文章编号：0253-374X(2019)03-0386-06 DOI:10.11908/j.issn.0253-374x.2019.03.012

基于CAN-FD总线的车载网络安全通信

罗 峰，胡 强，刘 宇
（同济大学 汽车学院，上海 201804）

摘要：以数据加密和入侵检测为基础，建立了一种基于灵活数据速率控制器局域网络的汽车通信网络信息安全方法.提出了包括安全传输、安全启动、时间同步与密钥分配的汽车网络安全通信协议，并通过建立网络仿真模型验证安全协议的有效性.搭建了基于硬件实例的安全通信节点，测试硬件节点的实际通信性能和加密性能.最后针对汽车通信网络潜在的攻击方式，以Dolev-Yao入侵模型攻击和拒绝服务攻击为测试方法，对安全通信模型进行了安全性攻击测试和入侵检测功能验证，确定了网络入侵检测的判定指标.测试结果验证了该方法的安全性和可用性.

关键词：安全通信；车载网络；信息安全
中图分类号：U463.67 **文献标志码**：A

Secure Communication Method for In-Vehicle Network Based on CAN-FD Bus

LUO Feng, *HU Qiang*, *LIU Yu*
(School of Automotive Studies, Tongji University, Shanghai 201804, China)

Abstract: A security method for vehicle communication network based on controller area network with flexible data-rate (CAN-FD) was established with data encryption and intrusion detection. Secure communication protocols for vehicle network including secure transmission, secure boot, time synchronization, and key distribution were proposed, and a network simulation model was established to verify the validity of the secure protocols. Secure communication nodes based on hardware instance were established to test the actual communication performance and encryption performance of the hardware nodes. Aiming at the potential attack modes of the vehicle communication network, the Dolev-Yao intruder model attack and the denial of service attack were used as the test methods to test the security of communication model and verify the intrusion detection function. And the judgment index of the network intrusion detection was determined. The experimental results had confirmed the security and usability of the method.

Key words: secure communication; vehicle network; cybersecurity

智能网联汽车是当前汽车技术领域的一个重要发展方向.随着汽车网联技术的发展，汽车上对外的接口逐渐增多，针对汽车的网络攻击成为了一个新的问题[1].当前对于汽车网络的安全通信研究中，Herrewege等[2]基于CAN+（controller area network+），将数据场16个字节中的15个字节用于消息验证，通过哈希加密函数计算出数据帧的签名校验，实现通信的安全认证，但由于只有1个字节可以用于数据传输，会造成总线负载率升高.Hartkopp等[3]将CAN总线数据场的4个字节用于对报文和时间戳的认证，但是使CAN通信的有效数据降低，造成网络负载率的上升.Woo等[4]对CAN总线通信进行了无线攻击，并提出一种安全协议对CAN总线通信进行安全保护.针对高速数据的传输，Woo等[5]提出了一种基于CAN-FD（controller area network with flexible data-rate)加密通信的方法，实现了在汽车网络上进行数据的分级加密传输，但缺乏相应的时间检测机制.国内学者在CAN总线通信的身份认证方面提出了一种动态口令身份认证方法[6]，实现通信的完整性检查.在入侵检测方面，国内的研究者提出了一种运用信息熵的算法对通信入侵的异常现象进行检测的方法[7]，但未体现该方法在汽车级微控制器的计算处理能力下的性能效果.

在目前的国内外研究中，对汽车通信网络的保护主要包括对数据的加密以保护通信的机密性、对消息的校验以保证数据的真实性以及通信网络的入

收稿日期：2017-10-27
基金项目：中央高校基本科研业务费专项资金(22120170265)
第一作者：罗 峰(1969—)，男，教授，博士生导师，工学博士，主要研究方向为汽车电子. E-mail: luo_feng@tongji.edu.cn
通信作者：胡 强(1991—)，男，博士生，主要研究方向为汽车电子. E-mail: 404huqiang@tongji.edu.cn

侵检测，但是缺乏在汽车级微控制器的计算处理能力下的实际性能分析和可行性验证. 针对目前的车载网络安全通信问题，通过对车载网络通信的安全需求分析，以数据加密和入侵检测为基础，建立一种基于 CAN-FD 网络的汽车通信网络信息安全方法，并通过硬件实例验证该方法的实时性和负载率是否满足汽车网络要求.

