北京航空航天大學
BEIHANG UNIVERSITY

第二十六届“冯如杯”学生学术科技作品竞赛
项目论文

针对车载信息系统的攻击渗透与防御技术

2016 年 4 月

摘要

安全性能是汽车在设计和使用的过程中人们最关注的性能之一。汽车最早在 1886 年被发明，至今已经是一种较为成熟的工业产品。现今投入使用的大部分汽车已经具备了足够的物理稳定性和安全性。然而，随着近几年来以车联网和无人驾驶为代表的智能汽车技术的快速发展，人们意识到汽车也将作为一种新的终端而接入互联网。在此趋势下，与汽车相关的信息安全问题开始受到研究者的重视，成为了一个较新的热门研究方向。

本项目对普遍应用的汽车内控制器局域网总线（Controller Area Network Bus，以下简称 “CAN-BUS”）进行研究，尝试寻找其在通信过程和协议设计方面存在的安全漏洞。更进一步，我们尝试针对发现的安全问题提出相应的解决方案。

本项目分两个阶段进行。第一阶段从渗透攻击的角度切入，探索针对汽车 CAN-BUS 信息安全漏洞的攻击和渗透方式，同时收集总线数据流样本。第二阶段，我们对先前采集的数据样本进行特征分析，结合分析结果建立对应车型的 CAN-BUS 数据流特征模型，再基于模型，提出特定情况下 CAN-BUS 异常状态的检测方法，最后我们编写了检测和预警应用程序的原型。

关键词：CAN 总线，信息安全，智能汽车

Abstract

The security performance of vehicles is one of the most important considerations that both drivers and engineers care about. The first vehicle was invented in 1886, up to now it has been a complete product that could adapt to almost all of application scenarios with its high physical stability. However, with intelligent car techniques keeping improving recent years, there are many defects of car's information system discovered. Through these defects, it's not difficult to hack a car and get some control authorities of the car, which certainly put cars into an unsafe situation. Therefore, vehicles are no longer safe enough especially when facing the internet.

This project focuses on Controller Area Network (CAN-BUS) and its communication protocol which are normally used in vehicles.

Our project can be divided into two stages. The first stage begins with a series experiments that trying to control a specific car by information injection. In this way we confirm the existence of potential security defects of CAN-BUS. The second stage contains statistics and analysis work. Basing on the result we build a prototype of a risk detection system, which could warn the driver if the car was attacked by CAN-BUS data injection.

Keywords: CAN-BUS, Information Security, Intelligent Automobile

目录

图表目录

一、引言

（一）项目背景

目前，电子控制单元（Electronic Controller Units，以下简称“ECU”）被广泛应用以参与汽车各项功能的实现和控制。ECU 通常由传感器和控制器两部分组成，而控制器部分通过与车内控制器局域网总线（Controller Area Network Bus，以下简称“CAN-BUS”）连接进而实现通信协作。一辆普通轿车的信息系统通常可能包含有数个至数十个 ECU，ECU 之间通过 CAN-BUS 交换的信息内容能涉及到诸多关键的汽车状态，包括实时运动参数、发动机参数及驾驶操作动作等。

另一方面，车载诊断系统（On-board Diagnostics，OBD）是一套用于读取汽车状态信息进而帮助检修诊断的协议标准，其自 1996 年在美国发布推广开始，到目前为止已被全球大多数汽车厂商所接受，它们汽车产品都会配备 OBD 诊断接口。OBD 标准选择了 CAN-BUS 作为汽车状态信息来源之一，其物理接口与 CAN-BUS 直接相连，因此使用一些特定的设备就有可能从 OBD 接口对 CAN-BUS 进行监听。与此同时，通过 OBD 接口也能向 CAN-BUS 写入信息。

由于智能汽车及相关技术的发展，汽车接入互联网将成为必然趋势。而沿用上世纪 80 年代设计的 CAN-BUS 及其通信协议缺乏在信息安全方面的考虑，因而暴露于混杂的互联网环境下的汽车将面临风险，潜在的安全漏洞可能成为引起严重事故的导火索。2015 年 7 月 24 日，菲亚特克莱斯勒美国公司宣布召回约 140 万辆存在软件漏洞的汽车，成为全球首例因黑客风险而召回汽车的事件。紧接着在 2015 年 8 月召开的黑客大会（Black Hat and Defcon）上，两位安全研究人员 Charlie Miller 和 Chris Valasek 演示了远程入侵汽车的网络系统的方法[1]。已经有事实证明了汽车信息安全问题的严重性。

