DOI：10.7652/xjtuxb201706016

车载控制器局域网络总线的动态口令身份认证方法

吴尚则[1]，秦贵和[2,3]，刘毅[3]，郭森[3]，戚琦[1]，刘恬佳[1]
(1.吉林大学软件学院，130012，长春；2.吉林大学符号计算与知识工程教育部重点实验室，130012，长春；
3.吉林大学计算机科学与技术学院，130012，长春)

摘要：针对车载控制器局域网络(CAN)总线存在缺陷、严重威胁车载信息安全的问题，提出了一种基于挑战/应答模式的车载CAN总线动态口令身份认证方法。该方法考虑到CAN总线是使用极为广泛的标准车载总线及广播形式发送消息的特点，通过利用身份认证技术来确认消息的身份，保证了总线上消息传输的可信任性；根据对身份认证实现模式的研究，采用基于挑战/应答模式的动态认证方法，由于每次认证的挑战值都是随机的，因此每次生成的口令都是不同的；在每次通信时，所使用的认证码都是根据口令生成的，并通过哈希函数生成下次使用的口令。实验结果表明，与传统的CAN总线的方法相比，使用该方法后可以在保证CAN总线真实性的同时，保证传输消息的完整性，从而大幅度提高了车载信息安全级别。

关键词：车载信息安全；车载控制器局域网络总线；身份认证
中图分类号：TP399 **文献标志码**：A **文章编号**：0253-987X(2017)06-0097-06

A Method for Identifying Authentication of Dynamic Passwords for In-Vehicle Controller Area Network Buses

WU Shangze[1], QIN Guihe[2,3], LIU Yi[3], GUO Sen[3], QI Qi[1], LIU Tianjia[1]
(1. College of Software, Jilin University, Changchun 130012, China; 2. Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun 130012, China; 3. College of Computer Science and Technology, Jilin University, Changchun 130012, China)

Abstract: A method for identifying authentication of dynamic passwords for in-vehicle controller area network (CAN) buses is proposed based on the challenge/response mode to deal with the problem that in-vehicle CAN buses are defective, which poses a serious threat to the in-vehicle information security. The method makes use of the peculiarity that the in-vehicle CAN buses are the widely used standard vehicle bus and broadcast messages, and uses the identity authentication technique to confirm the identity of a message, thus ensures the trustworthiness of the message transmission. According to the research on the implementation patterns of identity authentication, the dynamic authentication method is employed. Since the challenge value of every authentication is random, each generated password is different. The authentication code used in each communication is generated based on a password, and the hash function is used to generate a new password for next use. Experiments and a comparison with the traditional CAN show that the proposed method ensures both the integrity of the messages and the authenticity of

收稿日期：2016-12-15。 作者简介：吴尚则(1992—)，男，硕士生；秦贵和(通信作者)，男，教授，博士生导师。 基金项目：国家自然科学基金青年科学基金资助项目(61300145)；吉林省重点科技攻关资助项目(20150204034GX)。
网络出版时间：2017-03-28 网络出版地址：http://www.cnki.net/kcms/detail/61.1069.T.20170328.1133.008.html

the CAN bus. Hence, the degree of security of vehicle information is substantially raised through using the proposed method.

Keywords: in-vehicle information security; controller area network bus; identity authentication

现代汽车不仅仅是在车内可以进行信息交互，还可以通过网络和应用功能接口与外界进行联系，但是这些给人们带来方便快捷的应用功能成为了恶意攻击的重点。2014 年的黑帽大会公布出 20 余款车型存在安全隐患[1]，车载信息安全问题成为了公众关注的焦点。但是，目前并没有一个真正意义上的安全保护措施或方案能成功抵御威胁车载信息安全的各种各样的恶意攻击，研究工作都是基于某些具体的问题开展实施的。文献[2]提出并设计了一种用户移动设备、网关、车内电子控制单元(ECU)的 3 步认证机制，实现对目标设备的验证。文献[3]针对车辆被动无钥匙进入系统中会出现的中继器攻击的特点，提出一种能检测出恶意查询行为的新型距离边界协议。最近几年，各大汽车厂商也把汽车的信息安全问题的研究提到日程上来，国外的很多机构成立了专门的项目组对其进行研究，例如汽车信息安全项目[4]等。汽车信息安全项目的目标是设计出适用于车载网络组件的安全系统架构，其中包括入侵检测模块、访问控制模块、认证和加解密模块等，并根据处理功能的复杂程度，将这些操作通过轻量级、中量级、全量级的 3 种不同级别的硬件部件来实现。

