电动汽车 CAN 总线协议的重放攻击与防御方法

王勇[1]，李亚菲[1]，陈雪鸿[2]，刘丽丽[3]，吴旻[1]
（1. 上海电力大学，上海市 杨浦区 200090;
2. 国家工业信息安全发展研究中心，北京市石景山区 100040;
3. 华电电力科学研究院有限公司国家能源分布式能源技术研发（实验）中心，浙江省杭州市 310030）

Replay Attack and Defense Method of CAN Bus Protocol for Electric Vehicle Charging

WANG Yong[1], LI Yafei[1], CHEN Xuehong[2], Liu Lili[3], WU Min[1]
(1.Shanghai University of Electric Power, Yangpu District, Shanghai 200090, China;
2.China Industrial Control Systems Cyber Emergency Response Team, Shijingshan District, Beijing 100040,China;
3.National Energy Distributed Energy Technology Research and Development (experimental) Center, Huadian Electric Power Research Institute Co., Ltd., Hangzhou 310030, Zhejiang Province, China)

Abstract: The CAN protocol is used to communicate data between electric vehicles and the charger adopts. However, the protocol is a broadcasting protocol without authentication scheme, lacks encryption function and CAN frame does not contain the source address and the destination address, which makes it possible for hackers to carry out replay attack, which makes the energy interconnection face huge risk. In order to verify the security problems of CAN communication protocol, this paper uses STM32F767, usb-can converter and PC to build the hardware environment of CAN communication. In order to enhance the security of CAN protocol, an algorithm of adding random Numbers to resist replay attack is proposed. Under the experimental environment of Eclipse, the normal charging, replay attack and defense by adding random Numbers of electric vehicles are simulated. Experimental results show that this method can effectively enhance the ability of CAN bus to resist replay attack.

Keywords: electric vehicles; CAN protocol; replay attack; add a random number

摘　要：CAN通信协议是当前能源互联网中电动汽车与充电桩之间的通信协议，但是由于该协议是没有认证方案的广播协议、缺乏加密功能以及CAN帧中不包含源地址和目的地址，存在黑客重放攻击的可能,严重威胁能源互联网的安全。为了验证CAN通信协议存在的安全问题，本文采用STM32F767、USB-CAN转化器和PC机搭建有关CAN通信的硬件环境。为了增强CAN协议的安全性，提出了一种加随机数抵御重放攻击的算法。在Eclipse的实验环境下模拟电动汽车正常充电、重放攻击以及加随机数进行防御的三种模式过程。实验结果表明，该方法可以有效增强CAN总线抵御重放攻击的能力。

关键词：电动汽车；CAN协议；重放攻击；加随机数

0　引言

控制器局域网(controller area network ,CAN)是一种串行通信协议，分为CAN2.0A和CAN2.0B两个版本，A版本的协议为11位标识符（标准帧），B版本在兼容11位ID标识符的同时，向上扩展到29位ID标识符。BMS与充电机之间的通信就采用的是CAN2.0B协议，该协议具有通信速度快、通信距离远，可同时连接多个CAN节点、多主控制等优点，但是由于CAN协议本身存在的一些安全漏洞，使得电动汽车在充电过程中也面临着一系列信息安全问题，因此，增强CAN通信协议的安全性具有十分重要的意义。

随着信息技术在充电服务网络中的大规模应用，

基金项目：国家自然科学基金项目（61772327）；上海自然科学基金（16ZR1436300）；浙江大学工业控制技术国家重点实验室开放式基金（ICT1800380）；智能电网产学研开发中心项目（A-0009-17-002-05）。

The National Natural Science Foundation of China(61772327); Shanghai Natural Science Foundation(16ZR1436300); Open Research Fund from State Key Laboratory of Industrial Control Technology(ICT1800380); Smart Grid Industry-University Research and Development Center Project(A-0009-17-002-05).

CAN协议漏洞可能会造成一些通信安全问题，比如：黑客故意攻击充电桩，使充电桩无法给电动汽车正常充电，给车主的生活带来诸多不便；恶意窃取用户的充电账号、支付密码以及充电位置等个人信息，侵犯用户的隐私权，也可能对用户造成一定经济上的损失；有些用户可能会去篡改相关充电数据，减少计费，给运营公司的利益带来损害[1]。据相关新闻报道，2018年8月郑州某黑客通过用笔记本连接万达的KFC、星巴克等店内WiFi，掌握了后台系统高级权限，利用自己编写好的脚本对电动汽车公司批量发送恶意指令，致使该公司1400个电动汽车充电桩系统服务器不能正常运转，损失严重。