本项目主要分两阶段进行。第一阶段我们分析了部分相关资料[1]，自行设计并进行了一系列针对特定车型汽车的信息注入攻击实验，从而验证了汽车 CAN-BUS 被注入攻击的可能性，进而分析出 CAN 通信协议在设计上存在的安全缺陷。第二阶段主要对 CAN-BUS 数据流进行统计分析，我们对丰田系列的部分汽车建立了特征模型，并编写了基于数据特征模型的风险检测程序。

（二）项目创新点

本项目的创新点在于：

1、自行设计实验，并通过实验验证和指出了汽车 CAN-BUS 的安全漏洞；

2、对现的安全漏洞进行分析，针对性地提出检测方式，并编写了可视化的监测程序；

3、结合车联网与无人驾驶技术的发展趋势，关注汽车信息安全，具有一定的探索性和前瞻性。

二、汽车总线注入攻击验证实验

（一）实验原理

对于现代汽车，电子控制单元（ECU）及连接多个 ECU 的控制器局域网络（CAN）组成了汽车电子控制系统中最重要的一部分。通过 CAN-BUS 传递的数据主要包含汽车各部件的实时状态汇报，而仪表组、防抱死制动系统（ABS）、雷达辅助泊车等辅助驾驶系统的正常工作往往需要依赖于 CAN-BUS 传来的汽车状态信息。

CAN 协议是一种数据链路层协议，遵照 ISO-11898 系列标准，CAN 标准数据帧的格式如下[2]：

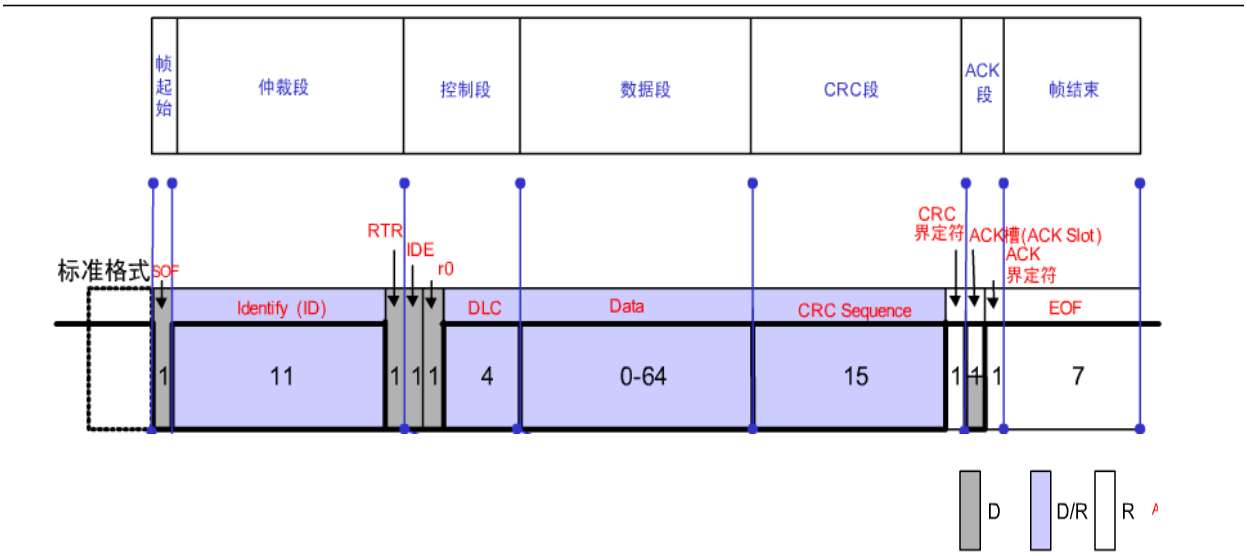

图 1 CAN 协议-标准帧格式

我们关注的字段为 ID（11bit）和 Data（1-8 Byte）。ID 具有标识作用，同时也作为链路层的碰撞优先级，Data 为封装的应用层协议内容。其余字段作用仅是实现链路层的通信，在实验过程中无需人为控制。

CAN-BUS 采用简单的总线型拓扑结构，报文以广播形式发送到总线上。在介质访问控制方面，CAN-BUS 使用总线控制器进行仲裁。生碰撞时，仲裁的原则总是允许高优先级的帧通过，丢弃低优先级的帧。以帧 ID 的值为判定依据，值越小则优先级越高。ECU 在工作时持续监听总线，对接收到的帧依据控制器中的实现写好的固件程序对 ID 进行识别，从而决定是否接受或丢弃。

通过实验，我们发现了以下两点 CAN-BUS 存在的安全漏洞：

（1）CAN-BUS 没有硬件地址的设计，所有的报文均直接广播到总线上。这导致无法通过截获的报文追查和验证信息来源，也无法根据硬件地址对接入总线的设备进行筛查。

CAN-BUS 缺乏来源目的地址导致的结果是任何接入 CAN-BUS 的设备均可发送伪造的数据帧，且只要内容适当，伪造帧与真实帧并无区别，而且发送者无法被追踪。这造成了使用伪造帧冲洗、替换真实帧成为可能。对比 Internet 采用的以太网协议，其因为应用 MAC 地址（介质访问控制子层，Media Access Control，MAC）而加强了安全性。