车载信息安全不仅仅包含抵御外部恶意攻击，对车载总线网络进行安全防护也是尤为重要的，尤其是车载控制器局域网络(CAN)总线的安全问题。身份认证技术在保障汽车安全中起到了非常重要的作用，对于身份认证的研究有很多。文献[5]使用非对称密钥和公钥体制，设计了两种基于身份签名的认证方案，实现路边单元与车辆之间的身份认证；文献[6]对多服务器认证方案进行了改进，提出了一种更为安全的、动态的基于身份的认证方案。本文根据 CAN 总线协议特点和对嵌入式系统的网络安全接入问题的研究[7]，设计了一种适合车载 CAN 总线的身份认证方法来提供对车载信息安全的保护。

1 CAN 总线分析与设计思想

1.1 CAN 总线特点和安全性分析

CAN 总线因其信息共享、可靠性高等优点，成为一种应用极为广泛的车载总线。CAN 是一种基于帧标识(ID)的多主广播总线系统。在 CAN 总线协议中，每个 ECU 之间信息的传输是靠帧来完成的。每个 ECU 发送的帧中都包含代表自己身份的特定 ID。对于接收方来说，因为是总线结构，所以总线中的每个节点都能接收到数据帧，但在实际情况中，这样接收是没有意义的，需要根据 ID 来设置屏蔽，使节点只接收固定的帧[8]。

由于 CAN 总线上的消息可以被任意节点读取，没有任何安全措施来提供必要的安全保护，因此无法保证信息的真实性与完整性[9]。黑客攻击的途径也有很多[10]，例如间接通过 WIFI 接口、蓝牙接口等方式入侵到总线上，甚至有通过 OBD-II 或者其他工具直接连接到车内总线，进行非法操作。但是，无论是直接攻击还是通过无线接口进行攻击，最终都是通过强行进入总线网络，控制节点发送恶意的帧。

1.2 设计思想

正是因为 CAN 总线自身存在的缺陷，通过上述的那些攻击手段，使任何节点都可以伪造其他节点向总线上关键节点发送消息，无法保证节点的真实性与消息完整性，这是车载信息安全中尤为重要并亟待解决的问题。因此，为了防止因伪造正常节点身份而导致安全隐患的发生，本文提出了一种身份认证的方法来保障 CAN 总线的信息安全。

2 身份认证的基本方法和原理

身份认证技术是为了确认操作者的身份，防止攻击者假冒合法用户的身份恶意访问有用资源。身份认证一般通过 3 种方法来实现：①根据所知道的信息；②根据所得到的信息；③根据自身特有的信息来证明身份。根据认证模式，身份认证可分为静态认证和动态认证。

静态认证就是通过输入账号密码来实现，其过程非常简单，但也因此容易受到重放攻击。如果在总线传输过程中密码被截获，攻击者重复发送该密码，则会成功入侵总线网络，这就造成了不可估量的严重后果。

动态认证相比于静态认证，有着其特有的优势，每一次使用的密码都不同，安全性也提高了很多。动态口令认证主要分为基于时间同步与挑战/应答模式两种方法。

CAN 总线是基于事件触发的，根据帧的位跳变

来进行同步，没有精确的时间参数[11]。在基于时间同步的方法中，时间参数作为变量参与整个认证过程，因此基于时间同步的认证方法是不可行的。挑战/应答模式是非同步的认证方法，适合 CAN 总线的自身特点。一般情况，目前的认证多数都采用双因素认证[12]。本文根据对动态口令的研究[13]，提出了一种基于挑战/应答模式的动态口令认证与静态认证方法相结合的身份认证方法。

