# 车载CAN总线网络安全问题及异常检测方法

于 赫[1],秦贵和[1,2],孙铭会[1,2],闫 鑫[3],王璇喆[3]

(1.吉林大学 计算机科学与技术学院,长春 130012;2.吉林大学 符号计算与知识工程教育部重点实验室,长春 130012;3.吉林大学 软件学院,长春 130012)

**摘 要**:在汽车智能化进程加快以及车联网技术快速发展的背景下,分析了车载CAN总线网络安全现状,总结了车载CAN总线网络潜在的安全漏洞,归纳了对车载CAN总线网络的攻击手段,提出了使用信息熵的车载CAN总线网络异常检测方法,并对该方法的有效性进行了实验验证。理论分析及实验结果均表明:使用信息熵的车载CAN总线网络异常检测方法是有效可行的。

**关键词**:计算机应用;CAN总线;异常检测;信息熵;车载网络安全

**中图分类号**:TP393 **文献标志码**:A **文章编号**:1671-5497(2016)04-1246-08

**DOI**:10.13229/j.cnki.jdxbgxb201604034

## Cyber security and anomaly detection method for in-vehicle CAN

YU He[1], QIN Gui-he[1,2], SUN Ming-hui[1,2], YAN Xin[3], WANG Xuan-zhe[3]

(1. *College of Computer Science and Technology, Jilin University, Changchun* 130012, *China*; 2. *Symbol Computation and Knowledge Engineer of Ministry of Education, Jilin University, Changchun* 130012; *China*; 3. *College of Software, Jilin University, Changchun* 130012, *China*)

**Abstract**: With the rapid developments of intelligent vehicle technology and vehicle networking technology, automotive information security issues are facing severe challenges. In this paper, the current situation of in-vehicle CAN cyber security is analyzed, and the potential security vulnerabilities and attacks for In-vehicle CAN bus are summarized. Then, an In-vehicle CAN bus anomaly detection method, which uses information entropy, is proposed. Experiments are carried out to verify the effectiveness of the proposed method. Theoretical analysis and experimental results show that the proposed method is feasible and effective.

**Key words**: computer application; controller area network(CAN) bus; anomaly detection; information entropy; vehicle cyber security

**收稿日期**:2015-09-08.

**基金项目**:吉林省科技发展计划项目(20150204034GX);国家自然科学基金项目(61300145);中国博士后科学基金项目(2014M561294);吉林省科技发展计划青年项目(20150520065JH);吉林省博士后科研项目(RB201364).

**作者简介**:于赫(1982-),女,博士研究生.研究方向:实时网络控制系统,CAN总线安全.
E-mail:he08@mails.jlu.edu.cn

**通信作者**:孙铭会(1983-),男,讲师,博士.研究方向:车载网络安全,人机交互,物联网.E-mail:smh@jlu.edu.cn

在过去 20 年里，CAN（Controller area network）总线网络取代复杂沉重的电缆，成为当今应用最广泛的车载通信网络。现在，几乎所有汽车制造商都采用 CAN 总线实现汽车内部控制系统与各个执行机构的数据通信。在通信技术和网络不发达的时代，车载信息系统是隔离且相对安全的。在此环境下诞生的 CAN 总线网络，控制信息和敏感数据直接广播至网络。随着汽车智能化和网络化进程加快，特别是云技术的广泛应用，汽车信息安全问题面临前所未有的考验。

本文分析了车载网络安全现状，对目前车载 CAN 总线潜在的安全漏洞，以及可能的攻击手段进行了归纳，提出了使用信息熵的车载 CAN 总线网络异常检测方法，使用该方法可以检测车载 CAN 总线洪泛、重放等攻击，并且检测效果良好。

## 1　汽车信息安全问题现状

### 1.1　汽车信息安全隐患

现在的汽车都配有大量电子设备，除了基本的电控、媒体系统，还有智能化的高级辅助驾驶系统，如自动启停、泊车、ACC 系统，更有可与手机等智能设备连接的信息娱乐系统等，这些系统都会从车载 CAN 总线网络获取数据。从智能化发展方向上看，汽车连接互联网将是不可避免的，而这些电子设备、智能信息系统都可能成为黑客入侵汽车网络系统的途径。一旦黑客入侵这些系统并能够成功连接到车内 CAN 总线网络，即意味着驾驶者可能已经丧失了汽车的控制权。著名白帽黑客 Miller 和 Valasek 博士在 2013 黑客大会上发表的白皮书中公开了攻击两款在售车型的全部细节，甚至还包括攻击所用的源代码、编译器及连接件原理图[1]。在 2014 年黑帽大会（Black Hat）上，他们公布了一份对市场上 20 余款车型网络安全性的报告，对不同汽车厂商不同车型抵御恶意攻击的能力进行评估[2]。2015 年黑帽大会，他们将演示通过“0day”漏洞，攻击车载娱乐系统，使用笔记本电脑远程控制一辆 Jeep Cherokee 汽车[3]，这些公开的报告把汽车信息安全问题从边缘推上了前台，以期望引起汽车制造商（OEM）以及研究学者对汽车信息安全问题的关注。

### 1.2　相关研究工作

汽车的信息安全性应该是未来 OEM 在应用新产品、新技术时首要考虑的问题。近年来 OEM 对汽车信息安全的关注度逐年提高，欧盟及美国相关机构也积极资助开展汽车信息安全项目，如欧盟的 SEVECOM[4]、OVERSEE、EVITA 项目等。EVITA 项目旨在设计原型和验证用于车载网络安全组件的系统架构，以保护敏感数据免受篡改[5]。EVITA 标准列出了三个层次的安全规范，其中的 Light HSM 确保 ECU 与传感器、执行器之间的安全交互，Medium HSM 则保障 ECU 间的通信环境安全。虽然 EVITA 定义了车载网络安全系统框架，但是其并不提供具体的安全保障技术。