（2）CAN-BUS 总线控制器所采用的仲裁规则过于简单，使得高优先级的帧总能成功抢占到总线资源。

由此导致的结果是，如果有大量高优先级（ID 字段值较小，极端情况如 0x000）的数据帧以一定的频率被发送至总线，将会导致总线被持续占据，而其他 ID 的帧将无法发送成功。对于汽车，总线若被大量无效帧阻塞，ECU 将难以接收到正常用以维持工作的数据帧，持续一段时间后将会引发故障。

以上两点 CAN-BUS 及其通信协议的设计缺陷使得车载信息控制系统变得十分脆弱，当漏洞被外人恶意利用并实施攻击时，汽车的行车安全无法得到保障。

针对总线仲裁机制的攻击相对简单，但在尝试进行伪造帧注入攻击之前，需要事先通过读取到的信息分析出 Data 字段内各字节数据所对应的实际含义。原因是报文中 Data 字段的内容及其含义最初由汽车设计者，即厂商所定义，资料不对外公开。我们无法直接得知 Data 字段内容含义，因此仅能通过实验和测试以破译。在此简单介绍破译所使用的方法：

我们使用的基本方法是锁定某一 ID，尽可能掌握其正常情况下的数据变化规律，例如对于丰田 RAV4 车型，ID 为 0x0B4 的数据帧的内容形式如下：

0x 0B4 | 00 00 00 00 XX 00 00 YY

图 2 丰田 RAV4 CAN 报文实例

经统计分析可知，ID-0x0B4 帧的前 4 字节及第 6、7 字节保持不变，第 5（XX）和第 8（YY）字节内容在一定时间内处于变化状态。我们在实验时使用设备以一定规

模和略高于正常水平的频率发送 0x 0B4 帧，分别对于 XX 和 YY 两个字节，使其取值从 FF 开始向 00 递减，并持续观察汽车是否发生行为变化，通过多次试验最终我们发现第 5 Byte 的数据内容直接关系到车速表指示值。

通过上述方法可以快速定位一些对应于容易被观察到的汽车参数的数据帧内容，比如仪表盘示数、车身部件开关等。但对于大多数其他内容（主要是涉及汽车运动状况和发动机参数的部分），其数据帧的变化行为较为复杂，现象不易监测，破译工作十分困难。

（二）实验内容

我们的实验利用 OBD 接口为媒介，向 CAN-BUS 发送信息，测试了 2 种注入途径。

第一种主要设备是个人电脑和 USB-CAN 分析仪。设备之间采用有线连接，通过 OBD 接入 CAN-BUS（但不与 OBD 交互)；

另一种是经由移动终端（iPhone 或 Android 智能手机），配合基于 EML327 的车载蓝牙诊断仪（与 OBD 交互）实现无线注入。

图 3 注入攻击的两种途径

接下来分别详细介绍这两种途径，并列举部分实验结果。

（1）有线连接方式

• 设备和软件：

个人电脑（PC），USB-CAN 分析仪、软件 EcanTools

• 注入流程：

按顺序连接各设备，连接至 OBD 接口，当 PC 端软件配置完成后即可从窗口读取到实时 CAN-BUS 信息流。Ecantools 软件提供信息发送功能，设定帧 ID 和帧内容后，可以以 1ms~1000ms 的间隔发送 CAN 帧。

