DOI：10.7652/xjtuxb201812010

车载 FlexRay 总线安全协议的设计与实现

韩正士[1]，秦贵和[1,2]，赵睿[1]，刘毅[1]，梁云龙[3]
（1. 吉林大学计算机科学与技术学院，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. 吉林大学软件学院，130012，长春）

摘要：针对智能车、网联车的高速发展所引发的车载信息安全问题设计了车载 FlexRay 总线安全协议。该协议包含两个模块：节点身份认证模块和网络安全加密模块。节点身份认证模块采用密钥交换算法以及非对称加密算法保证连入总线节点身份的合法性；网络安全加密模块采用对称加密算法以及哈希算法保证总线传输数据的机密性、真实性和新鲜性。与其他协议相比，该协议既能够提供节点的身份认证，又能在不影响总线实时通信的基础上保护总线的信息安全。实验结果表明，该协议能够在满足实时通信的基础上为汽车提供从启动到运行全方位的信息安全防护，提升了车载 FlexRay 总线的信息安全防护级别。

关键词：车载信息安全；FlexRay 总线；安全协议；实时通信
中图分类号：TP399 **文献标志码**：A **文章编号**：0253-987X(2018)12-0063-07

Design and Implementation of Security Protocol for In-Vehicle FlexRay Buses

HAN Zhengshi[1], QIN Guihe[1,2], ZHAO Rui[1], LIU Yi[1], LIANG Yunlong[3]
(1. College of Computer Science and Technology, 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 Software, Jilin University, Changchun 130012, China)

Abstract: A security protocol for in-vehicle FlexRay buses is proposed in allusion to the in-vehicle information security issue caused by the rapid development of intelligent vehicles and networked vehicles. The protocol contains two modules: a node identity authentication module and a network security encryption module. The node identity authentication module uses a key exchange algorithm and a asymmetric encryption algorithm to ensure the identity legality of the connected node, and the network security encryption module uses the symmetric encryption algorithm and a hash algorithm to guarantee the confidentiality, authenticity and freshness of the data transmitted by a bus. Compared with previous protocols, the proposed protocol provides node identity authentication and protects the information security of the on-board bus without affecting the real-time communication of the bus. Experimental results show that the protocol provides all-round information security guarantee for buses from start-up to operation on the basis of real-time communication, and greatly improves the security level of the FlexRay bus information.

Keywords: in-vehicle information security; FlexRay bus; security protocol; real-time communication

收稿日期：2018-01-29。 作者简介：韩正士(1993—)，男，硕士生；秦贵和(通信作者)，男，教授，博士生导师。 基金项目：吉林省重点科技攻关资助项目(20150204034GX)。
网络出版时间：2018-10-29 网络出版地址：http://kns.cnki.net/kcms/detail/61.1069.T.20181026.0919.002.html

汽车不仅是简单的机械装置,现代汽车包含大量用以检测和控制车辆状态的电子控制单元(ECU)。ECU 通过不同的总线网络进行信息交互,各个总线网络通过网关连接构成车载总线网络系统[1]。常见的车载总线网络包括 CAN、FlexRay、MOST 和 LIN 等。

传统汽车与外界是隔离的,所以车载总线在设计之初并没有考虑到车载信息安全问题。然而,随着汽车智能化与网联化的发展与普及,汽车通过网络与外界的信息交互愈加频繁,汽车内部与外部的访问接口也随之增多,车载信息安全问题面临着前所未有的挑战[2]。

近年来,世界各地的研究者对车载总线信息安全问题展开了大量研究。Koscher 等提出通过在汽车诊断端口设置特殊仪器攻击车载总线网络的漏洞能够控制刹车、雨刷器等,由于被攻击车辆缺少对通信数据进行解析和验证的过程,所以很容易被攻击[3];著名白帽黑客 Miller 和 Valasek 利用笔记本与车载总线相连,可以读取与写入总线数据,从而控制车辆的转向、制动等功能,威胁车辆安全[4];Woo 等利用手机 APP 通过蓝牙和 Wi-Fi 与车载诊断系统(OBD)接口设备相连,对车内 ECU 节点进行攻击,攻击行为甚至可以关闭发动机[5]。

