

doi: 10.7690/bgzdh.2018.10.004

导弹测发控系统 CAN 通信协议的设计与实现

陈基昕, 王 忠, 赵锦宇
(火箭军工程大学基础部, 西安 710025)

摘要: 针对导弹测发控系统实时性、可靠性和安全性的实际需求, 提出一种面向导弹测发控系统的 Missile-CAN 通信协议。详细定义报文的 29 位标识符和数据通信模式, 制定 CAN 网络的管理机制。在通信的安全性上采用 AES 加密算法对传输报文进行加密。介绍实验系统硬件平台, 并设计软件实现方法。仿真实验结果表明: 网络的通信质量良好, 总线利用率符合导弹测发控系统实时性要求, 验证了 Missile-CAN 协议的可行性。

关键词: 导弹测发控系统; CAN 总线; 通信协议

中图分类号: TJ765 **文献标志码:** A

Design and Implementation of CAN Bus Communication Protocol for Missile Test and Launch Control System

Chen Jixin, Wang Zhong, Zhao Jinyu
(Basic Department, Rocket Force University of Engineering, Xi'an 710025, China)

Abstract: Aiming at the real time, reliability and security of test and launch control system for missile, a Missile-CAN communication protocol for missile test and launch control system is proposed. The 29 bit identifier and data communication mode of the message are defined in detail, and the management mechanism of the CAN network is formulated. In the security of communication, AES encryption algorithm is used to encrypt transmission messages. The hardware platform of the experiment system is introduced and the method of software realization is designed. The simulation experiment results show that the communication quality of the network is good and the utilization rate of the bus conforms to the real-time requirement of test and launch control system for missile, and the feasibility of the Missile-CAN protocol is verified.

Keywords: test and launch control system for missile; CAN bus; communication protocol

0 引言

CAN 总线的协议对物理层和数据链路层做了详细的定义和规范, 但 CAN 应用层没有做统一的规范。对于不同的控制系统, 用户使用时会产生诸多不便^[1]。制定标准化的应用层协议, 不仅方便技术人员学习、使用和维护不同厂家制造的设备, 保证设备的互操作性, 而且能节约生产成本。国际上制定了一些较为通用的 CAN 应用层协议, 如 DeviceNet 协议、CANopen 协议等^[2]。笔者对面向导弹测发控系统的 CAN 通信协议进行研究, 对保证系统的实时性、可靠性和安全性有重要意义。

1 导弹测发控系统概述

导弹测发控系统是对导弹各信号和系统性能进行测试, 配合地面测试设备检查是否符合发射条件, 对检查合格的导弹按命令进行发射的系统^[3]。地面测试设备通过 CAN 总线互联通信, 系统实时性要

求最高可允许总线负载率达到 40%~50%^[4]。导弹测发控系统需把弹上和地面设备看成一个整体, 严格把控设备工作的先后次序, 相互统筹配合。弹上被测信号由配电转接箱引入地面测试设备, 进行信号调理和测试, 由地面测发控系统对测试结果进行处理、分析和判断是否出现故障, 若测试合格, 则按正常操作流程进行导弹的发射任务。导弹测发控系统包含了 10 个节点, 结构组成如图 1 所示。

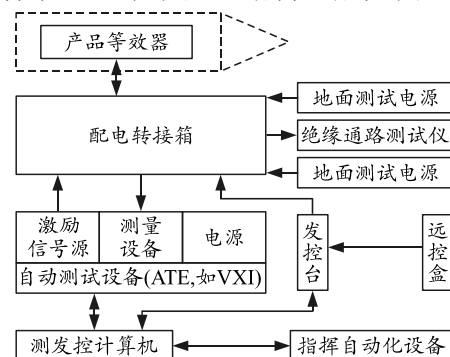


图 1 导弹测发控系统结构

收稿日期: 2018-07-19; 修回日期: 2018-08-16

作者简介: 陈基昕(1994—), 男, 福建人, 硕士研究生, 从事嵌入式系统与嵌入式网络研究。

2 构建 Missile-CAN 协议的需求分析

CAN 能适应多种场合的测控网络，但是 CAN2.0A/B 协议存在局限性，发送报文里没有自己的地址信息、发送大于 8 个字节的数据帧时需分块发送、无法监测网络的故障节点等。制定 CAN 应用层的协议应根据具体的工程需求来分析。导弹测发控系统的高可靠性、实时性和安全性是导弹能够既成功又准时发射的必备条件；因此，构建面向导弹测发控制系统的 CAN 应用层协议 Missile-CAN 应当具备以下条件：