针对上述问题，当前国内外有关CAN协议的安全性研究主要包括：CAN总线异常检测、数据加密传输与认证、防火墙技术、安全框架研究。

在CAN总线异常检测领域，于赫、秦贵和等提出了基于信息熵及消息相对距离的车载CAN总线网络异常检测方法[2]，归纳了目前车载CAN总线潜在的安全漏洞以及可能的攻击手段，该方法可以用于检测车载CAN总线网络的泛洪、重放等攻击。张子键，张越等分析了已有的应用于CAN总线的异常检测系统[3]，提出了一种新型的CAN总线异常检测算法，能够检测总线中的异常帧，并设计了能够接入CAN总线的异常检测系统，同时该系统可以验证所提算法的有效性。吴玲云等提出了一种基于随机森林模型的CAN总线报文异常检测方法[4]，首先用采集的大量正常和异常报文数据构造随机森林模型,并进行一系列的参数调整;然后将待检测的CAN总线报文输入到对应ID的随机森林模型中;最后通过模型完成报文正常或异常的分类。Larson等提出了一种基于安全规则的车载CAN网络网络入侵检测算法[5]，该算法通过提前指定一组安全规则去约束ECU的行为，只要违反了这些规则，则判定为非法ECU行为。

在数据加密传输与安全认证方面，赵兵、岑炜等采用国密SM1加密算法，增加了安全存储单元，设计了一种具有安全防护功能的电动汽车充电桩控制策略，可以防止数据在通信过程中被非法截获或篡改，保证了数据传输的完整性和机密性[6]。赵翔、刘志红等采用嵌入式系统，改进了一次一密的加密方式，采用密钥池技术简化加密算法，加大了电动汽车充电数据的破解难度[7]。高德欣、梁珂通过采用SHA1不可逆加密算法将用户信息加密存到数据库、分账户权限管理以及采用DES+RSA算法进行数据传输三方面的设计，极大地提高了电动汽车充电桩监控系统数据的安全性[8]。

在防火墙技术研究方面，唐良等针对当前车载网络中面临的信息安全问题设计了一种类似于防火墙功能的车载网关，用来过滤传统以太网的威胁数据包[9]。肖鹏，李媛媛等提出了一种针对车载信息系统安全的防火墙技术，该防火墙能够对进出汽车内外网络之间的通信流量进行实时扫描，并对可疑的数据包进行过滤，一定程度可以避免来自外网的攻击[10]。

在安全框架的研究方面，Li H,Ru Y K等从CAN总线和3G网络出发，分析了电动汽车充电通信网络当前面临的威胁，构建了以防火墙和入侵检测系统为主的电动汽车充电信息安全防护架构[11]。Petit J和Schmidt R等采用了隐私影响评估方法研究了ISO15118标准中关于充电设施充电和支付的隐私保护措施，并设计了基于匿名证书等隐私增强技术的隐私保护系统[12]。Fazouane M和Kopp H等针对ISO15118标准中提到的POPCORN隐私保护协议，概述了验证该协议隐私属性的方法，指出其存在的问题并给出了相应的改进措施[13]。莫飘分析了充电机与站内监控中心以及充电机与电动汽车电池管理系统之间的通信网络，从信息交换安全需求、CAN总线网络安全需求等方面进行通信网络安全需求分析，建立了信息安全评估模型，为后续研究提供了理论依据[14]。

上述4个方面的研究在一定程度上解决了CAN协议的通信安全问题，但是在数据加密传输和安全认证方面，如赵兵、岑伟等提出的国密SM1加密算法，可以防止CAN数据被非法截获或篡改，但是并不能够抵御重放攻击。当前单就重放攻击而言，一般采取的防御方案有：加时间戳、加序列号、加随机数，有时为了抵御其他类型攻击还会与其他加密或身份认证算法结合。陈宇琦针对无线射频识别系统中存在的安全问题，提出了一种基于时间戳的无线射频重放攻击的抵御方案[15]。在电动汽车充电过程中遭到的重放攻击而言，目前研究较多的是如文献[2]提出的异常检测方法用来检测重放攻击，并未给出电动汽车充电CAN总线遭到重放攻击时具体的防御措施。

本文针对当前存在的问题，在使用STM32F767、USB-CAN转换器和PC机实现了有关CAN协议的环回通信以及与PC之间的通信之后，分析CAN协议的安全性，然后用JAVA编写的程序模拟电动汽车的充电过程，进行重放攻击，并通过加随机数有效抵御重放攻击，有效保证电动汽车充电通信过程的信息安全。