• 攻击实例分析：（以下实验以丰田凯美瑞为实验对象）

[1] 总线阻塞瘫痪实验

选取发送的 CAN 帧 ID 为 0x000，Data 为 00 00 00 00 00 00 00 00；

发送的时间间隔为 1 毫秒，总发送量为 1000 帧，持续发送；

结果为短暂延迟后可观察到汽车仪表盘几乎完全熄灭，同时可听到警报声。原因是大量 ID-000 的帧抢占了总线，导致仪表盘系统正常显示需要的数据帧无法被收到。

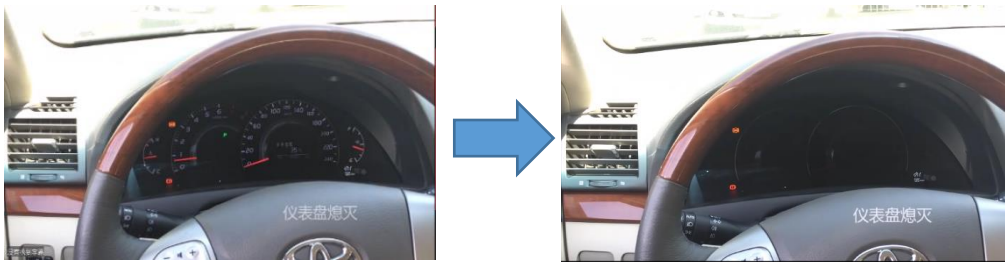

图 4 攻击试验：仪表盘熄灭

[2] 修改仪表显示

在前文中提到过 ID-0B4 的帧，其第 5 字节具有控制仪表车速的作用。

设定 CAN 帧，ID 为 0B4，Data 为 00 00 00 00 FF 00 00 FF；

发送时间间隔为 5 毫秒，总发送量为 2000 帧，持续发送；

图 5 攻击试验：控制车速表

在开始发送后很快可以观察到仪表盘车速表的指针迅速偏转，并在发送结束前一直处于最高速度位置，此行为同时还引发了汽车的超速警报。

（2）无线连接方式

• 设备和软件：

iPhone 或 Android 智能手机，ELM327 车载蓝牙诊断仪、LightBlue Exploer App (或自行编写 APP)

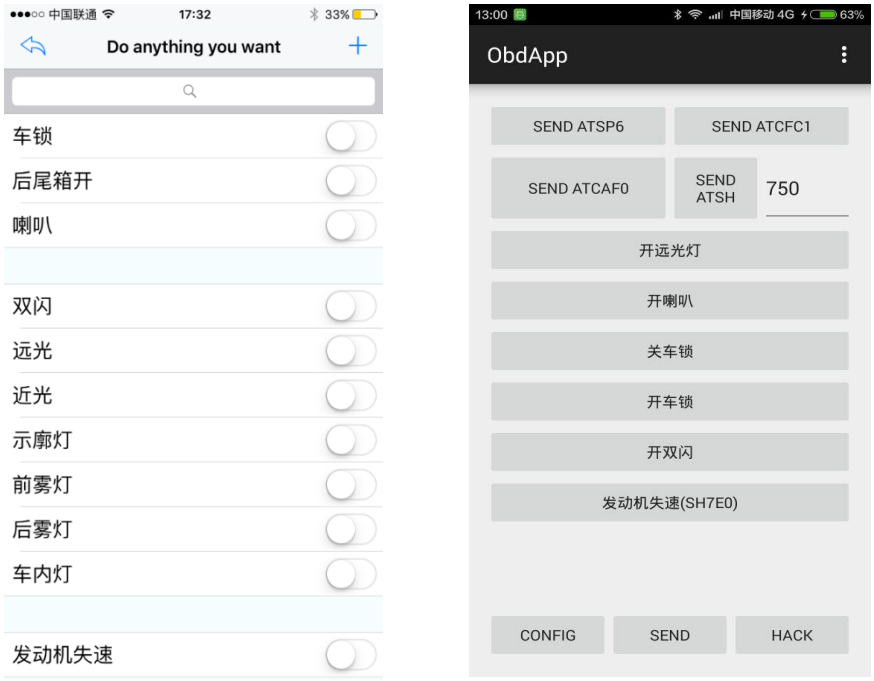

图 6 自行编写的 iOS 和 Android APP 界面

• 注入流程：

先将 EML327 蓝牙诊断仪插在汽车 OBD 接口上（通常情况下接口持续供电，与汽车是否点火无关），之后用手机进行蓝牙配对，配对完成后需使用 APP 对诊断仪进行前的一系列配置设置，配置完成后即可以向诊断仪发送任意内容的 CAN 帧，发送的内容随后即经过 OBD 接口转发进入 CAN-BUS。

• 攻击实例：

利用蓝牙设备从手机端发送特殊 ID 的诊断帧，能产生效果。实验中成功测试了使用诊断帧控制车门锁和车灯组的工作。

（三）实验评估

对比两种不同途径的注入方式，我们发现借助 USB-CAN 分析仪高频率大规模发送 CAN 帧可以轻易使得 CAN-BUS 进入阻塞状态，或者实现特定数据帧的冲洗和替代，但这种方式需要设备之间进行有线连接，并且需要在 PC 端安装专用的驱动程序和配套软件，不方便配置。

相比之下，经由 EML327 蓝牙诊断仪的注入方式设备和配置均较为简单，但蓝牙诊断仪的信息注入过程涉及到与 OBD 接口的交互，由于部分车型的 OBD 接口后设置有网关等安全机制，所以通过这种途径的注入的信息将有可能被网关阻止；另一方面 EML327 蓝牙诊断仪不支持高频率发送数据，因此难于实现总线阻塞攻击或者伪造数据帧。但通过此途径发送的诊断帧仍是有效的，配合无线连接的特点，这一注入途径亦有不小的威胁性。