这些研究工作使人们开始重视车载信息安全防护技术的研究与发展。EVITA 明确定义了电子安全入侵保护应用的安全要求,并为车载网络开发了适当的解决方案[6];SeVeCOM 为车与车通信和车与基础设施通信定义了安全架构,并为这些网络安全功能的部署提出了一个路线图[7];OVERSEE 的目标是制定一个开放式的汽车信息平台以保证信息的安全性和可靠性,该项目为车载应用开发提供了一个标准化的运行环境和接口,为车内资源的访问提供了统一的策略并整合了安全模块[8];AUTOSAR 4.1.0 增加了密码服务管理和密码抽象库以支持密码学相关技术和功能的使用[9],但是这些项目并没有给出具体的安全措施,也没有为具体的车载网络设计具体有效的安全协议。

为了设计出具体的安全协议保护车载网络的信息安全,从汽车的启动阶段入手,利用动态口令方法设计了车载总线的身份认证协议[10],然而该协议没有考虑车辆运行阶段面临的伪造、重放等攻击风险;文献[11-13]中提出的安全协议考虑了车载总线网络的广播特性,从车载总线负载受限的角度出发设计了车载总线安全协议,但是该协议不仅不能保护信息的机密性,而且增加了总线的通信延迟。

本文针对车载 FlexRay 总线的特点及其安全需求,提出了车载 FlexRay 总线安全协议。不同于现有的将车辆启动安全与通信安全分离的协议,本文提出的安全协议充分考虑了车辆启动阶段和通信阶段所面临的安全问题,在满足实时通信的基础上,为车辆提供从系统启动到结束全方位的信息安全保护。为验证本文提出的安全协议不仅能为车载 FlexRay 总线信息安全提供更加全面有效的防护,而且满足其他协议不能满足的高实时性通信需求,搭建了基于飞思卡尔 MC9S12XF512 的 FlexRay 总线线控子系统,并进行了全面的测试,结果证明本文提出的安全协议在有效性和实时性方面的性能更好。

1 FlexRay 总线概述及其安全需求

FlexRay[14]是一种高速、高可靠性、高确定性以及具备故障容错能力的总线技术,被广泛用于车载线控系统。

1.1 FlexRay 总线概述

FlexRay 总线支持双通道传输,每条通道的传输速率最高可达 10 Mbit/s,双通道最高可达 20 Mbit/s,而且双通道冗余通信可以提供很多网络不具备的可靠性。同时 FlexRay 总线支持多种拓扑结构,包括总线型、星型、多星型和混合型,为网络配置提供了灵活性。

FlexRay 总线的通信是在周期循环中进行的,每个通信周期由静态段、动态段、符号窗和网络空闲时间构成[14]。静态段采用 TDMA 技术实现时间触发,该技术将固定的时隙分配给固定的节点,每个节点只能在自己的时隙内发送数据。动态段采用 FTDMA 技术实现事件触发,每个节点利用报文 ID 中定义好的优先级竞争微时槽,一旦出现总线访问,时槽就会根据需要的时间扩展。

1.2 FlexRay 总线安全需求

车载 FlexRay 总线面临的攻击方式包括:恶意窃听总线数据、伪造攻击、重放攻击。为保证总线的信息安全,FlexRay 总线安全协议需要满足以下 4 点安全需求:①节点身份真实性,网络启动阶段对节点的合法性进行验证,确保连入网络的每一个节点都是合法的;②数据机密性,保证总线中传输的敏感消息即使被窃听也不泄露消息的真实内容;③数据真实性,保证消息来自合法的发送方,确保消息不是被伪造或者篡改的;④数据新鲜性,保证数据包是发送节点近期产生的,确保消息不是被重放的。

