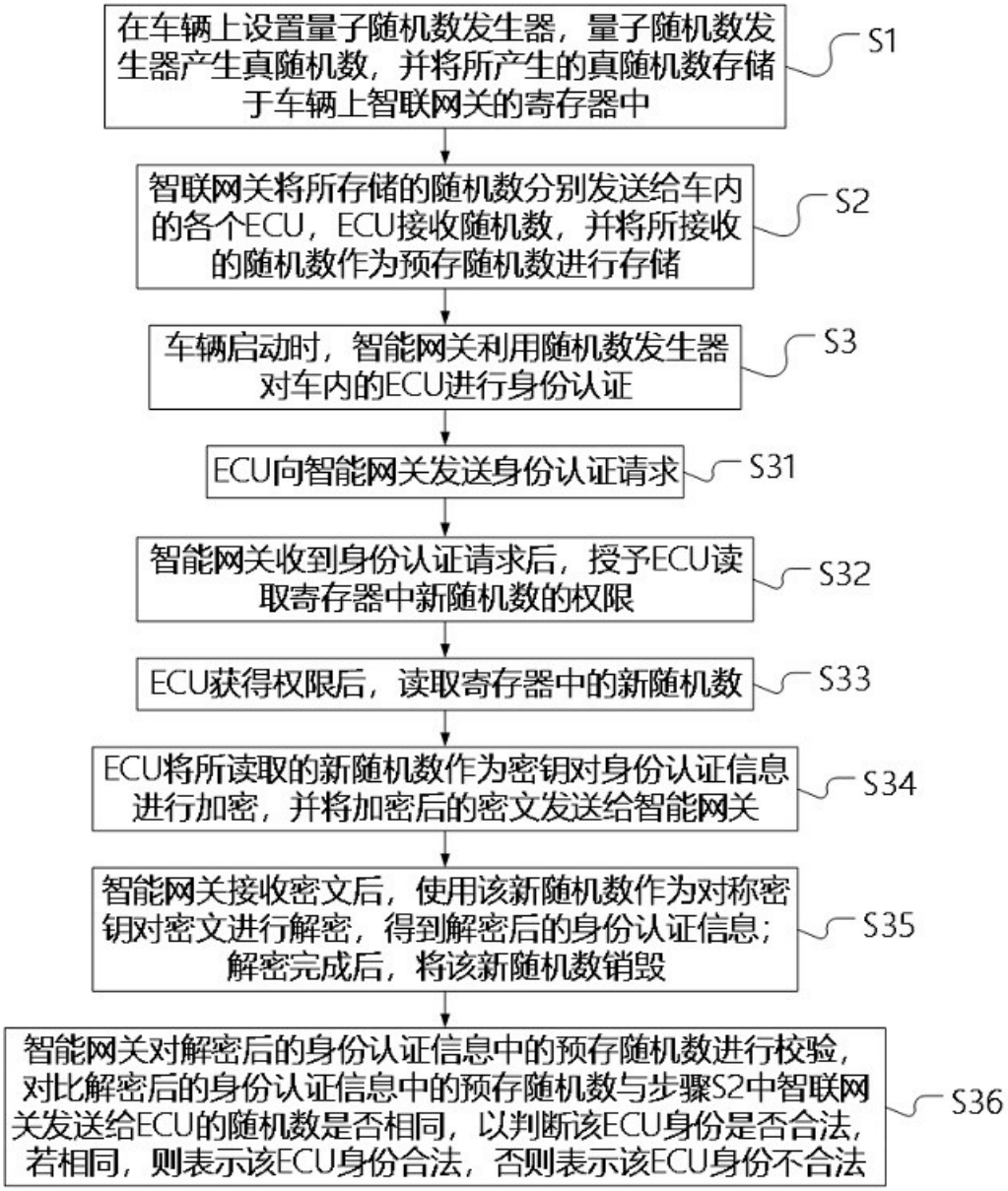

在车辆上设置量子随机数发生器，量子随机数发生器产生真随机数，并将所产生的真随机数存储于车辆上智联网关的寄存器中
S1
智联网关将所存储的随机数分别发送给车内的各个ECU，ECU接收随机数，并将所接收的随机数作为预存随机数进行存储
S2
车辆启动时，智能网关利用随机数发生器对车内的ECU进行身份认证
S3
ECU向智能网关发送身份认证请求
S31
智能网关收到身份认证请求后，授予ECU读取寄存器中新随机数的权限
S32
ECU获得权限后，读取寄存器中的新随机数
S33
ECU将所读取的新随机数作为密钥对身份认证信息进行加密，并将加密后的密文发送给智能网关
S34
智能网关接收密文后，使用该新随机数作为对称密钥对密文进行解密，得到解密后的身份认证信息；解密完成后，将该新随机数销毁
S35
智能网关对解密后的身份认证信息中的预存随机数进行校验，对比解密后的身份认证信息中的预存随机数与步骤S2中智联网关发送给ECU的随机数是否相同，以判断该ECU身份是否合法，若相同，则表示该ECU身份合法，否则表示该ECU身份不合法
S36