- 1) 合理设置各节点的报文优先级，使报文在有效的传输时延内，经过仲裁机制后，都能抢夺到总线的使用权，保证每个节点的数据能成功发送出去。
- 2) CAN 测控网络中，要使数据实时有效传到目的节点，需设置有效的数据交换方法，如主从应答的命令/响应模式。
- 3) 完整的设备定义，提供完整的设备描述和设

备访问规则。

- 4) 协议的可扩展性，用于定义在未来使用过程中可能需要的拓展功能，克服某些不可预见的缺陷。
- 5) 根据系统需求合理选择报文的滤波机制。
- 6) 网络管理方面，能够监控总线状态，判断某个网络节点是处于正常或故障状态。
- 7) 数据的传输过程中，对报文使用安全性极高的 AES 加密算法进行加密。

3 Missile-CAN 协议设计

3.1 Missile-CAN 报文格式设计

CAN2.0 的规范分为具有 11 位标识符的 CAN2.0A 和具有 29 位标识符的 CAN2.0B^[5]。为了充分利用资源，使一个报文携带更多的数据信息，笔者采用 29 位标识符的 CAN 报文格式。由于导弹测发控制系统的网络节点数少于 2⁴ 个节点，因此源节点和目标节点分别只占用 4 位标识符即可。Missile-CAN 报文标识符分配如表 1 所示。

表 1 报文标识符分配

PRI		ACK		源节点				功能码				目标节点			
ID28	ID27	ID26	ID25	ID24	ID23	ID22	ID21	ID20	ID19	ID18	ID17	ID16	ID15	ID14	ID13
错误响应码		Length Flag		Seg Flag		保留		保留		资源节点					
ID12	ID11	ID10	ID9	ID8	ID7	ID6	ID5	ID4	ID3	ID2	ID1	ID0			

CAN 网络中的设备由源节点地址 (SMAC_ID) 或目的节点地址 (DMAC_ID) 唯一标识，设备通信时必须检查已知连接的两端点，确认收发双方的 SMAC_ID 和 DMAC_ID 值相同。

优先级 (PRI)：CAN 总线上的数据传输根据报文的优先级高低采用非破坏性的仲裁技术^[6]，如果不合理分配各数据类型的优先级，则有可能导致部

分数据长时间无法发送，因此需综合考虑报文的实时性、报文长度、报文传输频率和报文传输延等等因素。

响应标志位 (ACK)：该位根据报文性质进行区分，用来表示帧是否需要应答确认。

功能码 (FUNC_ID)：根据报文所能够实现的功能，把 FUNC_ID 从 0x00-0x0f 定义如表 2 所示。

表 2 功能码定义

FUNC_ID	功能	描述
0x00	Reserve	为将来预留拓展功能
0x01	建立连接	用于 Missile-CAN 主从节点间建立通信
0x02	删除连接	用于 Missile-CAN 主从节点间撤销通信
0x03	MAC ID 检测	检测网络上是否具有相同 MAC ID 的节点
0x04	设备复位	用于对 Missile-CAN 设备的复位操作
0x05	连续写端口	用于修改资源节点中的数据
0x06	连续读端口	用于读取资源节点总的的数据
0x07	事件触发端口	用于定时循环传送数据
0x08-0x0e	Reserve	为将来预留拓展功能
0x0f	错误响应	用于系统出错时的响应

错误响应码 (ERR_ID)：用于表示报文的错误类型，包括功能码不存在、资源不存在、命令不支持、功能码参数非法和连接不存在等错误。

有效数据标志位 (LengthFlag)：表示该报文中有效数据的字节数。

分段传输标志位 (SegFlag)：当需要传输的数据超过 8 个字节时，对数据进行分段传输。

保留位 (Reserve)：可以作为将来拓展的其他功能。

资源节点编号 (S_ID)：设备根据报文的资源节

点编号对内部单元进行操作。

3.2 Missile-CAN 的数据传输协议

1) 数据通信模式：在一般的测控网络中，数据的通信模式是指收发双方完成一次通信的数据交换规则^[7]。采用灵活的数据通信模式有助于提高网络的通信效率。CAN 协议中通常包含 3 种通信模式：

① 命令/响应的通信模式：主站向从站发起通信请求并建立连接。从站接收到命令帧后，判断该请求命令是否合法，若合法则向主站返回响应报文，若该请求命令出错，则在返回的响应报文中包含对应的错误码。通信过程如图 2 所示。