1 问题分析

1.1 CAN总线系统结构

CAN总线系统一般由4部分构成：CAN控制器、CAN收发器、数据传输终端和数据传输线。CAN总线系统结构如图1所示。

1）CAN控制器，接收控制单元中微处理器发出的数据，处理数据并传给CAN收发器。

2）CAN收发器，将数据传到总线或从总线接收数据给控制器。

3）CAN数据传输终端，是一个电阻，一般为120Ω，可以防止数据在线端被反射。

4）两条CAN数据传输线，双向对数据进行传输，分别称为CAN-H和CAN-L，两条线电位相反，但始终保持电压总和为一常数，可以免受外界电磁干扰，对外也无辐射。

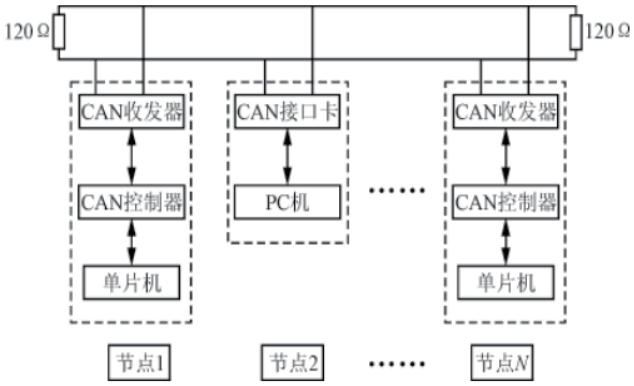


图1 CAN总线系统结构

Fig. 1 CAN bus system structure

1.2 CAN协议数据结构分析

CAN设备以封包的形式在CAN网络上传输数据，这些封包称为帧，也称作消息。CAN帧指完整的CAN传输单元，包含仲裁ID、数据字节、确认位等。一个CAN帧包含以下元素，如图2所示。

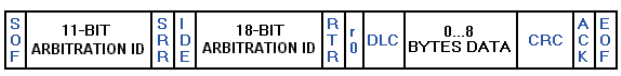


图2 标准CAN帧格式

Fig.2 Standard CAN frame format

1）SOF（帧起始）位：用一个显性位（逻辑0）表示消息开始。

2）仲裁ID：消息的识别码并定义优先级。帧有两种格式，标准格式使用11位的仲裁ID，扩展格式使用29位的仲裁ID。

3）IDE（标识符扩展）位：区分标准帧和扩展帧。

4）RTR（远程传输请求）位：用于区分远程帧和数据帧。用一个显性RTR位（逻辑0）表示数据帧。用一个隐性RTR位（逻辑1）表示远程帧。

5）DLC（数据长度码）：表示数据段包含的字节数量。

6）数据段：包含0~8字节的数据。

7）CRC（循环冗余校验）：包含15位的循环冗余校验码和一个隐性分隔符位。CRC段用于检测错误。

8）ACK（ACK确认）槽：正确接收消息的控制器均会在消息末尾附加一个ACK位发送。传输节点检查总线上的ACK位，如未发现ACK位，则重新发送消息。NI Series 2 CAN接口具有只侦听(listen-only)模式，因此，可以抑制监控硬件所发送的ACK位以避免其影响总线的行为。

9）EOF：帧结束位。

CAN信号指CAN帧数据段中包含的独立数据片段，也可称为通道。由于数据段最多可包含8个字节的数据，因此一个CAN帧可包含0~64个独立信号（如为64个通道，则全为二进制数）。

1.3 CAN协议通信过程

CAN总线是一种串行通信协议，CAN节点发送的数据是以报文的形式广播给网络中所有节点。CAN收发器接收到数据就把数据传送给CAN控制器，再由CAN控制器判断是不是所需数据，不是则忽略。CAN协议在数据链路层处理数据的流程如图3所示。

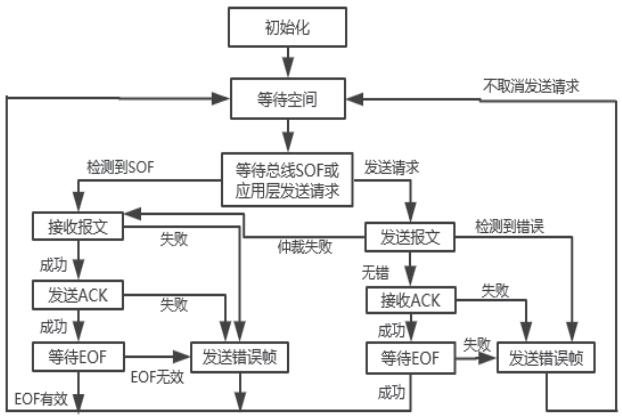


图3 CAN协议在数据链路层处理数据的过程

Fig. 3 The process of CAN protocol processing data in data link layer

1.4　CAN协议安全性分析

CAN协议在刚开始设计的时候，只考虑将几个节点与可靠的网络连接起来，替代之前点对点的通信系统，减少系统布线的重量及复杂性，当时并没有考虑安全性。但是现代汽车可以连接100个节点，最终用户可以轻松访问CAN总线，这就容易引发CAN总线的安全问题，如嗅探，重放，帧伪造和帧注入攻击等各种安全问题。