1　安全需求

通过威胁分析可以确定网络通信基本的安全需求. 目前针对汽车网络通信的攻击主要有以下几种形式[8]：

(1) 信息窃取. 攻击者通过网络监听方式，直接获取通信内容，从而获取有关的车辆信息以及进行深入的网络攻击. 应对该攻击的主要方式是对通信的数据内容进行加密，保证信息的机密性.

(2) 重放攻击. 攻击者根据通信报文的特征，记录网络监听到的报文，再将记录的报文数据进行重发. 重放攻击在攻击者不知道报文内容的前提下也能进行. 针对重放攻击的主要应对机制是在通信过程中进行报文的时间标志检查，保证信息的新鲜性.

(3) 中间人攻击. 中间人攻击主要有报文拦截和报文篡改 2 种形式. 攻击者将网络中的通信节点分离，监听和记录网络上的通信内容，并对通信报文进行拦截或者篡改. 对于中间人攻击，需要对通信报文进行完整性检查和真实性校验.

(4) 拒绝服务攻击. 攻击者在网络上发送大量高优先级的报文，使网络的负载率达到最高值，影响网络正常通信. 因此需要采取相应的安全机制保证通信的可用性.

信息的机密性、新鲜性、完整性、真实性以及可用性是汽车网络通信的最基本的安全需求.

2　安全通信

安全通信在基于 CAN-FD 网络传输的基础上，加入了安全通信协议和入侵检测安全机制. CAN-FD 网络具有最高 10 Mbps 的通信速率以及多达 64 字节数据场容量. CAN-FD 网络的报文帧结构形式如图 1 所示[9].

2.1　安全协议

2.1.1　安全传输

汽车网络通信对加密算法的要求如下：

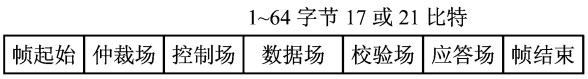

图 1　CAN-FD 帧结构

Fig.1　Frame structure of CAN-FD

(1) 算法应该具备轻量级要求，在汽车 ECU (electronic control unit)有限的硬件资源下，能够在保证网络通信实时性前提下正常执行算法.

(2) 具备足够的防破解能力.

(3) 适合车载网络的数据加密，最小加密块应小于报文数据场的字节数.

AES(advanced encryption standard)加密算法作为一种对称加密算法，具有执行计算时间短，兼容软件加密、硬件加密的方式等特点[10]. 本文中安全传输协议采用 AES-128 算法对传输数据进行加密和 MAC(message authentication code)计算. CAN-FD 总线中，数据场有 64 个字节(512 位)，将前 48 字节数据进行密文传送，后 16 个字节作为 MAC 校验. 16 字节(128 位)的 AES-MAC 理论上的暴力破解次数为 2^{128}，具有足够的安全性.

2.1.2　安全启动

在车辆启动时，密钥管理员需要对 ECU 进行轮询，确保所有子网内的 ECU 掌握正确的预共享密钥，图 2 所示是密钥管理员对 ECU1 进行安全启动询问过程. 首先密钥管理员生成随机数，将随机数和一个计数器值以明文形式发送给 ECU1，并生成 MAC 校验码，其中计数器值用来防止重放攻击. ECU1 收到请求后验证 MAC 和计数器值，将随机数通过预共享密钥进行加密和认证，发回给密钥管理员，密钥管理员对 ECU1 的应答进行解密. 当接收随机数和发送随机数一致且 MAC 有效时，说明 ECU1 能够正确使用预共享密钥，安全启动完成.