除了上文中提到的丰田系列的 RAC4 和凯美瑞，我们还对一些其它车型汽车进行过实验，得到结果有所不同，列表如下：

分类	特点	攻击难度	攻击危害	已攻击车型
一类	• OBD诊断座对外暴露CAN总线，易获取车辆状态信息。 • ECU数量少且多用物理线路直连发送控制信息，CAN信息几乎不参与控制，难以利用干扰总线的方式引起异常或故障 • 多见于低端车型	低 不易通过直接注入控制汽车 存在潜在危险性	低	长安悦翔
二类	• OBD诊断座对外暴露CAN总线，易获取车辆状态信息。 • ECU数量较多，仪表、车身及部分动力系统相关ECU单元的较为依赖CAN总线信息 • 大多数中低端车型	低 一旦破译相应车型的交互规则，将取得多方面的控制权限	中	丰田RAV， 凯美瑞， 雪铁龙凯旋， 荣威550
三类	• 在OBD入口处设有网关，访问CAN总线需要适当的应用层协议进行握手 • ECU数量多，许多部件可以被电子控制，如，方向盘，刹车，油门等 • 部分高端车型	相对较高 不易注入，但也并非十分安全	高	奥迪A6L

图 7 不同车型的攻击实验结果

总体看来，虽然因为网关和车内总线布局设计不同等因素，有的汽车具有相对更高的安全性，但所有被试汽车最终仍依赖于 CAN-BUS 作为 ECU 之间的主要通信网络。对于攻击者而言，只要存在能够让外界信息进入 CAN-BUS 的途径，都有可能进一步对汽车行为实施干扰。

上述一系列的实验验证了 CAN-BUS 及 CAN 通信协议存在的两点的安全缺陷：一是无硬件地址，报文的来源目的不可追查验证，二是总线的碰撞仲裁机制过于简单，无法应对阻塞。利用这些缺陷配合信息反向注入极有可能对汽车行为产生较大影响。

当汽车面临互联网时，ECU 将充当媒介沟通外界网络与汽车内部的 CAN-BUS，在此情况下，CAN-BUS 的安全漏洞势必成为汽车安全的巨大隐患。

三、数据分析与威胁检测

（一）CAN-BUS 数据特征

针对实验所暴露出的汽车 CAN-BUS 安全漏洞，本项目的第二阶段着眼于寻求合理有效的威胁检测手段。我们的目标是当汽车 CAN-BUS 受到干扰和注入攻击时，检测机制能够及时发现存在的异常情况并，向驾驶员和乘客发出预警，进而能够避免可能出现的安全事故。

利用 USB-CAN 分析仪，在汽车上读取到的 CAN-BUS 原始信息如下：

index	time	Name	ID	Type	Format	Len	Data
00000001	0.782.210	接收	1E0	DATA	STANDARD	4	00 00 00 00
00000002	837.131.227	接收	0B0	DATA	STANDARD	6	03 58 03 58 11 0C
00000003	0.000.017	接收	0B2	DATA	STANDARD	6	03 55 03 54 11 0C
00000004	0.000.009	接收	235	DATA	STANDARD	4	00 00 00 3B
00000005	0.000.008	接收	320	DATA	STANDARD	3	00 00 26
00000006	0.000.008	接收	260	DATA	STANDARD	8	0E 00 00 00 00 00 00 78
00000007	0.000.008	接收	020	DATA	STANDARD	3	00 00 07
00000008	0.000.011	接收	0B4	DATA	STANDARD	8	00 00 00 00 CD 03 50 DC
00000009	0.000.009	接收	025	DATA	STANDARD	8	00 11 00 0D 78 78 78 B3
0000000A	0.000.008	接收	0BA	DATA	STANDARD	3	06 10 D3
0000000B	0.000.008	接收	024	DATA	STANDARD	8	02 00 02 12 61 FF 80 22
0000000C	0.000.008	接收	2C4	DATA	STANDARD	8	05 E7 00 1A 00 80 33 87
0000000D	0.000.009	接收	2D5	DATA	STANDARD	2	30 85

图 8 CAN-BUS 原始数据

原始数据中主要有效信息为截获时间（相距上一帧的时间间隔，单位：ms）、帧 ID（表示为 3 位十六进制数，实际为右端的 11 个二进制位有效，最左一位应保持为 0）和数据内容 Data（十六进制）。

在实际实验中，我们在汽车的行车状态和停车（未熄火）状态分别记录了数据。选用于分析的样本数据共 4 段，其中属于行车时的数据有 2 段，停车时的有 2 段，每段数据包含 100 000 条 CAN 帧。对数据在 3 个层次上进行分析，说明如下：