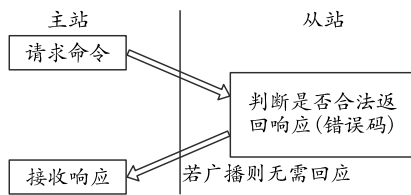


图 2 命令/响应通信模式

② 生产者/消费者的通信模式：比较灵活，节点间没有固定的联系，每个节点可以向多个节点广播发送信息，也可以接收多个节点发送来的信息，该方式可以及时有效地处理报警信息。通信过程如图 3 所示。

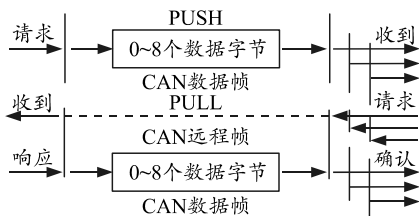


图 3 生产者/消费者通信模式

③ 事件触发的通信模式：包括定时循环发送和状态触发发送。该模式相比于命令/响应式更有利于适应 CAN 多主工作和非破坏性仲裁的特性，能够提高通信效率；因此，笔者研究的 Missile-CAN 协议采用命令/响应式和事件触发相结合的通信模式。

2) 数据通信协议：数据的通信协议一般分为面向节点和面向报文 2 类。

面向节点的通信协议，即在通信过程中，源节点地址和目标节点的地址是确定的，需要传输的报文在传输介质上通过节点寻址的方式进行通信，数据通信系统大多采用面向节点的通信协议。面向报文的通信协议，即在报文的标识符中做定义，接收节点根据报文中特定的标识符来判断是否要接收该报文，且报文可被一个或多个节点接收。数据的通信协议需要综合面向节点和面向报文 2 种类型的优

势，才能保证系统的可靠通信。

3.3 Missile-CAN 的网络管理

Missile-CAN 协议网络管理可实现节点的监控，其主要作用是能够检测和识别网络中的错误。Missile-CAN 协议网络管理由节点控制和通信控制来实现。

1) 节点控制：Missile-CAN 协议网络节点控制通过特定的状态转换机制实现，定义了总线检测、等待响应、在线初始化和通信错误 4 种通信状态。要启动网络中的某个节点，必须经历总线的检测，等待节点接收响应报文，方能进入节点的初始化，使主从设备间建立连接开始通信。协议通过设置特定报文和固定的响应时间详细定义了状态转换规则，如图 4 所示。

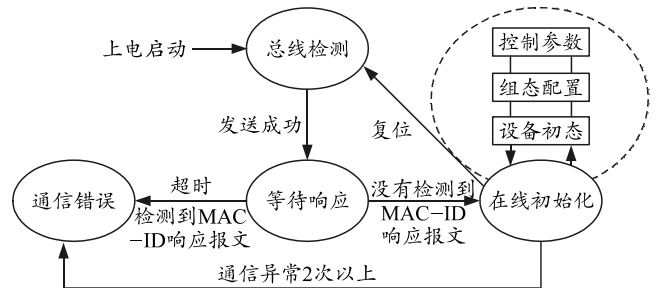


图 4 Missile-CAN 协议网络节点状态转换

系统上电或复位后进入总线检测状态，向总线上发送检测报文后需确认是否有其他节点的 MAC ID 与自身相同，此时若接收到其他节点发送的非 MAC ID 报文不予处理；在等待响应状态下，设置一个时间为 1 s 的定时器，若在定时范围内发送节点接收到了响应报文，则进入通信错误状态，若定时器超时仍未接收到响应报文，则进入在线初始化状态，若接收到其他报文仍不予处理；在线初始化状态下，主节点通过建立连接与从节点进行通信，并实现对从节点的配置，而后节点可实时处理在总线上传输的所有报文；通信错误状态下，说明总线上至少有 2 个节点的 MAC ID 相同，此时可对设备手动复位。

2) 通信控制：Missile-CAN 通信控制根据报文完成规定动作有无“超时”来判断通信是否出现了异常。

检测定时器：Missile-CAN 设备向总线上发送检测报文，同时启动检测定时器，用于查看网络上是否有地址相同的节点。若在规定时间内(时间可设置)有响应报文反馈，则说明网络上节点地址不唯一，需对发送节点或反馈响应报文的节点更改地址；