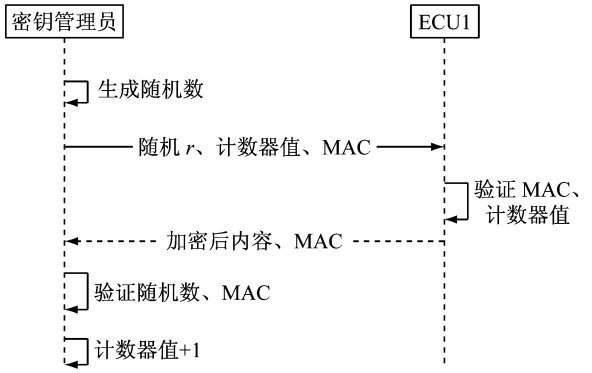

图 2　安全启动流程

Fig.2　Flow chart of secure bootstrapping

2.1.3 时间同步

高精度的时间戳是防止重放攻击的一种手段. 时钟同步是依靠某一个 ECU 作为“时钟基准”,其他 ECU 通过接收该 ECU 的时间戳信息,更新本地 ECU 时间戳参数. 由于在网络上传输数据、接收和发送数据、加密解密以及 MAC 校验都会产生延时,因此需要对传输产生的延时进行校正. 时间同步协议参考 IEEE 1588 协议[11],通过计算时间延时和偏移,得出报文发送时间和接收时间的偏差. 需要同步时间的 ECU 根据计算得出的时间偏差,修正接收的时间戳参数. 在同步的过程中的通信报文需要加入随机数校验和 MAC 校验机制,确保时间同步的安全性. 图 3 中延时 T_{delay} 和偏移 T_{offset} 的计算公式如下:

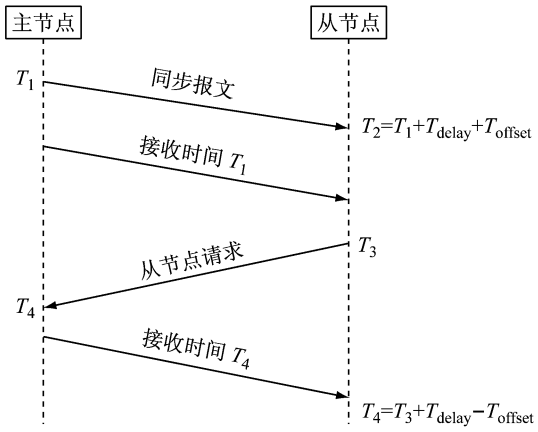

图 3 IEEE 1588 时钟同步机制

Fig.3 Time synchronization in IEEE 1588

$$T_{\text{daley}}=\frac{T_2-T_1-T_3+T_4}{2} \tag{1}$$

$$T_{\text{offset}}=\frac{T_2-T_1+T_3-T_4}{2} \tag{2}$$

式中:T_1 为主节点发送时间;T_2 为从节点接收时间;T_3 为从节点发送时间;T_4 为主节点接收时间.

2.1.4 密钥分配

安全通信中用于密钥分配、时钟同步和安全启动的密钥为预共享密钥,安全传输中使用的密钥为会话密钥. 假设会话密钥在车辆每次启动时会进行一次更新. 一个 ECU 节点可以具备多组会话密钥,用于不同类型的安全通信. 图 4 中,每个 ECU 的预共享密钥依次为 K_1,K_2,…,K_5. 其中 ECU1、ECU3、ECU4 具有会话密钥 1,ECU2 和 ECU5 具有会话密钥 2,从而实现同一子网内通信内容的逻辑隔离,保护会话内容的隐私性. 在实际使用中,每个 ECU 的安全模块中可以储存多个密钥,用于不同场合下的加密认证.