3　身份认证方法

身份认证方法一共分为两个阶段：初始化认证阶段和通信阶段。初始化认证阶段作用在汽车打火初始化启动时，完成后会生成一个通信阶段用到的初始动态口令，该阶段是本文论述的重点。在提出的方案中，用到了 DES-64 bit 加密算法和 BKDR 哈希函数[14]。DES 是一种对称密码体制，加解密的密钥是相同的。哈希算法是一个单向密码体制，从明文到密文是一个不可逆的过程，没有绝对的解密过程。

3.1　初始化认证阶段

在车辆正常使用前，必须先启动车辆，与此同时完成初始化认证阶段。在汽车使用全过程中，只需初始化一次，直到下次使用启动时再进行初始化。假设在车辆出厂时就已经将共享的对称密钥和哈希函数的种子写入到各个 ECU 中，并在每次初始化结束后更新密钥和种子，以备下次初始化使用。

每个 ECU 节点中都包括以下信息，第 m 个 ECU 节点包括代表自身的认证帧发送 ID（分别为静态认证帧 S_m 和动态认证帧 D_m）、静态认证密码 P_m 和 ECU 节点号 N_m。车内的每个 ECU 在生产时都会为其设定一个映射表，该表反映出可收到的帧 ID 与其源 ECU 节点的相关信息。

对于一个节点，若收到某个节点发来的静态认证帧 ID 和动态认证帧 ID，则可根据该表判断出源发送 ECU 节点号和其静态认证密码，这是本文提出的身份认证方法的前提。该阶段共分为 4 步，假设第 m 个 ECU 节点作为源发送方，E 为加密函数，D 为解密函数，H 为哈希函数。

步骤 1　发送方对本节点拥有的静态认证密码 P_m 进行加密生成密文 C_P，发送给接收方。该步骤起到了输入登录密码的作用，等待接收方确认，该过程属于静态认证。接下来的步骤 2 至步骤 4 属于动态认证。C_P 表达式为

$$C_P = E(P_m) \tag{1}$$

步骤 2　接收方收到密文 C_P 后，对其进行解密得出解密后的明文 M_R 为发送方的静态认证密码，然后检索本节点的映射表，识别出源 ECU 节点号，并判断静态认证密码 P_m 与明文是否相同。若相同，则生成一个随机数 R，对其进行加密生成接收方密文 C_R 作为反馈帧的数据返回给发送方；若不相同，系统发出危险警报，告知系统该节点可能受到攻击，不能确认身份，用公式表示如下

$$M_R = D(C_P) \tag{2}$$

$$C_R = E(R) \tag{3}$$

步骤 3　源发送方收到反馈帧之后，对密文 C_R 进行解密得出发送方明文 M_P 为随机数 R，然后以 R 和 N_m 为输入参数进行加密，得出发送方第 2 次加密后的密文 $C_{P,2}$，得到的结果作为哈希函数的输入，经计算得出第 1 次通信时需要的动态口令 D_1，发送给接收方，用公式表示如下

$$M_P = D(C_R) \tag{4}$$

$$C_{P,2} = E(M_P \mid N_m) \tag{5}$$

$$D_1 = H(C_{P,2}) \tag{6}$$

步骤 4　接收方在步骤 2 中发出反馈帧后，开始计算动态口令。将生成的随机数 R 和源发送节点 N_m 第 2 次加密生成密文 $C_{R,2}$，作为哈希函数的输入，计算得出第一次通信动态口令 D_1。与步骤 3 源发送方发来的动态口令进行比较，若一致，返回确认帧，认为发送方为可信任的用户，发送方收到确认帧后，可以进行下一步的通信；若不一致或在一定的时间内收不到口令，则发出警报，告知系统该节点可能受到攻击，不能确认身份，表达式为