若没有接收到响应报文，则设备正常工作。检测定时器工作流程如图 5 所示。

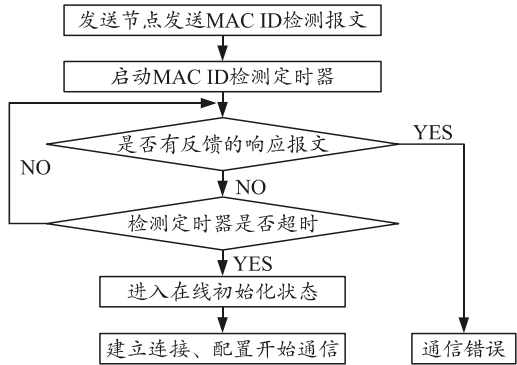


图 5 检测定时器工作流程

连接定时器：Missile-CAN 协议的主、从节点通过建立连接来通信，连接定时器用于设定主、从节点间通信的最短时间间隔。在定时范围内，若从节点接收到合法报文，则复位并重新启动连接定时器；若定时器“超时”，主、从节点仍未进行通信，则说明通信异常，从节点需删除该连接。连接定时器工作流程如图 6 所示。

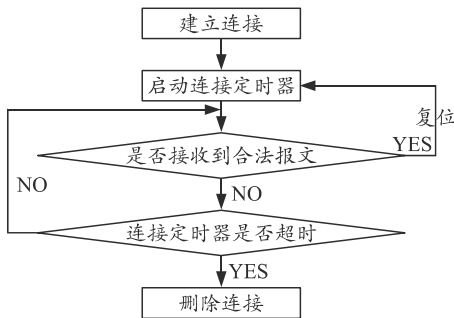


图 6 连接定时器工作流程

循环发送定时器：Missile-CAN 协议设置循环发送定时器用于时间触发传送。主、从节点建立连接并设定循环定时参数后，从节点启动循环发送定时器。当定时器计满“超时”，从节点将发送报文，并复位循环发送定时器，使定时器重新开始计时。循环发送定时器工作流程如图 7 所示。

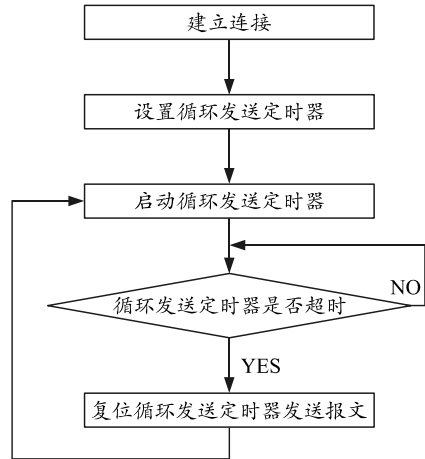


图 7 循环发送定时器工作流程

3.4 报文滤波机制

CAN 总线的滤波机制由控制器 SJA1000 的 4 个验收代码寄存器 (ACR_n) 和 4 个验收屏蔽寄存器 (AMR_n) 来实现。当一条消息发送至总线上，接收节点对比该消息是否与验收滤波器中预定义的值相同，若相同，控制器 SJA1000 才允许该消息存入 RXFIFO^[8]。本系统的节点数较少，且报文使用自定义 29 位标识符的扩展帧，选择单滤波扩展帧模式即可满足通信需求，其滤波原理如图 8 所示。