2　FlexRay 总线安全协议

2.1　模型假设

FlexRay 总线节点通信建立在时隙的基础上，因此协议为节点设置了基于通信时隙的本地通信计数器。除此之外，本文假设网关节点 G 是安全的且已经存储了每个从节点 E_i 的身份认证密钥 P_i 和通信密钥 K_i；每个从节点都存储了网关节点的认证密钥 P_G。图 1 给出了网络的架构图以及每个节点需要内置的密钥。

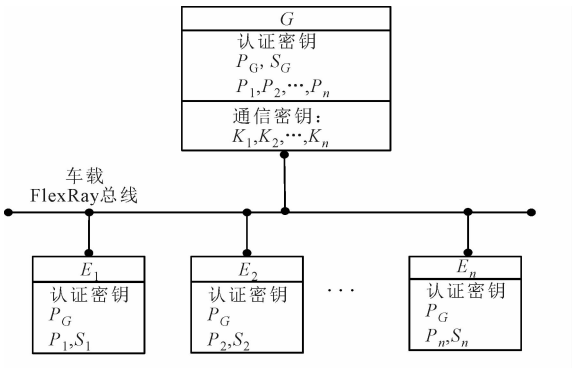

图 1　网络架构图

2.2　符号说明

本文提出的安全协议主要包含两个模块：节点身份认证模块和网络安全加密模块。表 1 列出了本文描述安全协议需要用到的符号及说明。

表 1　本文提出的安全协议所需符号及说明

符号	说明
G	网关节点
E_i	编号为 i 的节点
I_i	E_i 的标识号
$T_{i,j}$	E_i 在时隙的本地通信计数器
C	密文
M	明文
P_i	E_i 的 RSA 公钥
S_i	E_i 的 RSA 私钥
P_G	G 的 RSA 公钥
S_G	G 的 RSA 私钥
K_i	E_i 的通信密钥
R_i	G 与 E_i 认证生成的随机数
Q_i	网关利用 RSA 算法加密 R_i 生成的密文
Q'_i	E_i 利用 RSA 算法加密 R_i 生成的密文
R'_i	解密 Q'_i 获得的明文
U_i	由 RSA 算法加密 K_i 生成的密文
H_i	由 RSA 算法加密 I_i 生成的密文
$F(K_i, X)$	RSA 算法通过密钥 K_i 对数据 X 加解密
$V(K_i, X)$	RC5 算法通过密钥 K_i 对数据 X 加解密
$W(X)$	BKDR 算法对数据 X 计算消息认证码

2.3　节点身份认证模块

节点身份认证模块主要完成两个工作：一是网关对每个子节点的合法性进行认证；二是网关为每个通过认证的子节点分配通信密钥。本文利用 DH[15] 密钥交换协议的思想以及非对称加密算法 RSA[16] 公钥加密私钥解密技术完成该模块的工作。节点身份认证主要分为以下 4 个步骤。

步骤 1　节点 E_i 利用公钥 P_G 加密 I_i 发给网关节点，网关节点收到后利用私钥 S_G 解密，判断 I_i 是否为合法节点，是则转至步骤 2；否则认证失败，其形式化描述为

$$H_i = F(P_G, I_i) \tag{1}$$

$$I_i = F(S_G, H_i) \tag{2}$$

步骤 2　网关节点生成随机数 R_i 并利用公钥 P_i 加密发送给节点 E_i，节点 E_i 收到后使用私钥 S_i 解密得到随机数的明文 R_i，转至步骤 3，其形式化描述为

$$Q_i = F(P_i, R_i) \tag{3}$$

$$R_i = F(S_i, Q_i) \tag{4}$$

步骤 3　节点 E_i 利用公钥 P_G 加密随机数 R_i 发送给网关节点，网关节点收到后利用私钥 S_G 解密得到随机数 R'_i，此时判断 R'_i 是否等于 R_i，若相等转至步骤 4；否则认证失败，其形式化描述为