CAN协议具有的以下特点可能会对电动汽车充电的通信安全造成一定的威胁。

1）CAN总线是没有认证方案的广播协议[16]。因此，接入到CAN总线的所有节点都能接收到其他某个CAN节点发送的数据，数据容易遭到窃听，这就有可能受到重放攻击。攻击者有可能接入到CAN总线，接收充电桩与电动汽车电池管理系统BMS互相通信的报文，然后在任意时间重放到CAN总线网络中，干扰电动汽车正常的充电过程，给用户带来不便。

2）CAN数据缺乏加密功能。CAN协议采用明文传输数据，不包含加密和认证机制，CAN总线中也没有异常检测系统，虽然现在有不少研究者可以通过采取加密和身份认证的方法可以保证CAN数据的完整性和机密性，但是无法同时兼顾到网络的可用性，有可能造成通信开销过高，使可用性变差。

3）CAN总线支持多主工作。连接在CAN总线上的所有CAN节点都具有相同的访问权限，任何一个CAN节点可以在任何时候发送CAN数据帧，但是帧中不包含源地址和目的地址信息，相反，该帧由一个全网唯一的仲裁ID标记。CAN网络上的所有节点均接收到该帧，然后根据该帧的仲裁ID决定是否接受该帧。这就使得某个CAN节点可以伪装成其他CAN节点向CAN总线上发送数据，造成重放攻击。

4）CAN总线仲裁机制。如多个节点在同一时间向CAN总线上发送消息，优先级最高（仲裁ID最低）的节点自动先发送，优先级较低的节点必须等到总线空闲时才可再次发送消息，标识符越小优先级越高。按此方式，即可确保CAN网络中的CAN节点进行确定性的通信。如果某个CAN节点持续发送高优先级的信息，就会造成信道阻塞，影响正常的CAN通信。

由上可知，由于CAN总线的广播特性以及CAN帧中没有包含发送节点的地址信息，使得CAN总线容易受到重放攻击。电动汽车在充电过程中可能遭受重放攻击的环节如图4所示。

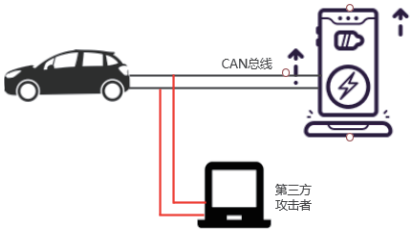


图4 充电过程中遭到重放攻击

Fig.4　Replay attack during charging

第三方攻击者通过非法接入充电桩与电动汽车电池管理系统BMS之间通信的CAN总线，利用CAN总线是采用广播通信的特点，连接到CAN总线上的CAN节点都可以接收到其中一个CAN节点发送的数据帧，攻击者可以向充电桩或电动汽车恶意重复发送之前从CAN总线接收的数据，从而干扰正常的充电过程，给用户带来不便。

2　实验测试与分析

2.1　实验环境

本文以STM32F767单片机为主控芯片，实现CAN数据的收发，可以进行数据的采集和处理，并通过CAN总线实现与PC机的数据互传以及环回模式下的报文自发自收，通信的总体框架大致包括三个部分：PC机、USB-CAN转换器、CAN收发模块电路（本文采用STM32F767单片机）。通过采用CAN总线分析仪可以把PC机接入CAN总线实现数据的收发，并且通过控制界面观察从CAN总线上接收到的数据以及向CAN总线上发送数据。PC机与STM32F767上的CAN模块通信的总体框图如图5所示。

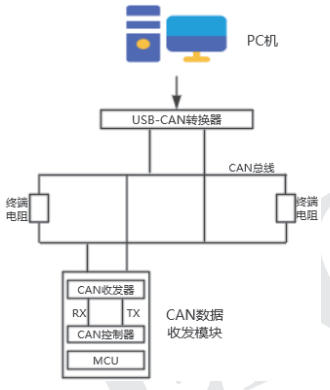


图5　CAN模块通信过程

Fig.5　Process of CAN module communication

本实验硬件设备物理连接情况如图6所示。在完成物理连接之后，在终端电脑上安装并运行串口助手及Embeded Debug v2.0软件。

图6 实验硬件环境搭建

Fig.6 Construction of experimental hardware environment

STM32F767的开发环境采用的是Keil Software公司推出的支持JTAG调试接口的开发工具Keil u Vision5，由于flymcu暂时不支持STM32F767通过串口下载代码，所以只能通过ST_LINK仿真器把编译无误的程序下载到开发板上。本文通过C++编写的程序主要包括3个部分：系统及外设初始化、CAN控制器初始化、数据收发及处理部分[17]。通过按键KEY_UP，可以切换CAN通信的模式——环回模式（Loop Back Mode）和正常模式（Normal Mode），通过串口助手以及Embeded Debug v2.0可以查看CAN数据的发送与接收情况。