$$C_{R,2} = E(R \mid N_m) \tag{7}$$

$$D_1 = H(C_{R,2}) \tag{8}$$

至此，初始化认证阶段结束，每个相关联的 ECU 间都生成了第 1 次通信时需要的初始动态口令。

3.2　通信阶段

在初始化认证阶段完成后，就进入了通信阶段。每次的通信都是基于动态口令完成的，并且会生成下一次通信需要使用的动态口令，M_i 为第 i 次通信的数据，D_i 为第 i 次通信动态口令，D_{i+1} 为第 $i+1$ 次通信动态口令，Q_i 为第 i 次生成的消息认证码。

发送方将第 i 次通信数据与通信动态口令相异或得到新的发送数据 M_d，并通过哈希函数计算出本次通信所需要的消息认证码（MAC）[15] Q_i，再对 D_i 进行哈希函数计算得出第 $i+1$ 次通信时需要的动态口令 D_{i+1}

$$M_d = M_i \wedge D_i \tag{9}$$

$$Q_i = H(M_i \mid D_i) \tag{10}$$

$$D_{i+1} = H(D_i) \tag{11}$$

在数据发送过程中，若将生成的认证码单独作为一个帧发送，则势必会增大总线的负载，增加了整车通信的负担。CAN 帧的数据域最多是 8 个字节，但在实际的情况中，使用时都少于 8 个字节，这样就可以把本次通信的认证码放在数据后，组成一个帧发送，避免增加总线的负载。在实验中，使用前 7 个字节长度用来装载数据，剩余 1 个字节长度来装载认证码。

在第 i 次通信中，接收方先用收到的数据 M_d 和本次通信动态口令 D_i 解出原始数据 M_i，再用数据 M_i 和本次通信动态口令 D_i 进行哈希函数计算，得到本次通信消息认证码 Q_i。对本次通信动态口令 D_i 进行哈希计算，得出下次通信用到的动态口令 D_{i+1}。由于在本次通信过程中，收发双方都知道本次通信的动态口令，因此接收方可以计算出消息认证码，与收到的消息认证码比较是否相同。若相同，则使用数据，并生成下次通信需要用到的动态口令；反之，则发出危险警报，用公式表示如下

$$M_i = M_d \wedge D_i \tag{12}$$

$$Q_i = H(M_i \mid D_i) \tag{13}$$

$$D_{i+1} = H(D_i) \tag{14}$$

4 实验结果与性能分析

为了验证本文提出的身份认证方法，实验选取 4 个飞思卡尔 CAN 开发板，模拟一个简单的车载 CAN 总线系统，节点号分别为 1、2、3、4，并使用 CodeWarrior 集成开发环境编码实现，以保证实验顺利进行。使用 USBCAN-II 来模拟一个攻击节点 S，其配套软件 CANtest，可以在 PC 机上显示监测到的总线上的 CAN 帧。在实验中，对总线真实性与完整性进行了测试，为了实验现象明显，在分析出对方为可疑身份和消息出现异常时，发出警报帧。

4.1 真实性测试分析

(1)S 并不知道节点在认证时的静态密码，所以无法发出静态认证帧，此时攻击无效。静态认证只能够判断出一些低级的攻击者身份。

(2)S 通过窃听总线消息，截获到静态认证帧，S 可以进行篡改或重放攻击。若进行篡改，在总线上一定会出现警报帧，检测出可疑身份。虽然静态认证这一步抵挡住了篡改，但是对重放攻击却没有作用。攻击者利用非法截获到的静态认证帧，在下一次初始化认证阶段重新发送便可以通过静态认证，进入动态认证。