$$Q'_i = F(P_G, R_i) \tag{5}$$

$$R'_i = F(S_G, Q'_i) \tag{6}$$

步骤 4　网关利用公钥 P_i 加密通信密钥 K_i 发送给节点 E_i；节点 E_i 利用私钥 S_i 解密获得通信所需要的密钥 K_i，其形式化描述为

$$U_i = F(P_i, K_i) \tag{7}$$

$$K_i = F(S_i, U_i) \tag{8}$$

2.4　网络安全加密模块

为保护通信阶段的信息安全，本文利用对称加密算法 RC5[17] 对数据进行加密，保护数据机密性；利用 BKDR 哈希算法对帧和本地通信计数器计算消息认证码，保护数据的真实性和新鲜性。

发送节点在发送消息前，需要对消息进行如下 4 个步骤的处理。

步骤 1　发送节点 E_s 利用加密算法 RC5 对明文数据 M 加密生成密文 C，即

$$C = V(K_i, M) \tag{9}$$

步骤 2　发送节点 E_s 利用 BKDR 算法对本地通信计数器 $T_{s,j}$ 和密文数据 C 计算消息认证码 A，即

$$A = W(C \,||\, T_{s,j}) \tag{10}$$

步骤 3　发送节点 E_s 将密文 C 与消息认证码 A 组

成 FlexRay 总线数据帧($C||A$)发送给接收节点 E_r。

步骤 4 帧发送完成后,增加发送节点 E_s 在时隙 j 的本地通信计数器 $T_{s,j}$,即

$$T_{s,j} = T_{s,j} + 1 \tag{11}$$

接收节点在接收到消息后,需要对消息进行如下 4 个步骤的处理才能获得安全的明文数据帧。

步骤 1 接收节点 E_r 收到来自发送节点 E_s 的帧后,首先利用 BKDR 哈希算法对本地通信计数器 $T_{r,j}$ 和帧的有效负载部分 C 计算消息认证码 A'

$$A' = W(C || T_{r,j}) \tag{12}$$

步骤 2 比较 A 和 A',若相等,则证明帧是安全的,转至步骤 2;否则,认为发生了伪造攻击或者重放攻击,丢弃该帧。

步骤 3 接收节点 E_r 利用 RC5 算法以及密钥 K_i 对密文 C 进行解密获取明文 M,即

$$M = V(K_i, C) \tag{13}$$

步骤 4 完成帧的确认和解密工作后,增加接收节点 E_r 在时隙 j 的本地通信计数器 $T_{r,j}$,即

$$T_{r,j} = T_{r,j} + 1 \tag{14}$$

3 车载 FlexRay 总线安全协议实验验证与结果分析

为验证本文提出的安全协议,实验选用 4 块具有代表性的 16 位车载微控制器 MC9S12XF512 开发板模拟车载环境下的线控子系统。其中 E_0 为攻击节点,G 为网关节点,E_1 和 E_2 为合法从节点。在集成开发环境 CodeWarrior 中完成代码编写。本实验设置的 FlexRay 总线通信速率为 10 Mbit/s,通信周期为 5 ms,静态时隙的长度为 0.05 ms,配置的静态帧长度为 32 B。

3.1 车载 FlexRay 总线安全协议有效性测试与分析

实验从节点身份认证、数据机密性、数据真实性以及新鲜性 4 个方面验证本文提出的安全协议的有效性。

3.1.1 *节点身份认证* 通过合法节点和非法节点的身份认证过程对比来验证本文提出的安全协议在身份认证方面的安全性能。

首先对合法节点进行了身份认证,两个合法节点 E_1、E_2 和网关节点 G 在网络的启动阶段拥有彼此的 RSA 公钥,所以顺利地完成了身份认证过程。

表 2 第 1~3 号和第 5~7 号数据分别列举了节点 E_1 和 E_2 身份认证过程中传输的认证帧,第 4 和第 8 号的帧数据是网关节点 G 为节点 E_1 和 E_2 颁发的通信密钥。