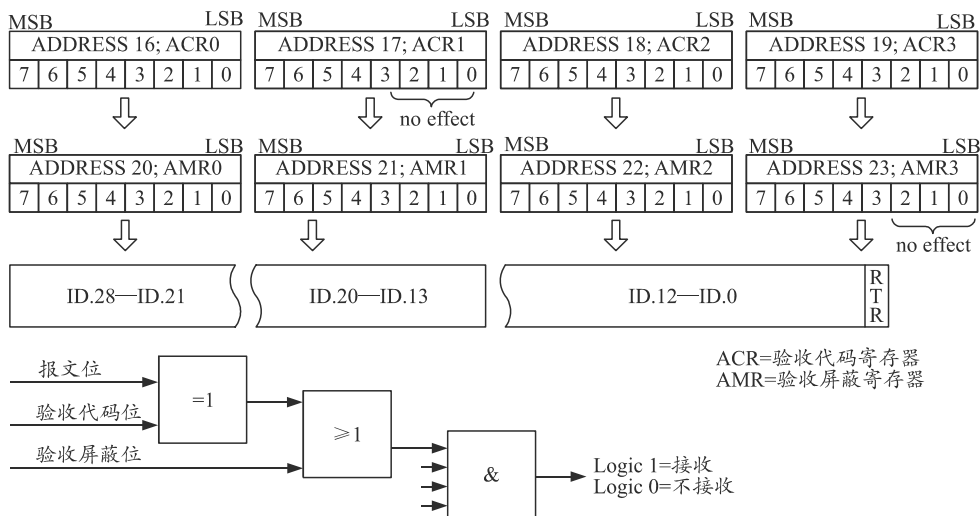


图 8 单滤波扩展帧模式

滤波规则：以扩展帧为例，AMR 所有为 0 的位所对应的 ACR 位，与接收的信息帧对应位对比，

若相同则通过滤波，接收该帧，报文的 29 位标识码需要满足以下公式：

$$[(ID.28 - ID.0) \equiv (ACR.29 - ACR.00)] \vee$$

$$(AMR.29 - AMR.00) \equiv 111 \dots 111 (29 \text{个}).$$

例如，在单滤波扩展帧模式下选择 PeliCAN 模式，要接收一个报文，该报文的 29 位标识符 ID.28-ID.0 为：0000 1110, 1001 0011, 1010 1010, 1100 1，则 4 个验收代码寄存器的设置为：ACR0=0x0E, ACR1=0x93, ACR2=0xAA, ACR3=0xC8。根据以上滤波规则，参与滤波机制的信息位所对应的验收屏蔽寄存器位都为 0，要注意 AMR₃ 的最后两位为“无关”，因此 AMR_n=0x00(n=0,1,2), AMR=0x03。

3.5 数据的加密算法

针对武器系统的特殊性，战场环境下数据通信很有可能遭到攻击和破坏，因此为保证系统的高安全性，Missile-CAN 协议采用 AES 加密算法对通信过程中的报文进行加密。

AES 加密算法先将 128 位的明文进行分组，得到一个 4×4 的明文状态矩阵作为算法的输入，然后选取密钥矩阵先对明文状态矩阵做一次轮密钥加变换，再经过 10 轮的轮函数加密，轮函数操作依次为字节替换、行位移、列混合和轮密钥加，由于最后一轮的列混合不仅不会提高安全性，反而会拉低算法运算速度，故该轮丢弃列混合变换^[9]。解密算法仍为 10 轮，由于算法的 4 个轮操作均为可逆变换，因此解密过程就是用与加密过程同样的密钥对每一轮的加密操作进行逆运算^[10]。算法的流程如图 9 所示。

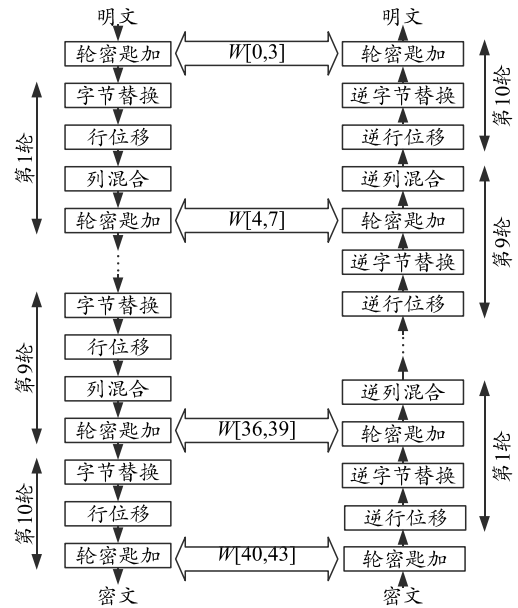


图 9 AES 加密算法流程

4 Missile-CAN 协议的仿真实验

4.1 实验系统硬件设计

硬件平台使用 CAN 总线实验板模拟导弹测发控制系统的通信节点。实验板的主控芯片采用稳定性较好的 STC89C52RC 单片机，CAN 控制器和收发器分别为 SJA1000 和 TJA1050，且开发板上有 1 个 4 位的数码管和 5 个 LED 灯，可显示通信的状况是否良好。为减小各器件的信号干扰，CAN 控制器 SJA1000 的 TX0 端和 RX0 端并不是与 CAN 收发器 TJA1050 的 TXD 端和 RXD 端直接相连，而是在节点中引入 2 个 6N137 的光耦隔离电路以及 1 个 B0505 电源隔离模块，能够有效降低误码率，提高电路抗干扰性，起到了电气隔离的作用。硬件接口电路原理如图 10 所示。