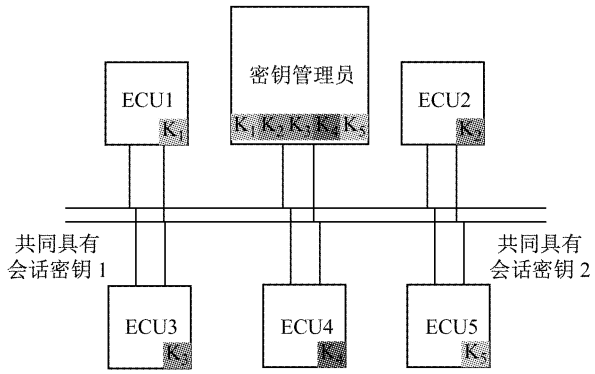

图 4 会话密钥分组

Fig.4 Session key grouping

密钥分配有以下 2 个场景:①ECU 通过预共享密钥向密钥管理员发送更新请求;②密钥管理员通过预共享密钥向 ECU 发送密钥更新请求.

密钥分配会话采用随机数验证机制,其中随机数由密钥管理员和会话 ECU 生成. 同时在通信过程中加入时间戳和 MAC 校验以及通信加密机制,保证密钥更新安全进行.

2.2 入侵检测

安全通信过程中引入入侵检测机制. 在通信过程中,ECU 需要实时检测通信的安全状态. 安全通信的状态码定义如表 1 所示.

表 1 安全通信状态码定义

Tab.1 Definition of secure communication status code

错误码	错误说明
0	状态正常
1	MAC 认证错误
2	Counter 错误
3	随机数不符
4	ECU 离线
5	加密密钥载入错误
6	校验密钥载入错误
7	等待超时
8	时间戳错误
9	网络高负载

3 安全通信系统验证

3.1 系统仿真

安全通信系统通过 CANoe 软件进行仿真验证,搭建网络仿真模型. 设置 CAN-FD 通信速率为 2 Mbps,时间戳允许误差为 100 ms. 仿真过程为密钥管理员和 5 个 ECU 节点之间实现安全启动、时间同步、密钥分配以及安全传输协议. 利用 CANoe 设计仿真控制面板,如图 5 所示. 仿真程序中安全协议执行的流程如图 6 所示.

图 5　安全协议仿真面板

Fig.5　Panel of secure protocols

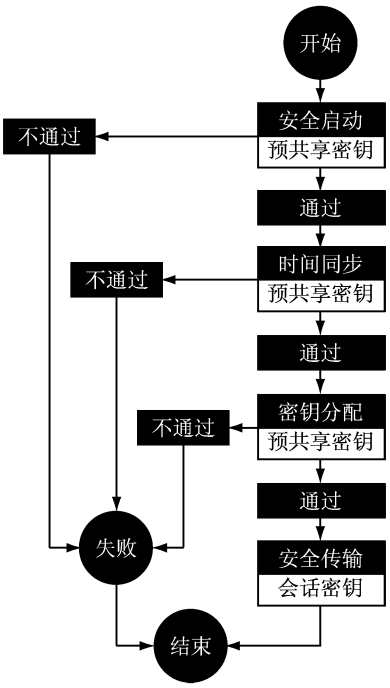

图 6　安全通信流程

Fig.6　Process of secure communication

仿真实验中 CAN-FD 的通信速率为 2 Mbps，连续实现安全启动、时间同步、密钥分配协议用时约为 20.8 ms. 如图 7 所示，在仅执行安全协议过程中，CAN Statistics 数据栏的统计结果显示网络仿真通信最大负载率为 3.10%，平均负载率为 1.41%. 因此采取该安全通信机制不会对总线负载率造成太大压力. 在安全会话过程中，CAN-FD 报文的数据场中前 48 个字节用于数据传输，后 16 个字节用于数据校验，数据场的传输利用率为 75%，通信效率较高.