（1）对总线网络低层特性的分析

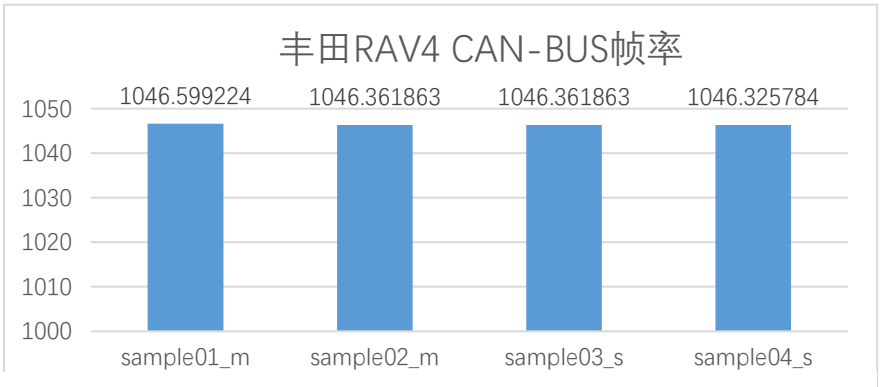

图 9 丰田 RAV4 CAN-BUS 帧流量

我们对 CAN-BUS 在无干扰情况下的数据帧出现频率进行计算，对 4 段数据分别计算，得到结果接近一致。即无论行车或停车，丰田 RAV4 在正常情况下的 CAN-BUS 数据帧流量稳定为约 1046 帧每秒。