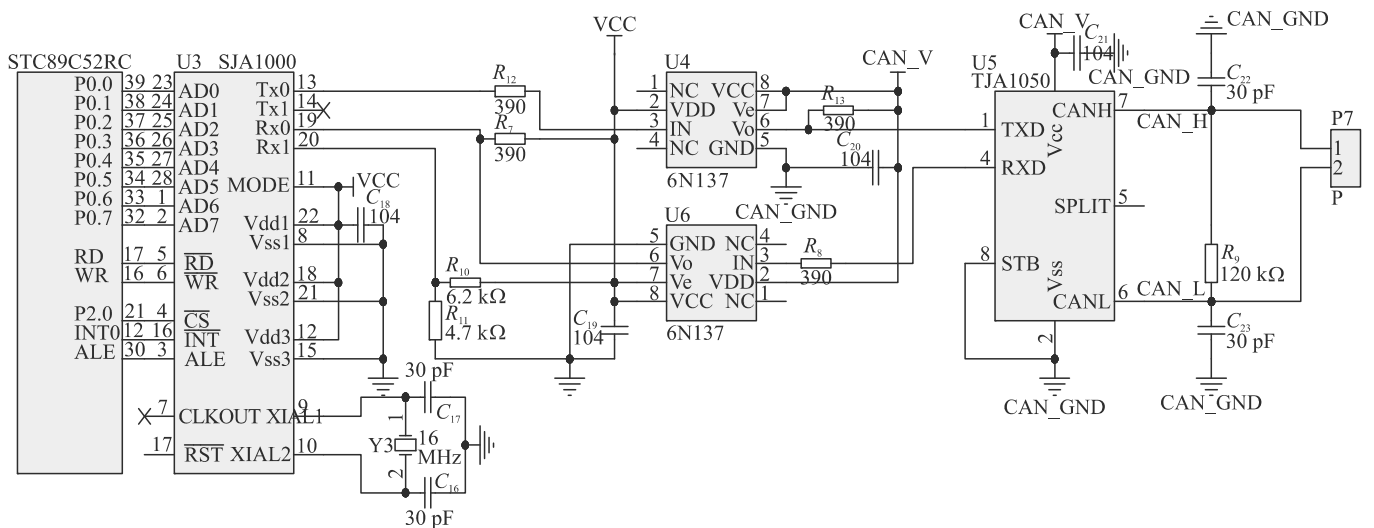


图 10 硬件接口电路原理

4.2 实验系统软件设计

1) SJA1000 初始化。

系统上电后，首先要初始化 SJA1000 来确定工作方式、波特率以及输出特性等。初始化设置必须先关闭总中断，然后在复位模式下进行，主要包括时钟分频寄存器(CDR)的设置、验收屏蔽寄存器(AMR)的设置、验收代码寄存器(ACR)的设置、波特率参数设置、总线定时寄存器(BTR0/BTR1)的设置和输出控制寄存器(OCR)的设置。初始化的流程如图 11 所示。

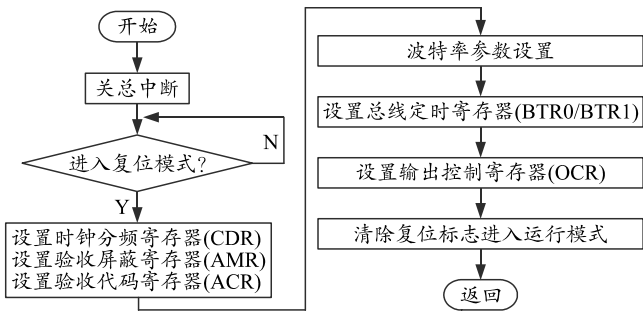


图 11 SJA1000 初始化流程

2) 发送和接收程序设计。

本系统采用查询方式发送数据。主控制器(MCU)按固定周期轮询查看状态寄存器(SR)，判断发送缓冲区是否被释放^[11]。当 TBS=1 时，要传送的数据被写入发送缓冲区，然后置命令寄存器(CMR)中发送请求位 TR=1，数据开始发送，发送完成后置位 TCS=1，即数据发送成功。发送程序的流程如图 12 所示。