(3)S 伪造 3 号节点身份，同时窃取到了静态认证帧和动态口令。由于静态认证无法抵御重放攻击，S 便可进入动态认证，在动态认证过程中，若篡改该节点的动态口令，则会出现警报帧，检测出可疑身份。表 1 显示若对动态口令进行重放攻击(第 24 号)，第 28 号显示在总线上出现警报帧，表明重放攻击无效。

这是因为虽然静态密码帧抵挡不住重放攻击，但是动态口令根据随机数的不同每次生成的也不同，使用后马上失效，只有一次使用价值，即使截获到上次的动态口令，攻击者在下一次重复发送时，接收方产生的随机数发生变化，本次的动态口令也发生变化，与上次被截获到的不相同，因此可检测出可疑身份。

4.2 完整性测试分析

在通信阶段，S 截获到 3 号节点发出的帧。若随意篡改数据部分，根据对通信流程的分析，通信双方生成的认证码必然不同，则会出现警报帧。

表 1 对动态认证帧重放攻击后总线检测结果

序号	传输方向	帧 ID	帧格式	帧类型	数据长度	数据							
1	接收	0x00000009	数据帧	标准帧	0x08	26	c2	4b	1f	fe	7d	8a	a5
2	接收	0x00000006	数据帧	标准帧	0x08	30	30	30	30	30	30	30	30
3	接收	0x00000004	数据帧	标准帧	0x08	b4	2d	af	32	6d	c3	0c	01
4	接收	0x0000000e	数据帧	标准帧	0x08	31	31	31	31	31	31	31	31
5	接收	0x0000000b	数据帧	标准帧	0x08	46	52	45	45	46	4c	59	00
6	接收	0x00000002	数据帧	标准帧	0x08	1f	34	ad	86	d8	0f	cb	db
7	接收	0x0000000e	数据帧	标准帧	0x08	30	30	30	30	30	30	30	30
8	接收	0x0000000c	数据帧	标准帧	0x08	b4	2d	af	32	6d	c3	0c	01
9	接收	0x00000005	数据帧	标准帧	0x08	a0	c1	86	86	fe	7d	8a	a5
10	接收	0x00000002	数据帧	标准帧	0x08	31	31	31	31	31	31	31	31
11	接收	0x0000000a	数据帧	标准帧	0x08	af	70	2f	78	79	31	9b	70
12	接收	0x0000000e	数据帧	标准帧	0x08	30	30	30	30	30	30	30	30

（续表 1）

序号	传输方向	帧 ID	帧格式	帧类型	数据长度	数据							
13	接收	0x0000000e	数据帧	标准帧	0x08	01	00	00	00	00	00	00	00
14	接收	0x0000000c	数据帧	标准帧	0x08	b4	2d	af	32	6d	c3	0c	01
15	接收	0x0000000a	数据帧	标准帧	0x08	f8	f3	8f	34	95	62	95	e7
16	接收	0x0000000d	数据帧	标准帧	0x08	a4	80	62	cc	fe	7d	8a	a5
17	接收	0x0000000a	数据帧	标准帧	0x08	31	31	31	31	31	31	31	31
18	接收	0x00000006	数据帧	标准帧	0x08	30	30	30	30	30	30	30	30
19	接收	0x00000004	数据帧	标准帧	0x08	b4	2d	af	32	6d	c3	0c	01
20	接收	0x0000000f	数据帧	标准帧	0x08	46	52	45	45	46	4c	59	00
21	接收	0x0000000a	数据帧	标准帧	0x08	30	30	30	30	30	30	30	30
22	接收	0x00000002	数据帧	标准帧	0x08	74	e3	15	6c	ec	a6	01	86
23	接收	0x00000008	数据帧	标准帧	0x08	b4	2d	af	32	6d	c3	0c	01
24	发送	0x00000009	数据帧	标准帧	0x08	26	c2	4b	1f	fe	7d	8a	a5
25	接收	0x0000000e	数据帧	标准帧	0x08	f8	f3	8f	34	95	62	95	e7
26	接收	0x00000005	数据帧	标准帧	0x08	63	83	d2	a5	fe	7d	8a	a5
27	接收	0x00000002	数据帧	标准帧	0x08	31	31	31	31	31	31	31	31
28	接收	0x000000ee	数据帧	标准帧	0x08	31	31	31	31	30	30	30	30
29	接收	0x00000009	数据帧	标准帧	0x08	a5	80	62	cc	fe	7d	8a	a5
30	接收	0x000000ee	数据帧	标准帧	0x08	31	31	31	31	30	30	30	30
31	接收	0x00000007	数据帧	标准帧	0x08	01	00	00	00	00	00	00	00
32	接收	0x00000002	数据帧	标准帧	0x08	30	30	30	30	30	30	30	30
33	接收	0x00000000	数据帧	标准帧	0x08	b4	2d	af	32	6d	c3	0c	01
34	接收	0x00000006	数据帧	标准帧	0x08	18	9e	9f	b0	cb	67	bb	c7