（2）对帧 ID 的分析

这一部分的分析从帧 ID 的角度出发，对每一 ID 的数据帧出现单独计数，发现在一定的窗口（总帧数或时间）内，每一 ID 的帧出现次数保持稳定不变。

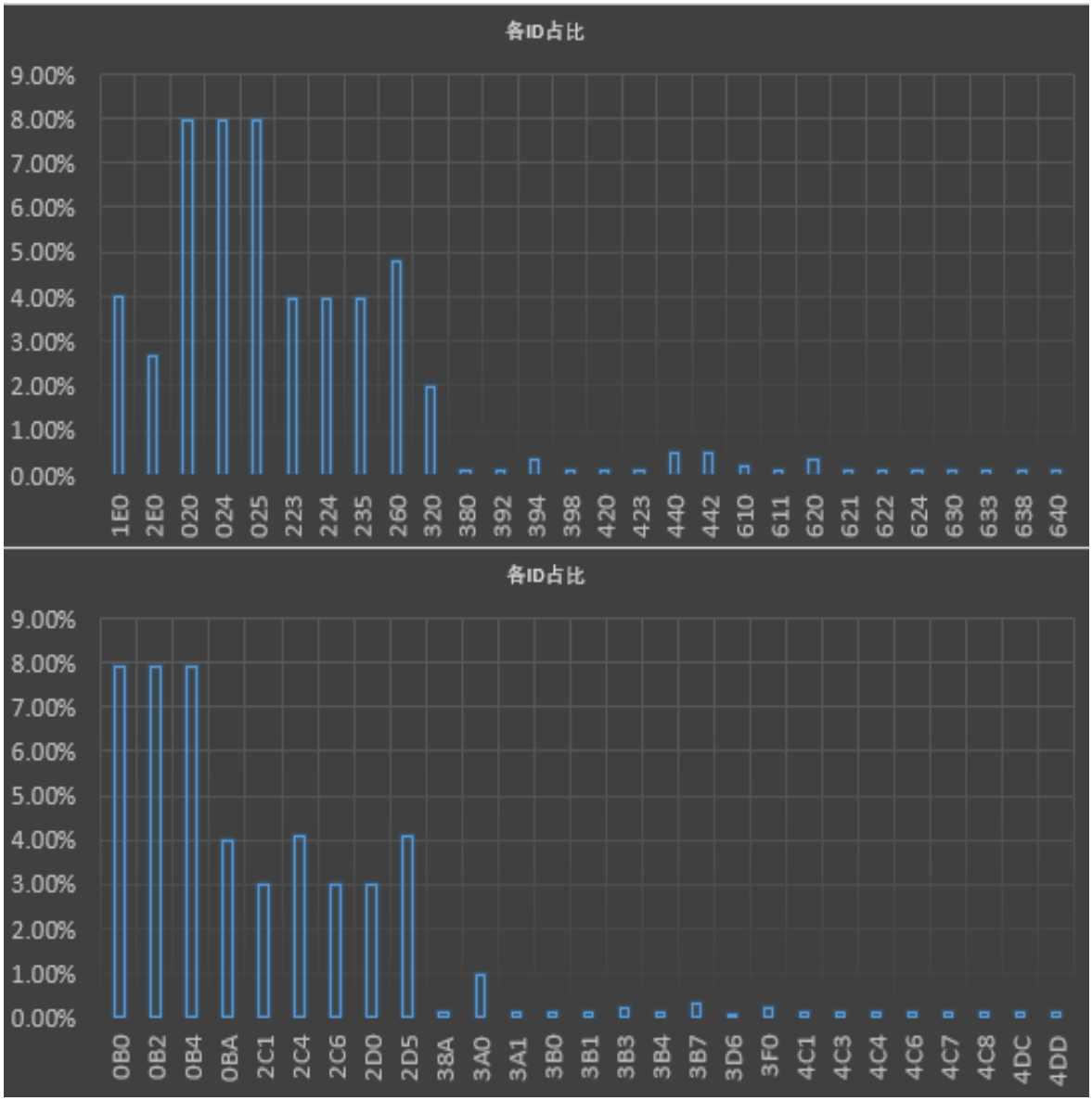

图 10 丰田 RAV4 各 ID 频率（每 10 万帧）

在分析中还能看出，对于丰田 RAV4，其正常状况下 CAN-BUS 上所出现的帧 ID 范围是固定的（55 种），说明在汽车的正常使用过程中，不应该出现其他特殊 ID 的帧（例如 0x7E0 等诊断帧）。

（3）对 Data 字段内容的分析

通过对数据进行初步观察，可以发现 Data 部分的大部分内容并不固定，而是出于变化状态，除了一些明显与汽车的可见行为（仪表示数、车身机构动作）密切相关的内容可以通过实验找出之外，其余大多数内容较难判断其实际含义和对应的功能，所以在对其内容进行分析时我们采取的方法是锁定部分已知内容，即特定 ID 的特定字节值进行监控，分别计算在正常情况下这些字节值的变化情况，建立变化曲线作为模型。

（二）检测方法

经数据特征分析，我们提出了如下检测方法：

对于某一特定车型，需先对其采集一定量正常情况下的 CAN-BUS 信息，利用这些信息对该车型的 CAN-BUS 数据流进行建模，之后的检测工作均通过和已有模型的对比来完成。

对于利用诊断帧实现的控制行为，因为每种诊断帧都具有特殊的 ID 编码，通过对比正常情况下出现的 ID 集合与所读数据即可发现。

对于注入高频高优先级帧引起总线阻塞和注入高频伪造帧替代正常帧这两种攻击方式，其共同特点是需要以较高频率以一定规模注入数据。因此只要对 CAN-BUS 总传输流量及每一 ID 在一定时间内的出现率进行监控，即可侦测到可能的攻击行为。

图 11 数据特征模型-频率

监测程序对每个 ID 计算其在一定时间窗口内的出现频率，与标准模型进行对比，从而判断是否发生此类异常。标准模型包括频率均值和浮动范围，均值为 4 份样本共 40 万条数据帧的平均值，浮动范围由对样本数据的扫描得出，以各 ID 在给定时间窗口内频率出现过的最大值和最小值作为上下界。

（三）监测程序原型

基于上述的数据分析和检测方法，目前我们编写了能用于汽车 CAN-BUS 数据流监测的程序原型，并使用第一阶段实验中所用过的 USB-CAN 分析仪作为数据读取工具。监测系统软件程序部分的主要功能包括：