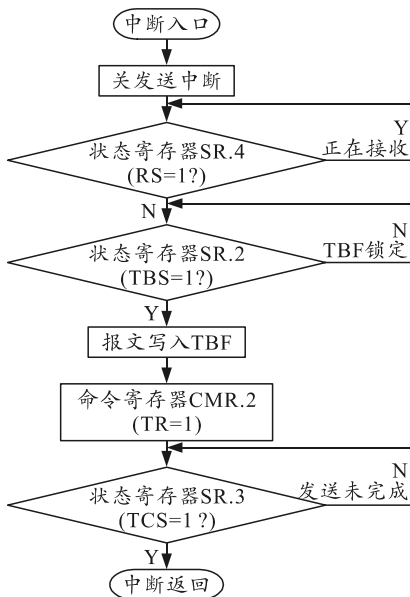


图 12 发送程序流程

接收子程序比发送子程序复杂，因为在处理接

收报文的过程中，同时要对诸如总线关闭、错误警报和接收溢出等情况进行处理。MCU 周期性地查询 SJA1000 的状态寄存器，直到接收发送缓冲区的状态标志位 RBS=1，则读取接收缓冲区的数据，并置位命令寄存器中的释放接收缓冲区标志位 RRB=1，然后依次读取状态寄存器 SR.1、SR.7、SR.6 位状态，判断接收溢出、总线开闭和是否错误，并做出相应处理。发送程序的流程如图 13 所示。

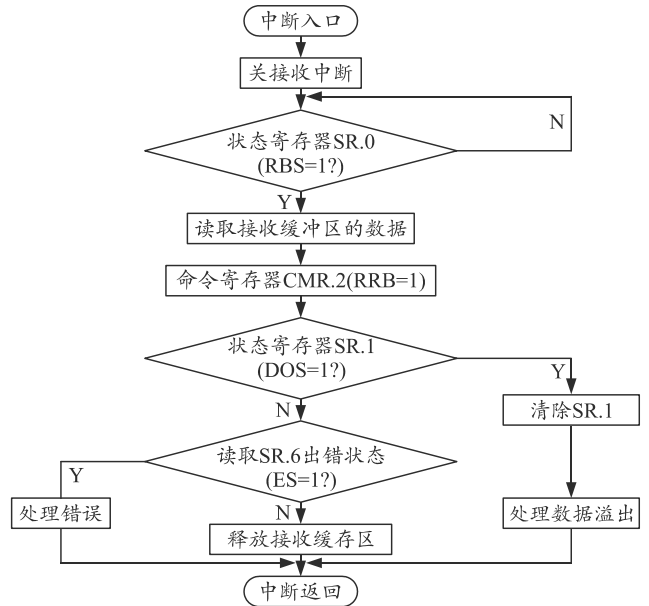


图 13 接收程序流程

3) AES 加密算法。

按照字节替换、行位移、列混合和轮密钥加的混合运算连续加密 10 轮，其主程序代码如下：

```

void aes(char *p, int plen, char *key){
    int keylen = strlen(key);
    int pArray[4][4];
    int k,i;
    ... ..
    extendKey(key);//扩展密钥
    for(k = 0; k < plen; k += 16) {
        convertToIntArray(p + k, pArray);
        addRoundKey(pArray, 0);//第一次轮
        密钥加
        for(i = 1; i < 10; i++){
            subBytes(pArray);//字节代换
            shiftRows(pArray);//行移位
            mixColumns(pArray);//列混合
            addRoundKey(pArray, i);//轮密
            匙加
        }
        subBytes(pArray);//字节代换
    }
}

```

```

shiftRows(pArray);//行移位
addRoundKey(pArray, 10);//轮密钥加
convertArrayToStr(pArray, p + k);
}
}

```

4.3 仿真实验结果

实验使用 CAN 总线专业的开发与测试工具 CAN-scope 分析仪。该仪器具备示波器、逻辑分析仪、误码率分析仪和协议分析仪的功能于一身，可从物理层、数据链路层、应用层多方位地对 CAN 总线的正确性、可靠性做定性定量的测量和分析。网络采用总线型的拓扑结构，把实验板的 CAN_H、CAN_L、VCC、GND 端对应相连，其中的一块开发板接 CAN-scope 分析仪，CAN-scope 分析仪可以通过 USB 接口把 CAN 网络与电脑的上位机软件 CANTest 相连。待系统通信稳定，CAN-scope 通信指示灯连续稳定地闪烁，可打开报文与波形同步观察的界面，如图 14 所示。