在每次通信的过程中，都会生成下一次使用的动态口令，因此每次通信计算出的认证码都是一次性的，即使对截获到的帧进行重放攻击，但是上一次通信时的认证码已经失效。表 2 中第 19 号表示重放攻击，第 21 号显示在总线上出现警报帧，表明重放攻击无效。

表 2　对数据帧重放攻击后总线检测结果

序号	传输方向	接收时间标识	帧 ID	帧格式	数据长度	数据							
1	接收	0x0438dcf9	0x04000008	数据帧	0x08	67	23	c0	70	8a	15	ff	b3
2	接收	0x0438f11e	0x0400000c	数据帧	0x08	28	c3	86	9c	8a	15	ff	4b
3	接收	0x04390544	0x04000008	数据帧	0x08	51	b6	48	78	8a	15	ff	fd
4	接收	0x04391969	0x0400000c	数据帧	0x08	bd	93	36	5d	8a	15	ff	da
5	接收	0x04392d8e	0x04000008	数据帧	0x08	d3	b0	5f	89	8a	15	ff	fc
6	接收	0x043941b3	0x0400000c	数据帧	0x08	e1	ff	2a	2b	8a	15	ff	52
7	接收	0x04413468	0x04000008	数据帧	0x08	46	4d	31	58	8a	15	ff	b3
8	接收	0x0441488d	0x0400000c	数据帧	0x08	8e	49	43	58	8a	15	ff	b5
9	接收	0x04415cb3	0x04000008	数据帧	0x08	b8	02	5e	0c	8a	15	ff	e3
10	接收	0x044170d8	0x0400000c	数据帧	0x08	d0	53	89	63	8a	15	ff	40
11	接收	0x044184fe	0x04000008	数据帧	0x08	37	2a	c1	d8	8a	15	ff	a3
12	接收	0x04419923	0x0400000c	数据帧	0x08	ce	fd	df	47	8a	15	ff	54
13	接收	0x0441ad48	0x04000008	数据帧	0x08	85	aa	b4	8d	8a	15	ff	08
14	接收	0x0441c16d	0x0400000c	数据帧	0x08	a4	bd	1a	b2	8a	15	ff	d3
15	接收	0x0441d592	0x04000008	数据帧	0x08	d1	98	ce	8d	8a	15	ff	be
16	接收	0x0441e9b8	0x0400000c	数据帧	0x08	18	fe	6d	80	8a	15	ff	05
17	接收	0x0441fddd	0x04000008	数据帧	0x08	31	95	f6	30	8a	15	ff	cf

（续表 2）

序号	传输方向	帧 ID	帧格式	帧类型	数据长度	数据							
18	接收	0x04421203	0x0400000c	数据帧	0x08	de	99	a2	06	8a	15	ff	21
19	发送	无	0x04000008	数据帧	0x08	67	23	c0	70	8a	15	ff	b3
20	接收	0x04422628	0x04000008	数据帧	0x08	bf	07	b7	44	8a	15	ff	19
21	接收	0x0442375c	0x0400000d	数据帧	0x08	31	31	31	31	30	30	30	30