对非法节点进行身份认证,由于缺少认证密钥,非法节点企图完成身份认证只能通过两种方式。

方式一是暴力破解。非法节点向网关节点发送伪造认证帧,试探能否被网关节点接受。这种情况下认证成功的可能性为

$$P = n/2^{16k} \tag{15}$$

式中:P 为身份认证成功的概率;n 为合法节点数;k 为用于身份认证的数据帧字节长度。当用于身份认证的数据帧长度 k 足够大时,身份认证成功的概率 P 接近于 0,因此暴力破解的攻击方式是无效的。

表 2 第 9~12 号的帧数据列举了实验中非法节点 E_0 发送的伪造认证帧,在身份认证的步骤 1 网关节点成功地识别出该帧是非法认证帧。

方式二是攻击节点通过恶意监控其他合法节点的认证过程,重放监听到的合法认证帧。然而协议使用的是动态认证模式,每一次认证过程都不同。这种情况下认证成功的可能性为

$$P = n/2^{8k} \tag{16}$$

与暴力破解类似,当用于身份认证的数据帧 k 足够大时,身份认证成功的概率 P 接近于 0,因此这种通过恶意监控其他节点认证过程并重放合法认证帧的攻击方式是无效的。

表 2 第 13~15 号和第 16~18 号数据分别列举了实验中非法节点 E_0 重放的 E_1 和 E_2 的合法认证帧。虽然 E_0 完成了身份认证的步骤 1 和 2,但在步骤 3 仍被网关 G 检测出非法认证。

通过分析与实验验证得出,本文设计的安全协议能够保证连入网络节点的合法性。

3.1.2 *数据机密性* 本文提出的安全协议使用 RC5 加密算法对数据加密来保障数据的机密性。

表 3 给出了实验中部分数据的前 4 个字节,由表 3 可以看出,节点发送的数据与总线实际传输的数据存在巨大差异,因此即使被恶意窃听也不会暴露关键信息,且由 RC5 算法的特性可知,在通信密钥不被泄露的情况下攻击者破解密文的概率几乎为 0,从而保证了数据的机密性。

3.1.3 *数据真实性和新鲜性* 本文提出的安全协议使用 BKDR 哈希算法对数据和通信计数器计算消息认证码来保护数据的真实性和新鲜性。实验中截取计算出的消息认证码的其中 4 个字节填到 FlexRay 总线数据帧的有效数据后面作为有效消息认证码。攻击者想要伪造帧消息进行伪造攻击,只有通过暴力测试的方法选取消息认证码,即从 2^{32} 个

可能的消息认证码中选择一个，填入帧的后 4 个字节发送给接收方。由于 FlexRay 总线通信周期的限制，想要逐个去试探发送这些可能的消息认证码，大概需要 2^{20} h 甚至更多，这对攻击者来说是十分不现实的。

表 4 给出了实验中的部分数据的前 8 个字节及其消息认证码，其中第 1～6 号数据是节点 E_1 和 E_2 发送的合法帧，第 7～9 号数据是攻击节点 E_0 进行伪造攻击时发送的伪造帧，接收节点收到伪造帧时成功检测出发生了伪造攻击，保证了数据的真实性。

假设攻击者能够监控总线传输的帧消息，网络就面临着被重放攻击的危险。在本文提出的安全协议中，收发节点共同维护一个基于收发时隙的通信计数器，消息认证码是 BKDR 哈希算法对消息和通信计数器同时计算得到的，因此即使消息相同，发送时间不同，计算出的消息认证码也是不同的。