安全传输的数据由 AES-128 算法进行加密和解密. 表 2 中列出了在安全传输过程中，ECU1 和 ECU3 之间的通信数据. 其中 ECU1 在 CAN-FD 报文数据场前 48 个字节中传输数据，后 16 个字节发送报文仲裁场、时间戳等校验信息，经加密密钥和校验密钥分别生成密文和 MAC，发送给 ECU3. ECU3 校验 MAC 后解密报文数据. 可以看出 ECU3 解密的数据和 ECU1 发送数据完全吻合.

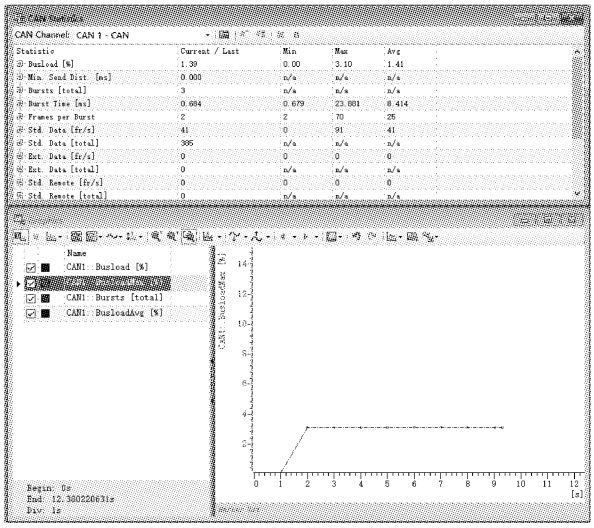

图 7　安全协议执行时的网络负载率界面

Fig.7　Bus load rate of executing secure protocols

表 2　CAN-FD 数据场分析

Tab.2　Analysis of the CAN-FD data field

节点	传输数据															
ECU1 发送原始信息	01	70	D6	FE	50	5C	94	3C	26	43	02	CC	15	D9	33	93
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	DC	75	5A	78	7A	D0	73	80	6D	0D	49	7F	84	1E	94	01
ECU1 发送密文	7B	68	D9	25	6E	7B	AC	92	F1	26	3A	35	E1	D8	05	2B
	0B	D8	3B	52	26	BA	E3	FA	97	9B	A8	B3	8E	A0	34	B8
	EC	7B	0C	A8	7C	8C	39	92	8F	23	0B	69	0C	05	F8	CC
	28	F5	30	2D	AE	5B	68	C4	21	00	63	7E	08	50	58	D6
ECU3 解密明文	01	70	D6	FE	50	5C	94	3C	26	43	02	CC	15	D9	33	93
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
	DC	75	5A	78	7A	D0	73	80	6D	0D	49	7F	84	1E	94	01

3.2 硬件实现

安全通信在微控制器 MPC5748G 上进行验证，如图 8 所示. MPC5748G 具有硬件安全模块，能够从硬件层面上实现 AES-128 算法和 MAC 认证，并具有随机数生成和密钥安全存储等功能[12].

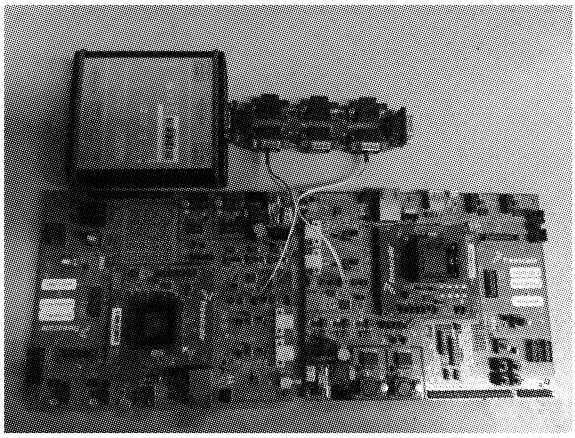

图 8 安全通信硬件节点

Fig.8 Secure communication on hardware

加密和解密的计算时间测试结果如图 9 所示. 当微控制器的时钟频率为 160 MHz，使用 AES-128 算法连续加密或解密 1 600 字节所消耗的时间约为 71.6 μs，平均每帧报文中由于加密和解密造成的额外延时为 5.73 μs. 该延时远小于 CAN-FD 报文的传输周期时间. 因此，引入该安全通信机制并不会影响网络通信的实时性.