本文通过有关CAN协议的环回通信以及与PC之间的通信来验证CAN协议采用明文进行数据传输以及CAN帧中不包含源地址和目的地址信息，只由仲裁ID进行标记。

2.2 环回模式通信

CAN总线的环回模式通信也就是自发自收，bxCAN把发送的报文当做接收的报文并保存在接收邮箱里，并没有把报文送到CAN总线上。通过按下键KEY0，CAN1和CAN2发送数据，通过在串口助手上选择相应的串口并设置波特率为115200，可以在串口助手的界面看到CAN1和CAN2均发送成功，发送的数据如图7所示。

图7 环回模式下发送数据

Fig.7 Send data in loopback mode

2.3 与PC机之间的通信

STM32F767与PC机之间在正常模式下的通信，也就是两个CAN节点之间的通信，开发板和PC机可以向CAN总线上发送和接收数据。但是PC机并不能直接连接到CAN总线上，要通过USB-CAN转换器才能往CAN总线上收发数据。USB-CAN转换器是USB协议和CAN协议的转换网关，也叫PC-CAN，可方便用户在电脑上进行现场数据CAN报文等的记录、分析和监控[18]。USB-CAN转换器内部的CAN总线控制器收到CAN总线上的信号后通过USB接口芯片传给PC机，同样PC机把CAN数据通过USB接口发给转换器内部的CAN总线控制器，再发送到CAN总线上[19]。由于STM32F767只有一个CAN模块连接到了CAN总线上，因此只有一个CAN模块可以从CAN总线上收发数据，选择好相应的端口号以及设置波特率为115200，再通过上位机软件Embeded Debug v2.0实现CAN数据的收发。

通过设置发送数据的ID，8位数据以及帧的类型，可以完成PC机向开发板的通信，如图8所示。

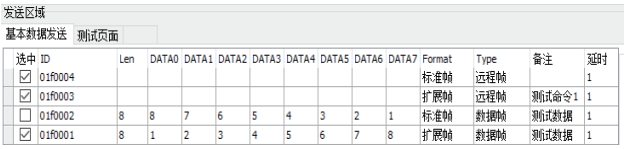


图8 PC机发送CAN数据

Fig.8 PC sends CAN data

通过按键KEY0,可以由开发板向PC机发送ID为0X012的8位标准CAN数据帧，如图9所示。

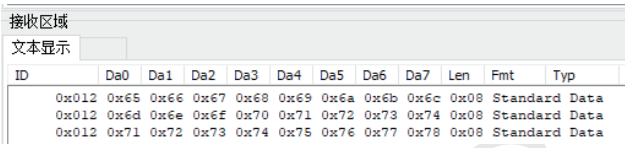


图9 PC机接收CAN数据

Fig.9 PC receives CAN data

通过对比报文传输界面可以发现，CAN协议确实是通过明文进行数据传输，没有进行任何加密，并且CAN帧中不包含源地址与目的地址，容易遭到重放攻击。

3 抗重放攻击算法

3.1　重放攻击

重放攻击（Replay Attacks），又称重播攻击、回放攻击或新鲜性攻击（Freshness Attacks），是指攻击者利用监听或其他方式盗取客户端发送给服务器的数据包，然后不断恶意或欺诈性地将盗取的数据再次原封不动地重复发送给服务器，重放攻击可以由数据发送者进行，也可以由第三方攻击者恶意拦截并重复发送[15]。由于重放攻击并不需要知道监听的信息是什么，只要做到重复发送该数据就可以了，所以一般采用的加密和身份认证只能防止数据被监听，以及保证用户的权限，并不能防御重放攻击。电动汽车充电过程中遭到重放攻击的过程如图10所示。

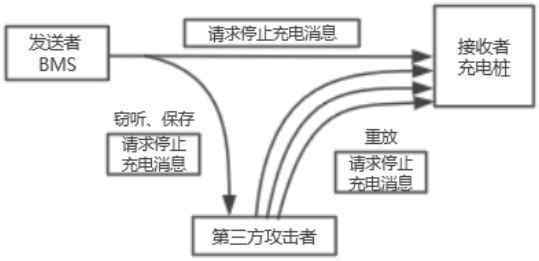


图10 重放攻击过程

Fig.10 Replay attack

3.2　加随机数防御重放攻击的算法

目前大多学者研究的是电动汽车电池管理系统BMS与充电桩之间的数据加密传输和身份认证，但是对数据进行加密，是防止数据被监听攻击，重点在于数据的安全保密性，身份认证是用来判断某个身份的真实性，确认身份后才可以根据不同的身份给予不同的权限，重点在用户的真实性，两种防御措施都不能够抵御重放攻击。本文提出了加随机数防御重放攻击的算法，其详细步骤如下。