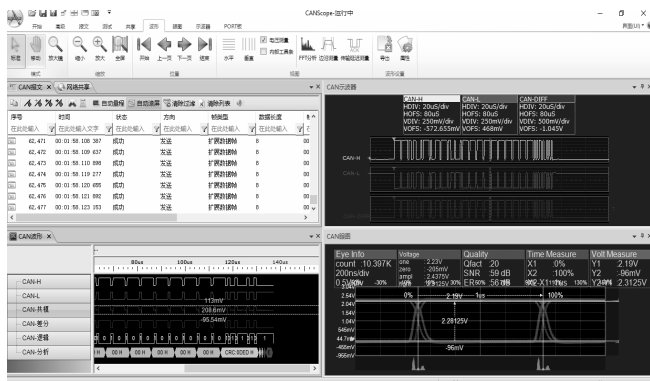


图 14 报文与波形同步观察的界面

报文的波形图符合预定发送数据的时序，说明在物理层上的通路有效。打开信息质量分析界面，可以看到每个节点的信号质量，如图 15 所示。此时点击 BusFlow，可以看到当前总线实际利用率的情况，如图 16 所示。

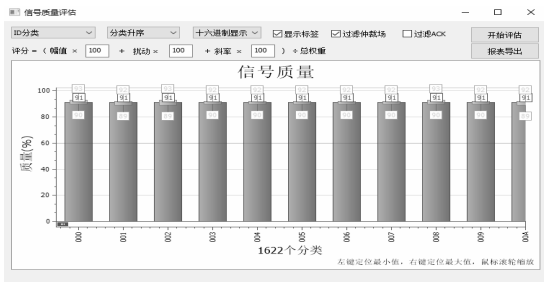


图 15 信号质量分析结果

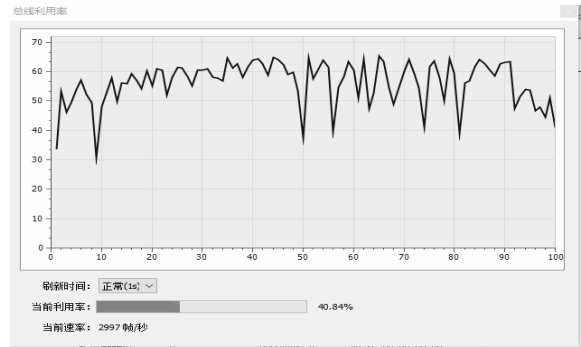


图 16 总线实际利用率界面

信号质量的评分均在 90%以上，说明 Missile-CAN 网络通信质量较可靠，没有出现故障节点。且总线利用率在 40%~50%，符合导弹测发控系统实际通信的实时性要求。

5 结束语

仿真实验结果表明：Missile-CAN 协议能满足导弹测发控系统对实时性、可靠性和安全性的实际需求，在导弹实际测试、发射和控制过程中具有一定的应用价值。

参考文献：

- [1] 王邦继. CAN 总线应用层协议的研究与实现[J]. 计算机工程与应用, 2011, 47(20): 14-16.
- [2] 王黎明, 夏立, 邵英, 等. CAN 现场总线系统的设计与应用[M]. 北京: 电子工业出版社, 2008: 25-26.
- [3] 王储. 某型号导弹测发控系统研制[D]. 哈尔滨: 哈尔滨工业大学, 2013: 6-7.
- [4] 张杨, 徐宏伟, 黎玉刚, 等. 基于 1553B 总线的导弹武器系统通信协议设计与仿真[J]. 弹箭与制导学报, 2014, 34(6): 177-180.
- [5] 饶运涛, 邹继军. 现场总线 CAN 原理与应用技术[M]. 北京: 北京航空航天大学出版社, 2003: 33-34.
- [6] 李恒征. 基于 CAN 总线的煤矿工作面控制系统远距离传输的研究与实现[D]. 淮南: 安徽理工大学, 2013: 17.
- [7] 卫威, 左政, 李振龙, 等. 乘用车 CAN 总线通信负载率算法设计[J]. 汽车电器, 2017, 12(3): 73-74.
- [8] 瞿军, 邵建波, 李昊. 基于 CAN 总线的舰载导弹测发控系统[J]. 火力与指挥控制, 2005, 30(8): 189-191.
- [9] 温巧燕. 现代密码学中的布尔函数[M]. 北京: 科学出版社, 2000: 97-98.
- [10] 张丽红, 凌朝东. 基于 AES 算法中 S 盒的分析研究与改进[J]. 信号处理, 2011, 27(9): 1428-1433.
- [11] 朱宇光, 周旦辉, 胡悦. 防空导弹抗干扰性能试验方法研究[J]. 兵工自动化, 2017, 36(1): 35-38.