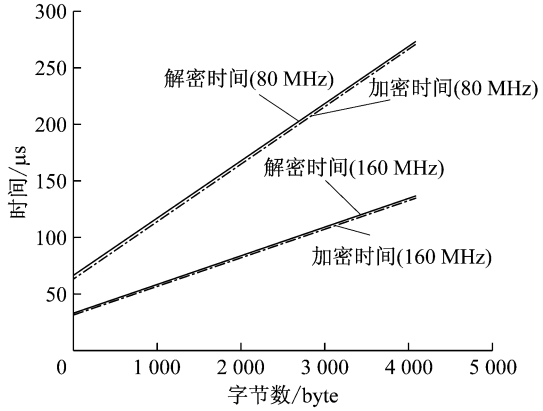

图 9 加密、解密计算性能

Fig.9 Calculation performance of encryption and decryption

4 安全测试和结果分析

使用 Dolev-Yao 模型进行安全通信攻击测试[13]. 在图 4 的 CAN-FD 网络安全通信基础上加入一个攻击者节点. 攻击者可以监听网络信息，改变网络拓扑结构，发起重放报文、篡改报文和拦截报文等攻击.

基本测试场景中使用 CANoe 作为网络仿真工具，建立的 CAN-FD 总线的通信速率为 500 kbps，并使用外接的 PCAN 工具仿真和记录工具进行拒绝服务攻击. 测试用例包括密钥破解、重放攻击、中间人攻击和拒绝服务攻击.

(1) 密钥破解. 设置攻击者节点为监听模式，攻击者监听总线，并对监听的报文信息进行记录. 通过主节点的请求报文和从节点的应答报文推测密钥，然后使用虚假 ECU 替换原从节点. 由于 AES-128 算法只能通过暴力破解，可以认为攻击者无法找出正确的密钥，网络监测状态为 MAC 认证错误.

(2) 重放攻击. 设置攻击者节点为发送模式，在报文监听的基础上，攻击者根据标识位等特征记录网络上报文信息，然后向网络上重新发送该报文. 由于报文中时间戳超过允许误差值，网络监测状态为时间戳错误.

(3) 中间人攻击. 攻击者将原网络分割开来，进行拦截、篡改报文攻击. 被拦截攻击后，网络监测状态为等待超时. 篡改报文攻击包括篡改 MAC 值、篡改报文标识符和直接篡改数据 3 种形式. 由于安全通信系统会计算每帧报文的 MAC 值，被篡改攻击后，网络监测状态为 MAC 认证错误.

(4) 拒绝服务攻击. 通过 CAN 卡从外部接入仿真的网络环境. 设置 PCAN 工具发送报文标识符为 0x01(高优先级)、数据场 64 个字节均为零的报文，间隔为 1 ms，如图 10 所示. 网络负载率在拒绝服务攻击后迅速达到 100%. 此时正常的通信报文无法成功发送，网络监测状态为网络高负载.

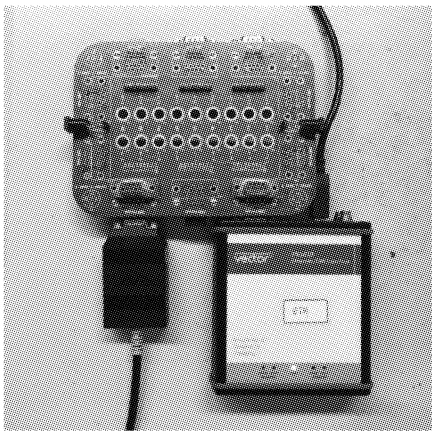

图 10 拒绝服务攻击的测试环境

Fig.10 Test environment for denial-of-service attack

综上，安全通信系统中网络遭受到攻击及入侵检测状态判断指标如表 3 所示.