1）设置随机数更新规则。本文采取JAVA中的new Random()函数产生随机数，该规则可以为不同的消息设置不同的随机数，使消息请求的随机数都具有新鲜性。

2）发送方与接收方进行消息的互相传输时，预先为消息建立对应的随机数。

3）发送方在传输数据时将产生的随机数一起传给接收方。

4）接收方在收到消息和随机数后，在自己的数据库中检测该消息请求的随机数是否出现过，如果检测到该随机数与之前某次发送数据所携带的数据重复，则可以认为遭到了重放攻击[20]。

5）同时接收方为每次接收到的随机数建立相应的索引并将其储存在数据库中。

加随机数抵御重放攻击算法流程图如图11所示。

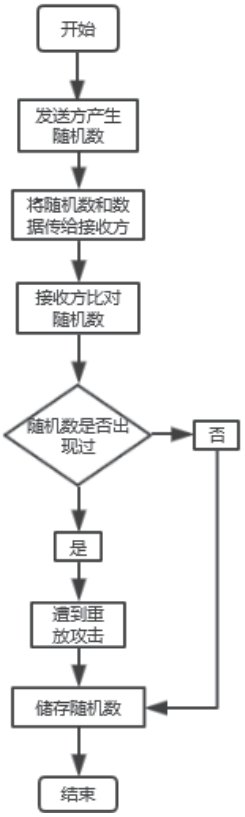


图11 算法流程图

Fig.11 Algorithm flow chart

3.3　实验分析

本实验以加随机数抵御重放攻击的算法为基础，在Windows10操作系统中，使用Eclipse Java 2018进行编程。模拟的电动汽车充电过程中的3种模式可供用户选择，如图12所示。

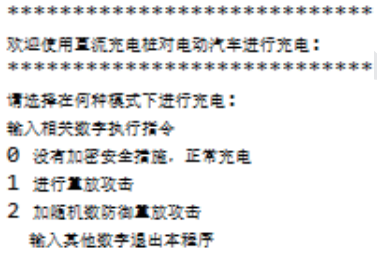


图12 三种充电模式

Fig.12 Three charging modes

3种情况下的实验结果与分析如下。

1）正常充电模式。

电动汽车正常的充电流程包括6个阶段，分别为：物理连接完成、低压辅助上电、充电握手阶段、充电参数配置阶段、充电阶段和充电结束阶段[21]。本文通过JAVA编写的程序模拟电动车充电的过程，当输入“0”时，进入电动汽车正常充电的模式，如图13所示，通过对CAN帧的分析，主要通过充电桩发给电动汽车电池管理系统BMS报文中的电压值的变化来体现整个充电过程的变化。

```
0
您输入了正确的充电指令
您选择的模式已经被设置
已检测到物理连接已经完成
直流充电桩和电动汽车建立充电握手，正在通信
收到帧ID:1804Ca7D,  数据：AB 03 00 7d 00 59 12 00
通过对第1和第2字节数据分析得：总电压93.9V
通过对第3和第4字节数据分析得：电流为0A
电池没有进行充电或放电.
通过对第6和第7字节数据分析得：在1号箱得到最高的电池电压为6.01V
开始充电
电压增加到5
电压增加到10
电压增加到15
电压增加到20
电压增加到25
电压增加到30
电压增加到35
电压增加到40
电压增加到45
电压增加到50
电压下降40
电压下降30
电压下降20
电压增加到25
电压下降15
电压下降5
电压下降0
充电状态设置为STOP
警告！！！充电停止，程序异常退出！！！
充电桩未收到电动汽车报文
充电异常终止
充电结束，祝您生活愉快！
```

图13 正常充电模式

Fig.13 Normal charging mode

2）重放攻击。

在本实验模拟攻击过程中，当充电桩给电动汽车发送的报文显示当前电压为45V时，实施重放攻击，即由第三方不断向充电桩发送一个之前由电动汽车发送给充电桩停止充电的消息，迫使电动汽车停止充电，攻击结果如图14所示。

```
1
您输入了正确的充电指令
您选择的模式已经被设置
已检测到物理连接已经完成
直流充电桩和电动汽车建立充电握手，正在通信
收到帧ID:18047eC3,  数据：CC 03 00 7d 00 F1 12 00
通过对第1和第2字节数据分析得：总电压97.2V
通过对第3和第4字节数据分析得：电流为0A
电池没有进行充电或放电.
通过对第6和第7字节数据分析得：在1号箱得到最高的电池电压为7.53V
开始充电
电压增加到5
电压增加到10
电压增加到15
电压增加到20
电压增加到25
电压增加到30
电压增加到35
电压增加到40
电压增加到45
在没有任何安全措施的情况下执行攻击
异常发生
重放攻击成功，充电停止！
```