5 结 论

本文针对 CAN 总线缺乏真实性与完整性的安全问题，提出了一种基于挑战/应答模式动静结合的身份认证方法，对车辆启动时和运行时都提供了安全的保护机制。根据实验结果，虽然在初始化认证阶段增加了汽车启动延时，但是在整个车辆使用时只初始化一次，而且保证了总线节点的真实性与通信消息完整性，大幅度提高了车辆的安全级别。

参考文献：

[1] MILLER C, VALASEK C. A survey of remote automo-tive attack surfaces [EB/OL]. (1998-09-10) [2016-11-24]. http://ioactive.com/pdfs/IOActive_Remote_Attack_Surfaces.pdf.

[2] HAN K, POTLURI S D, KANG G S. On authentication in a connected vehicle: Secure integration of mobile devices with vehicular networks [C]// Proceedings of the ACM/IEEE International Conference on Cyber-Physical Systems. Piscataway, NJ, USA: IEEE, 2013: 160-169.

[3] YANG T, KONG L, XIN W, et al. Resisting relay attacks on vehicular passive keyless entry and start systems [C]// Proceedings of the 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery. Piscataway, NJ, USA: IEEE, 2012: 2232-2236.

[4] European Commission Within the Seventh Framework Programme. E-safety vehicle intrusion protected applications (EVITA) project [EB/OL]. (2008-07-31) [2016-11-24]. http// www. evita-project. org.

[5] VIJAYALAKSHMI N, SASIKUMAR R. An ID-based privacy preservation for VANET [C]// Proceedings of the International Conference on Computing and Communications Technologies. Piscataway, NJ, USA: IEEE, 2015: 164-167.

[6] CHANG C C, CHENG T G, HSUEH W H. A robust and efficient dynamic identity-based multi-server authentication scheme using smart cards [J]. International Journal of Communication Systems, 2016, 29 (2): 290-306.

[7] 李飞. 基于 ARM 的嵌入式系统网络接入安全研究 [D]. 武汉：武汉工程大学，2013：25-33.

[8] WOO S, JO H J, LEE D H. A practical wireless attack on the connected car and security protocol for in-vechile CAN [J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 1-14.

[9] HOPPE T, KILTZ S, DITTMANN J. Security threats to automotive CAN networks practical examples and selected short-term countermeasures [M]// Computer Safety, Reliability, and Security. Berlin, Germany: Springer-Verlag, 2008: 235-248.

[10] 于赫. 网联汽车信息安全问题及 CAN 总线异常检测技研究 [D]. 长春：吉林大学，2016：15-31.

[11] 李芳，刘鲁源，吕伟杰. CAN 总线位定时和同步机制的分析 [J]. 电子产品世界，2005(5)：106-107.
LI Fang, LIU Luyuan, LV Weijie. The analysis of bit timing and synchronization mechanism of CAN bus [J]. Electronic Engineering and Product World, 2005 (5): 106-107.

[12] BONNEAU J, HERLEY C, OORSCHOT P C V, et al. The quest to replace passwords: a framework for comparative evaluation of web authentication schemes [C]// Proceedings of the IEEE Symposium on Security and Privacy. Piscataway, NJ, USA: IEEE Computer Society, 2012: 553-567.

[13] HU M, TENG G, WANG C, et al. Research of identity authentication of the mobile terminal voting system [C]// Proceedings of the 9th International Conference on Intelligent Information Hiding and Multimedia Signal Processing. Washington, DC, USA: IEEE Computer Society, 2013: 198-201.

[14] 胡向东. 应用密码学 [M]. 2 版. 北京：电子工业出版社，2011：87-88.

[15] JIANG Shunrong, ZHU Xiaoyan, WANG Liangmin. An efficient anonymous batch authentication scheme based on HMAC for VANETs [J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17 (8): 2193-2204.

（编辑 武红江）