表 4 的第 10～12 号数据给出了实验中攻击节点 E_0 进行重放攻击时发送的帧消息，接收节点接收到重放帧时成功检测出重放攻击，保证了数据的新鲜性。

以上实验证明本文提出的安全协议能够保证消息的机密性、真实性和新鲜性。

表 2　身份认证阶段节点间传输的认证帧的检测结果

序号	发送节点	时隙序号	数据长度	数据	单步认证结果
1	E_1	1	8	0x 00 b4 06 67 09 f5 05 6b	成功
2	G	4	8	0x 03 d8 04 bb 0c 0e 09 41	成功
3	E_1	1	8	0x 08 00 01 1e 07 f2 03 43	成功
4	G	4	16	0x 00 01 06 d8 04 bb 05 6b	空
				0c 0e 03 38 09 41 07 f9	
5	E_2	2	8	0x 07 e3 08 30 05 29 07 f2	成功
6	G	5	8	0x 04 60 06 e5 01 7e 04 56	成功
7	E_2	2	8	0x 0b f5 00 2f 03 8c 02 67	成功
8	G	5	16	0x 00 54 03 43 01 57 07 f2	空
				07 9f 01 1e 08 00 00 01	
9	E_0	3	8	0x 00 01 02 03 04 05 06 07	失败
10	E_0	3	8	0x 07 e3 00 05 29 07 07 db	失败
11	E_0	3	8	0x e3 00 d8 e1 3d 00 11 43	失败
12	E_0	3	8	0x ee 35 53 46 93 03 12 24	失败
13	E_0	3	8	0x 00 b4 06 67 09 f5 05 6b	成功
14	G	6	8	0x 06 f3 00 26 03 a0 02 4d	成功
15	E_0	3	8	0x 08 00 01 1e 07 f2 03 43	失败
16	E_0	3	8	0x 07 e3 08 30 05 29 07 f2	成功
17	G	6	8	0x 0b f5 00 2f 03 8c 02 67	成功
18	E_0	3	8	0x 07 f5 07 78 06 5d 05 46	失败

表 3　通信阶段节点发送数据(明文)与总线传输数据(密文)对比

序号	发送节点	时隙序号	数据长度	节点发送数据(明文)	总线传输数据(密文)
1	E_1	1	4	0x 25 87 13 27	0x 3f 63 a1 44
2	E_1	1	4	0x 1e b3 0a b2	0x 92 39 f7 0f
3	E_2	2	4	0x 1e b3 0a b2	0x e5 14 d8 24
4	E_2	2	4	0x 31 13 25 52	0x 35 4f b3 b4
5	G	4	4	0x 25 87 13 27	0x 3f 63 a1 44
6	G	5	4	0x 21 8e 11 26	0x cc 1a 0e d3

表 4 通信阶段攻击节点进行伪造攻击和重放攻击后总线检测结果

序号	发送节点	通信计数	数据(8 B)	消息认证码(4 B)	是否合法帧
1	E_1	1	0x 11 26 21 8e 00 03 00 04	0x 2e a9 5a 9e	是
2	E_1	3	0x 15 97 22 3e 00 03 00 04	0x f0 65 99 b7	是
3	E_1	4	0x 3d 44 21 25 00 08 00 03	0x 5b 20 c4 55	是
4	E_2	1	0x 4c 87 24 54 00 0e 00 03	0x bf 4f 83 c7	是
5	E_2	5	0x 56 49 21 a8 00 01 00 03	0x 8c 73 d6 f9	是
6	E_2	9	0x 21 51 35 91 00 0d 00 0c	0x 10 37 5b cf	是
7	E_0	25	0x 12 11 25 16 00 01 00 01	0x 25 56 49 93	否
8	E_0	31	0x 5e d7 07 49 00 0e 00 09	0x b4 f7 d5 17	否
9	E_0	33	0x 15 67 18 91 00 0a 00 0c	0x 45 27 e9 93	否
10	E_0	41	0x 11 26 21 8e 00 03 00 04	0x 2e a9 5a 9e	否
11	E_0	46	0x 15 97 22 3e 00 03 00 04	0x f0 65 99 b7	否
12	E_0	51	0x 4c 87 24 54 00 0e 00 03	0x bf 4f 83 c7	否