图1

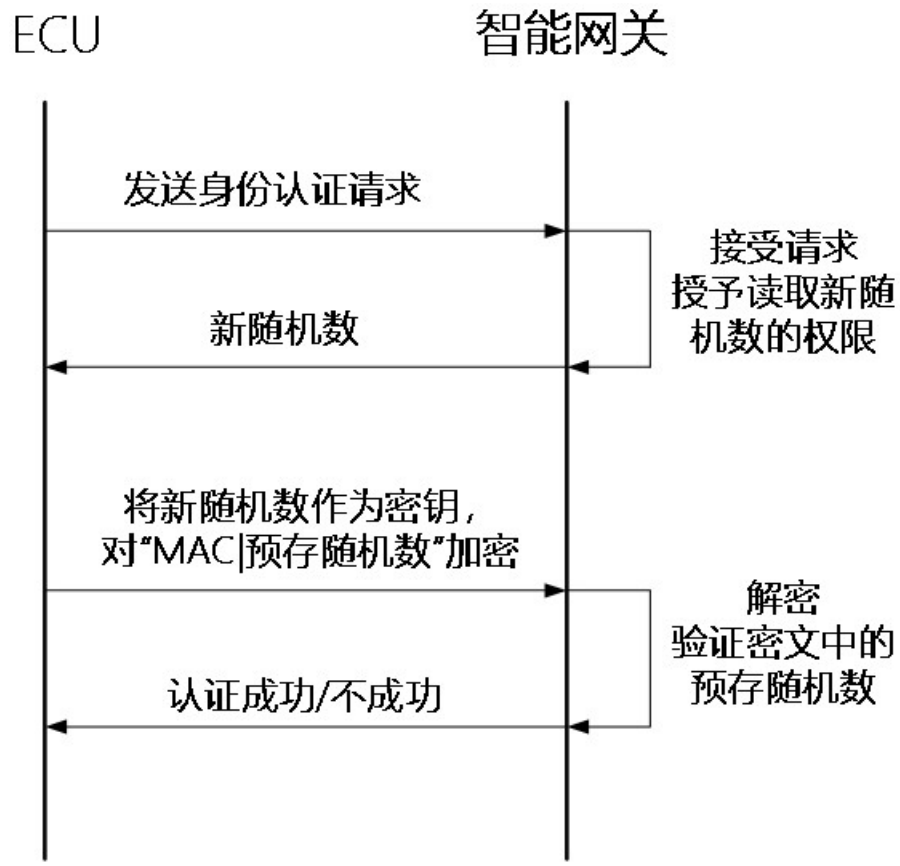

ECU
智能网关
发送身份认证请求
接受请求
授予读取新随机数的权限
新随机数
将新随机数作为密钥，对"MAC|预存随机数"加密
解密
验证密文中的预存随机数
认证成功/不成功

图2

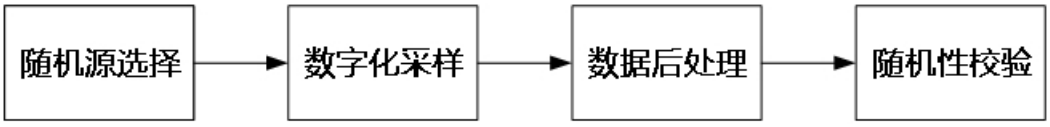

随机源选择
数字化采样
数据后处理
随机性校验

图3

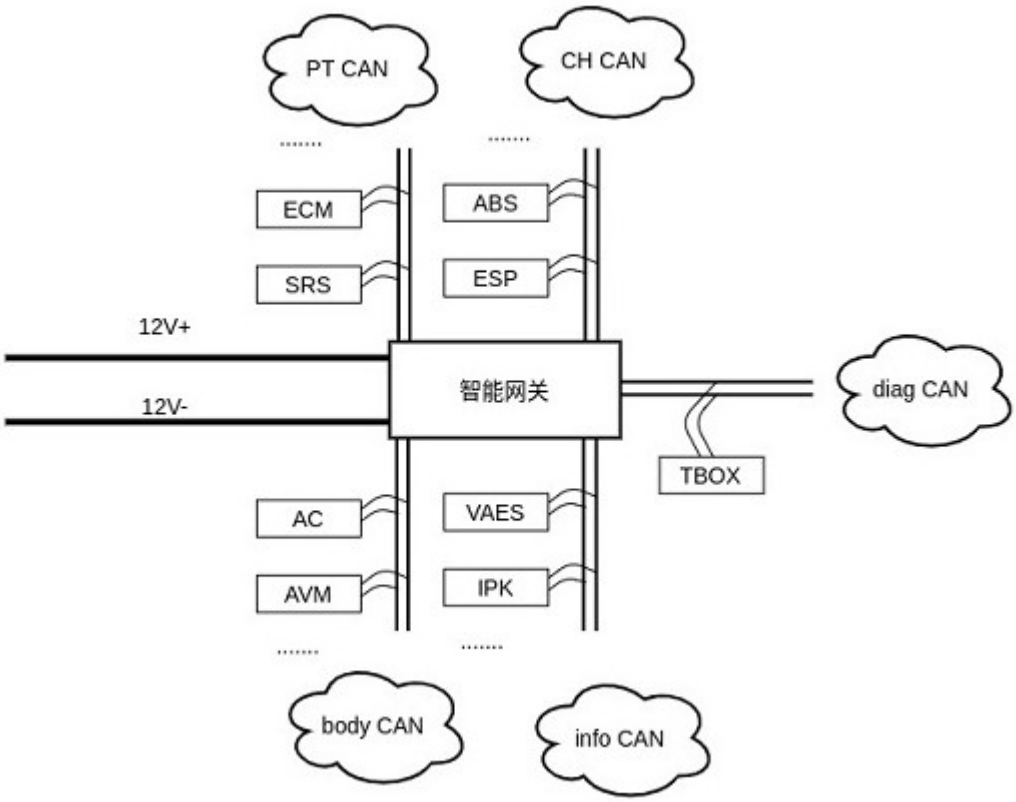

PT CAN
CH CAN
ECM
ABS
SRS
ESP
12V+
12V-
智能网关
diag CAN
TBOX
AC
VAES
AVM
IPK
body CAN
info CAN

图4