表 3　网络入侵判断指标

Tab.3　Judgment index of network intrusion

攻击类型	状态报告
更换密钥	MAC 认证错误
重放攻击	时间戳错误
拦截报文	等待超时
篡改报文	MAC 认证错误
DOS 攻击	网络高负载

5　结语

以数据加密和消息认证为基础，结合随机数和时间戳机制，建立了一种基于 CAN-FD 网络的汽车通信网络信息安全方法. 研究提出了包括安全传输、安全启动、时间同步与密钥分配协议的汽车网络安全通信流程，并建立了车辆网络仿真模型，验证了安全协议的通信机密性、新鲜性、完整性、真实性以及可用性. 针对汽车通信网络潜在的攻击方式，基于 Dolev-Yao 攻击模型和拒绝服务攻击场景，对安全通信模型进行了入侵测试. 测试结果验证了该安全通信方法的安全性和可用性.

由于测试用例的限制，提出的 CAN-FD 网络安全通信方法在实际运行环境中可能会遇到更复杂的网络攻击场景. 后续可以结合真实的车辆网络环境进行安全通信的性能分析.

参考文献：

[1] KOSCHER K, CZESKIS A, ROESNER F, *et al*. Experimental security analysis of a modern automobile [C]//IEEE Symposium on Security and Privacy. Oakland: IEEE, 2010: 447-462.

[2] VAN HERREWEGE A, SINGELEE D, VERBAUWHEDE I. CANAuth - A simple, backward compatible broadcast authentication protocol for CAN bus[C]//ECRYPT Workshop on Lightweight Cryptography. Louvain-la-Neuve: ECRYPT, 2011: 1-7.

[3] HARTKOPP O, REUBER C, SCHILLING R. Message authenticated CAN [C]//Embedded Security in Cars Conference. Berlin: ESCAR, 2012: 1-7.

[4] WOO S, JO H J, LEE D H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN [J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 993.

[5] WOO S, JO H J, KIM I S, *et al*. A practical security architecture for in-vehicle CAN-FD[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2248-2261.

[6] 吴尚泽，秦贵和，刘毅，等. 车载控制器局域网络总线的动态口令身份认证方法[J]. 西安交通大学学报，2017，51(6)：97.
WU Shangze, QIN Guihe, LIU Yi, *et al*. A method for identifying authentication of dynamic passwords for in-vehicle controller area networks buses[J]. Journal of Xi'an Jiaotong University, 2017, 51(6): 97.

[7] 于赫. 网联汽车信息安全问题及 CAN 总线异常检测技术研究[D]. 长春：吉林大学，2016.
YU He. Research on connected vehicle cyber security and anomaly detection technology for in-vehicle CAN bus [D]. Changchun: Jilin University, 2016.

[8] RUDDLE A, WARD D, WEYL B, *et al*. Deliverable D2.3: Security requirements for automotive on-board networks based on dark-side scenarios [R]. Darmstadt: EVITA Consortium, 2009.

[9] HARTWICH F. CAN with flexible data-rate[C]//International CAN Conference. Hambach Castle: CIA, 2012:1-9.

[10] National Institute of Standards and Technology. Advanced encryption standard (AES): FIPS PUB 197[S]. Gaithersburg: Federal Information Processing Standards Publications, 2001.

[11] IEEE Instrumentation and Measurement Society. IEEE standard for a precision clock synchronization protocol for networked measurement and control systems: 1588—2008[S]. New York: IEEE, 2008.

[12] ESCHERICH R, LEDENDECKER I, SCHMAL C, *et al*. SHE-Secure hardware extension functional specification[S]. [S.l.]: HIS AK Security, 2009.

[13] DOLEV D, YAO A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198.