图14 重放攻击模式

Fig.14 Replay attack mode

实验结果表明，当电动汽车在充电过程中遭到重放攻击时，充电过程停止，正常充电过程受到干扰。

3）加随机数抵御重放攻击。

将加随机数抵御重放攻击的算法应用到本实验后，在每次充电桩与电动汽车电池管理系统BMS进行CAN数据传输都加上随机数，在电压达到40V的时候进行重放攻击，输入数字“2”时候的实验结果如图15所示。

```
2
您输入了正确的充电指令
您选择的模式已经被设置
已检测到物理连接已经完成
直流充电桩和电动汽车建立充电握手，正在通信
收到帧ID:18047A1B,  数据：29 03 00 7d 00 78 12 00
通过对第1和第2字节数据分析得：总电压80.9V
通过对第3和第4字节数据分析得：电流为0A
电池没有进行充电或放电.
通过对第6和第7字节数据分析得：在1号箱得到最高的电池电压为6.32V
电动汽车已经与直流充电桩进行通信！
开始充电
电压增加到5
电压增加到10
电压增加到15
电压增加到20
电压增加到25
电压增加到30
电压增加到35
电压增加到40
现在开始执行重放攻击
重放攻击失败！
```

图15 抵御重放攻击模式

Fig.15 Mode of resisting replay attack

该实验结果表明，在BMS发送给充电桩的消息请求中加入随机数，如果该随机数与数据库中之前存储的随机数重复，则可以判定为重放攻击，充电桩不执行攻击者发出的停止充电命令，保证充电过程的安全进行。

通过分析与对比以上3个实验结果可以得出，采用加随机数可以有效抵御重放攻击，保证电动汽车充电过程中的信息安全。

3.4　进一步工作

所提出的抗重放攻击算法的局限性主要体现在以下两个方面。

1）虽然不要求时间同步，并且可以有效抵御重放攻击，但是需要额外保存使用过的随机数，会增加数据库保存开销。

2）对每次的消息请求都要查询数据库，会导致算法运行效率偏低。

基于以上分析，下一步工作的重点是研究如何提高算法的效率，减少保存和查询开销，提高算法在传输数据时的可用性，并且针对实际的电动汽车充电系统进行优化测试。

4　结论

本文通过用STM32F767、USB-CAN转换器和PC机搭建实验硬件环境，实现了CAN协议有关的环回通信以及与PC之间的通信，通过通信结果分析CAN协议目前存在的安全性问题；针对典型的重放攻击，本文提出采用加随机数的算法进行防御，并将根据该算法编写的相应程序部署于电动汽车充电充电的通信过程中，通过实验验证了抗重放攻击有效性，为CAN协议通信提供更安全可信的环境，增加了电动汽车充电过程中的信息安全性。

参考文献

[1] 张宝军.分布式电动汽车充电桩信息安全防护技术研究与实现[D].哈尔滨：哈尔滨工业大学，2018.

[2] 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，2016，46(4)：1246-1253.
Yu He, Qin Guihe, Sun Minghui et al .Cyber security and anomaly detection method for in-vehicle CAN[J].Journal of Jilin University,2016,46(4):1246-1235(in Chinese).

[3] 张子键，张越，王剑.一种应用于CAN总线的异常检测系统[J].信息安全与通信保密，2015，(8)：92-96.
Zhang Zijian, zhang Yue,Wang Jian. An anomaly detection system applied to CAN bus[J].Information Security and Communications Privacy,2015,(8):92-96(in Chinese).

[4] 吴玲云，秦贵和，于赫.基于随机森林的车载CAN总线异常检测方法[J].吉林大学学报，2018，56(3)：663-668.
Wu Lingyun, Qin Guihe, Yu he. Anomaly detection method for in-vehicle CAN bus based on random forest[J].Journal of Jilin University,2018,56(3):663-668(in Chinese).

[5] Larson U E, Nilsson D K,Jonsson E An approach to specification-based attack detection for in-vehicle networks[C]//Intelligent Vehicles Symposium, Eindhoven,2008:220-225.

[6] 赵兵，岑伟，翟峰，等. 具有安全防护功能的电动汽车充电桩控制装置[J]. 电器与能效管理技术，2013，(16)：53-57.
Zhao Bing, Cen Wei, Zhai Feng, et al. Electric vehicle charging pile control device with safety protection function[J]. Electrical & Energy Management Technology,2013(16):53-57(in Chine se).