3.2 车载 FlexRay 总线安全协议实时性测试与分析

在 FlexRay 总线的节点身份认证模块采用 RSA 算法进行认证和颁发密钥。按照协议的设计，从节点需要进行 3 次 RSA 加解密运算，网关节点需要进行 3 次 RSA 加解密运算，此外还要考虑通信的链路延迟，因此单个节点的认证时间为

$$T_{\text{auth}} = 6T_{\text{RSA}} + 4T_{\text{Slot}} \tag{17}$$

式中：T_{auth}为单个节点认证时间；T_{RSA}为 RSA 算法在微控制器 MC9SXF512 中加解密所需要的时间；T_{Slot}为 FlexRay 总线静态时隙的长度。

在 FlexRay 总线的网络安全加密模块，采用对称加密算法 RC5 和消息认证 BKDR 算法共同保障 FlexRay 总线的信息安全。按照协议的设计，收发节点各需要进行一次加解密运算和一次消息认证运算；此外还需要考虑通信的链路延迟，因此，FlexRay 总线帧的响应时间为

$$T_{\text{repose}} = 2(T_{\text{RC5}} + T_{\text{BKDR}}) + T_{\text{Slot}} \tag{18}$$

其中：T_{repose}为 FlexRay 总线数据帧响应时间；T_{RC5}为 RC5 算法在微控制器 MC9SXF512 中加解密所需要的时间；T_{BKDR}为 BKDR 哈希算法在微控制器 MC9SXF 512 中计算消息认证码所需要的时间。

实验使用示波器测量了各安全算法在微控制器 MC9SXF512 中的运行时间，其中 RC5 算法的运行时间为 2.12 ms，BKDR 算法的运行时间为 0.132 ms，RSA 算法的运行时间为 0.22 ms。

通过式(17)计算可知，单个 FlexRay 总线节点认证时间为 1.52 ms，而车辆的启动一般在 3 s 左右，足以完成所有节点的身份认证。

通过式(18)计算可知，FlexRay 总线的帧响应时间为 4.554 ms，小于总线的通信周期 5 ms，因此认为本文提出的安全协议不影响车载 FlexRay 总线的实时通信。

3.3 协议对比与分析

本节将本文提出的安全协议与文献[12-13]提出的 EPSB、CSCAN 安全协议进行了比较。EPSB、CSCAN 协议考虑了车载环境下资源受限的问题以及车载总线的安全需求，并且对车载总线网络运行过程中可能遇到的伪造、篡改等攻击方式进行了防护，但是他们都没有考虑车辆启动阶段车载总线上各节点的身份认证问题以及数据的机密性问题；EPSB 协议忽略了车载总线可能面临的重放攻击；EPSB 协议和 CSCAN 协议所存在的另一个问题是忽略了车载总线的实时通信需求，严重增加了车载总线的通信延迟，这增加了车辆的安全隐患。本文提出的安全协议在满足总线实时通信需求的基础上，对车辆启动阶段与运行阶段可能遇到的攻击都进行了安全防护，从而提升了车辆的信息安全级别。

4 结 论

本文针对车载 FlexRay 总线存在的信息安全问题实现了车载 FlexRay 总线安全协议。通过实验验证，与其他安全协议相比，本文提出的安全协议既能够提供节点的身份认证，又能在不影响总线实时通信的基础上保护消息的机密性、真实性和新鲜性，提高了车辆的信息安全防护级别。未来的研究工作将把本文提出的协议在实车上进行测试，并基于车辆实际驾驶环境中总线传输的标准向量进行安全性、实时性分析，确保该协议在复杂的驾驶环境中

仍能够提高车辆的信息安全防护能力。

参考文献：

[1] 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，2016：1-31.