1、加载事先记录的正常情况下的汽车 CAN-BUS 数据，进行统计分析后建立该车的 CAN-BUS 数据流特征模型；

2、对于录取好的任意一段静态数据，可导入程序进行模拟实时监测，用于程序测试、调试和展示；

各 ID 频率特征是我们的监测程序最主要关注和分析的数据特征。我们分别使用了条形图和灰度图（Grey Level Image）进行可视化处理。

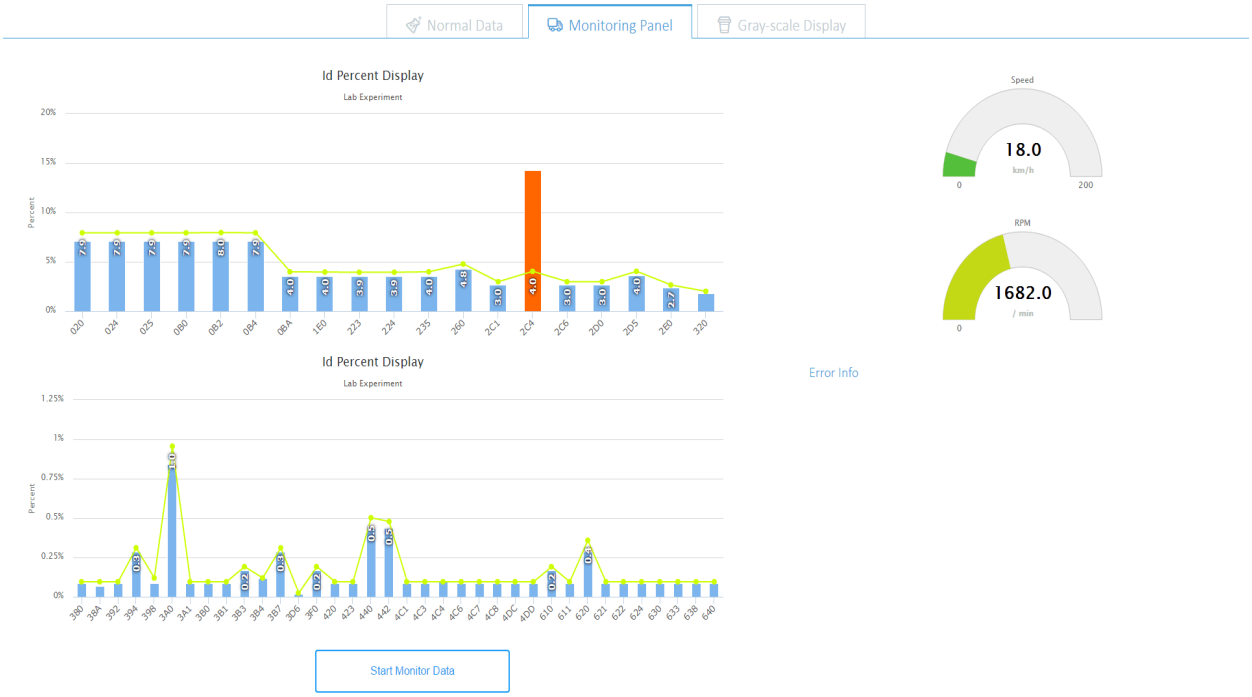

图 12 监测程序−ID 频率条形图

在条形图中，横坐标为各 ID，纵坐标为出现频率，采用的时间窗口宽度为 5s，蓝色的柱状图形表示最近 5s 内的各 ID 的出现频率，绿色的折线为该车型的频率特征模型（由正常数据确定）。上下两张图分别是相对高频出现的 ID 和相对低频出现的 ID，因其的频率数值相差较大，分开绘图以便观察。

图 13 监测程序-ID 频率灰度图

灰度图使用颜色深度表示各 ID 之间相对频率的高低，纵轴为 ID，横轴为时间，图随时间横向增长。正常情况下各条纹颜色深度应当稳定；异常时可观察到异常 ID 的灰色深度出现明显变化。上图中，上下分别为正常和异常情况下的灰度图。

四、后期工作

关于未来的工作，首先应围绕车载控制系统寻找其他可能存在的安全漏洞，我们希望能够发现新的安全漏洞，从而再针对性地提出应对措施。

其次，对于原始数据的分析处理方式，我们将可能尝试使用具有机器学习特性的算法对 CAN-BUS 数据模式进行深度挖掘分析，从而得出更准确有效的总线数据模型。

最后，我们希望能够设计并实现自己的硬件设备，将监测模块软件写入其中，随后可以将该硬件安装到汽车总线上执行工作，安全工作者通过远程通信访问即可获知汽车相关状态。

结论

项目第一阶段，我们对长安悦翔、丰田 RAV4、丰田凯美瑞等车型的汽车进行了一系列实验，实验通过向汽车 CAN-BUS 注入数据而控制部分汽车功能或引起人为故障。根据实验结果我们发现了 CAN-BUS 及 CAN 协议潜在的两点安全漏洞，即协议设计无硬件地址验证和总线的碰撞仲裁机制无法解决阻塞。

立足于第一阶段的结论，我们在第二阶段做了一些数据分析和建模工作，但由于时间和实验用车等因素的限制，目前只对丰田 RAV4 的总线数据流建立了相应的模型。另一方面，监测程序原型编写基本完成，可以根据导入的数据模拟监测过程，并用条形图和灰度图的方式呈现数据变化过程。

综上所述，本项目选取了车载信息系统中具有关键作用的 CAN-BUS 作为切入点，发现其存在的安全漏洞，进而提出了相应的检测方法，并完成了监测程序原型的编写。我们的结论在汽车信息安全这一话题领域下应当具有一定的参考价值。

在车联网、无人驾驶等智能汽车相关技术正在飞速发展的今天，汽车早已不是最初纯粹的机械设备，而是一种电子-机械紧密结合，并因智能化而迈进信息领域的高科技产品。汽车技术的进步和发展离不开多个领域的交叉合作，而信息安全将是这其中不可或缺的一环。

参考文献

[1] Charlie Miller, Chris Valasek, *Adventures in Automotive Networks and Control Units*, 2014

[2] 杨春杰，王曙光，亢红波. CAN 总线技术[M] 北京：北京航空航天大学出版社，2010