[7] 赵翔，刘志红，陈瞿明，等.电动汽车充电设施数据通信安全策略[J].电力系统自动化，2011，35（9）：92-94.
Zhao Xiang, Liu Zhihong, Chen Quming, et al. Data communication security strategy for electric vehicle charging facilities[J].Automation of Electric Power Systems,2011,35(9):92-94(in Chinese).

[8] 高德欣，梁珂.电动汽车充电桩移动监控系统信息安全设计[J].信息技术，2018（11）：44-48.
Gao Dexin, Liang Ke. A design for information security of electric vehicle charging pile mobile monitoring system[J]. Information Technology,2018(11):44-48(in Chinese).

[9] 唐良，李逸瀚，石春等.电动汽车信息安全网关的设计与实现[J].计算机应用于软件，2017,34（3）：277-283.
Tang Liang, Li Yihan, Shi Chun, et al. Design and Implement of information security gateway for electric vehicle[J]. Computer Applications and Software,2017,34(3):277-283(in Chinese).

[10] 肖鹏，李媛媛，李晓红.车载MOST网络防火墙的设计与实现[J].微计算机信息，2009,（21）：60-62.
Xiao Peng, Li Yuanyuan, LI Xiaohong. Design and implementation of firewall based on MOST[J].Microcomputer Information,2009,(21): 60-62(in Chinese).

[11] Li H,Ru Y Q,Li Y K, et al.Information Security Protection Design of Electric Vehicles Charging Station[J].Applied Mechanics & Materials, 2015, 741:681-686.

[12] Höfer C, Petit J,Schmidt R, et al.POPCORN: Privacy-Preserving Charging for Emobility[C]. ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles. ACM, 2013:37-48.

[13] Fazouaue M, Kopp H, Heijden R W V D, et al. Formal Verification of Privacy Properties in Electrical Vehicle Charging[M].Engineering Secure Software and Systems.

Springer International Publishing, 2015:17-33.

[14] 莫飘. 电动汽车充电站信息安全问题的研究[D]. 北京：华北电力大学，2012：44-45.

[15] 陈宇琦.一种基于时间戳的无线射频重放攻击抵御方案[J].现代计算机，2012，（3）：24-25.
Chen Yuqi.A solution of RFID against replay attacks based on timestamp[J].Modern Computer,2012(3):24-25(in Chinese).

[16] 张悠熠，朱元.车载CAN总线安全验证机制及性能检测[J].信息通信，2018（8）：15-17.
Zhang Youyi, Zhu Yuan, et al. Safety verification mechanism and performance detection of car CAN bus[J].Information & Communications,2018(8):15-17(in Chinese).

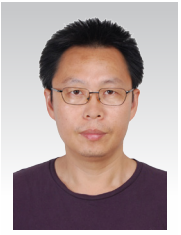
[17] 刘义平，公飞.基于STM32的CAN总线接口设计与实现[J].信息与电脑，2016（8）：154-157.
Liu Yiping, Gong Fei. Design and implementation of CAN bus interface based on STM32[J].China Computer & Communication,2016(8):154-157(in Chinese).

[18] 岳彬彬，李向阳.基于CotexM3 的 USB-CAN转换器开发[J].计算机工程与科学，2012,34（5）：68-72.
Yue Binbin, Li Xiangyang. Development of the USB-CAN converter based on CotexM3[J].Computer Engineering & Science,2012,34(5):68-72(in Chinese).

[19] 石磊，王学林，陈慧，等.USB-CAN总线通信协议转换器[J].自动化技术与应用，2004，23（6）：34-36.
Shi Lei, Wang Xuelin, Chen Hui, et al. Communication protocol convertor for USB-CAN bus[J].Techniques of Automation and Applications,2004,23(6):34-36(in Chinese).

[20] 肖斌斌，徐雨明.基于双重验证的抗重放攻击方案[J].计算机工程，2017,43（5）：115-125.
Xiao Binbin, Xu Yuming. Scheme of anti-replay attacks based on two-factor authentication[J].Computer Engineering,2017,43（5）：115-125(in Chinese).

[21] GB/T 27930-2015，电动汽车非车载传导式充电机与电池管理系统之间的通信协议[S].



王勇

作者简介：

王勇（1973），男，教授，研究方向为能源互联网信息安全，E-mail：wy616@126.com。

李亚菲(1995)，女，研究生，研究方向为电动汽车充电信息安全，E-mail:1156668369@qq.com。

吴旻（1996），男，本科，专业方向信息安全，E-mail:617926771@qq.com。

陈雪鸿（1976），高工，研究方向为工业互联网信息安全，E-mail:504531816@qq.com。

刘丽丽（1979），女，高级工程师，研究方向为多能互补分布式能源系统控制策略研究。E-mail:lili-liu@chder.com。

（责任编辑 张鹏）