[2] MUNDHENK P，STEINHORST S，LUKASIEWYCZ M，et al. Lightweight authentication for secure automotive networks [C] // Proceedings of the 2015 Design，Automation and Test in Europe Conference and Exhibition. Piscataway，NJ，USA：IEEE，2015：285-288.

[3] KOSCHER K，CZESKIS A，ROESNER F，et al. Experimental security analysis of a modern automobile [J]. IEEE Journal of Selected Topics in Quantum Electronics，2010，41(3)：447-462.

[4] 于赫，秦贵和，孙铭会，等. 车载 CAN 总线网络安全问题及异常检测方法 [J]. 吉林大学学报(工学版)，2016，46(4)：1246-1253.
YU He，QIN Guihe，SUN Minghui，et al. Cyber CAN bus network security problem and anomaly detection method [J]. Journal of Jilin University (Engineering Edition)，2016，46(4)：1246-1253.

[5] 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)：990-1010.

[6] HENNIGER O. E-safety vehicle intrusion protected applications (EVITA) project [EB/OL]. (2008-07-31)[2017-10-05]. http// www. evita. org.

[7] CHOI J，JUNG S. Unified security architecture and protocols using third party identity in V2V and V2I networks [J]. Wireless Communications and Mobile Computing，2012，12(15)：1326-1337.

[8] GROLL A，HOLLE J，RULAND C，et al. Oversee a secure and open communication and runtime platform for innovative automotive applications [C] // Proceedings of the 19th Intelligent Transport Systems World Congress. Piscataway，NJ，USA：IEEE，2012：EU-00690.

[9] 赵睿. 面向时间触发网络的车载控制系统调度优化方法与轻量级消息认证协议研究 [D]. 长春：吉林大学，2017：10-15.

[10] 吴尚则，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)：97-102.
WU Shangze，QIN Guihe，LIU Yi，et al. A method for identifying authentication of dynamic passwords for in-vehicle controller area network buses [J]. Journal of Xi'an Jiaotong University，2017，51(6)：97-102.

[11] NILSSON D K，LARSON U E，JONSSON E. Efficient in-vehicle delayed data authentication based on compound message authentication codes [C] // Proceeding of the 2008 IEEE 68th Vehicular Technology Conference. Piscataway，NJ，USA：IEEE，2008：1-5.

[12] GROZA B，MURVAY S. Efficient protocols for secure broadcast in controller area networks [J]. IEEE Transactions on Industrial Informatics，2013，9(4)：2034-2042.

[13] LIN C W，SANGIOVANNI-VINCENTELLI A. Cyber-security for the controller area network (CAN) communication protocol [C] // Proceedings of the International Conference on Cyber Security. Piscataway，NJ，USA：IEEE Computer Society，2012：1-7.

[14] POP T，POP P，ELES P，et al. Timing analysis of the FlexRay communication protocol [J]. Real-Time Systems，2008，39(1/2/3)：205-235.

[15] 尹少平，董丹. Diffie-Hellman 密钥交换协议设计与实现 [J]. 电力学报，2006，21(1)：9-12.
YIN Shaoping，DONG Dan. Design and implemention of Diffie-Hellman key exchange protocol [J]. Journal of Electric Power，2006，21(1)：9-12.

[16] 陈传波，祝中涛. RSA 算法应用及实现细节 [J]. 计算机工程与科学，2006，28(9)：13-14.
CHEN Chuanbo，ZHU Zhongtao. Research on the application and implementation of the RSA algorithm [J]. Computer Engineering and Science，2006，28(9)：13-14.

[17] RIVEST R L. The RC5 encryption algorithm [C] // Proceedings of the International Workshop on Fast Software Encryption. Berlin，Germany：Springer，1994：86-96.

（编辑　武红江）