Groza 等[6-8]针对车载 CAN 总线安全问题进行了多方面的研究工作，提出一系列轻型广播认证协议，如 EPSB、Libra-CAN，并验证了这些协议在 ECU 节点数目比较少的场景下的可用性。Groza 等[9]还通过实验证明在 CAN 总线网络中，根据信号特征识别信息发送节点的可行性，并推荐其可作为一种 CAN 总线网络的入侵检测方法。

Lin 等[10]设计了具有较低通信开销的纯软件 CAN 总线安全机制（IDT&C），其安全策略使用 CAN 消息 ID 表和消息计数器生成消息认证码（MAC）。Schweppe 等[11,12]建议车辆使用 EVITA HSM 的通信安全体系结构，在考虑 CAN 网络数据载荷的基础上，提出使用 32 位 MAC 的安全架构，但没有给出 MAC 的实施细节。

Woo 等[13]通过蓝牙或无线 OBD Ⅱ 诊断设备，远程向车载 CAN 总线网络发送攻击报文信息，给出了一种使用 AES-32 算法的轻量级消息加密方法，并给出该方法与 EPSB、IDT&C 在不同 ECU 数量下运行时间、传输响应时间和总线负载的对比，其在总线 ECU 数量少于 20 个时的总线负载率为 50%。

Lu[14]提出攻击者与系统之间的交互可以建模为一种马尔科夫决策过程（MDP），并建议对 ECU 存储系统进行加密，以防止攻击者对 ECU 代码的嗅探和篡改。

Larson 等[15]提出了一种建立在安全规则基础上的 CAN 总线网络攻击检测方法，该方法基于 CANopen 协议的对象字典，使用协议级的安全规则检测非法 ECU 行为，并提供了一组示例的安全规则。Muter 等[16]给出一种结构化的车载网络异常检测方法，引入一组异常检测传感器对消息帧 ID、数据负载、消息频率等进行检查，并

整合传感器结果以防止误报。

## 2 背景知识

CAN总线的使用依赖于消息帧ID的多主竞争式总线结构,仅使用成对双绞线进行通信,应用最高传输速率可达1 Mbit/s。其消息以广播形式发送至总线上,任一节点可以在任意时刻向网络发送消息报文,报文发送仲裁仅取决于至多29 bit的消息帧ID。

### 2.1 CAN帧格式

CAN总线中,ECU间使用数据帧传输信息,ECU向网络广播具有指定ID的数据报文,网络上的ECU可根据报文ID有选择地接收或者响应该报文。图1为CAN2.0B标准的数据帧格式,CAN2.0B协议兼容标准帧及扩展帧格式的数据报文。

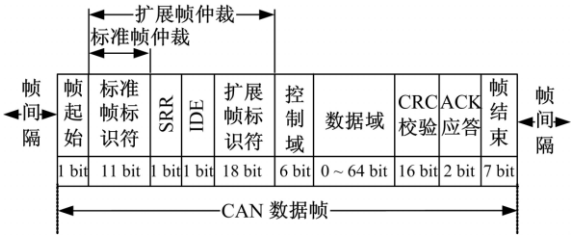


图1 CAN2.0B标准的数据帧格式

Fig. 1 Data frame format of CAN 2.0B Specification

一个CAN数据帧可携带0～8个字节的数据,报文可以使用11 bit标准帧ID或29 bit扩展帧ID,1 bit标识符扩展位IDE指示其是否使用扩展格式,CAN2.0B共定义了4种不用类型的消息报文,其他的是远程帧、错误帧和过载帧[17]。

### 2.2 电气特性

如图2所示,CAN总线仅使用两根信号线CAN高(CAN_H)和CAN低(CAN_L),通过两根信号线的差分电压表示"1"(隐性)和"0"(显性)。当总线同时传送显性和隐性两个值时,总线的结果为显性,即显性位"0"具有优先发送权。

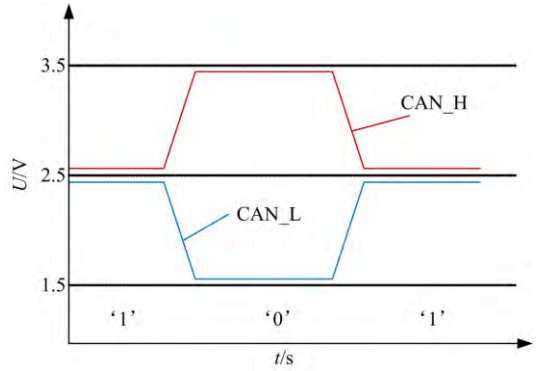


图2 CAN信号

Fig. 2 CAN signal

CAN总线在汽车电缆中很容易找到,CAN总线在空闲时的电压稳定在2.5 V左右,而有数据传输时会上下浮动1 V,约为3.5 V(CAN_H)或1.5 V(CAN_L)。

### 2.3 车载网络结构

一辆汽车通常有20～100个ECU,每个ECU完成特定的功能。这些ECU分布于车辆不同的位置,由几个主要网络连接起来。图3为上海大众09款途观的CAN总线系统结构图。其包含速度为500 kbit/s的动力系统CAN总线;100 kbit/s的车身CAN总线;100 kbit/s的娱乐CAN总线,这3个网络均连接到诊断模块(J533),诊断模块还包含标准OBDⅡ接口,并通过500 kbit/s的CAN总线与仪表板(IC)连接。

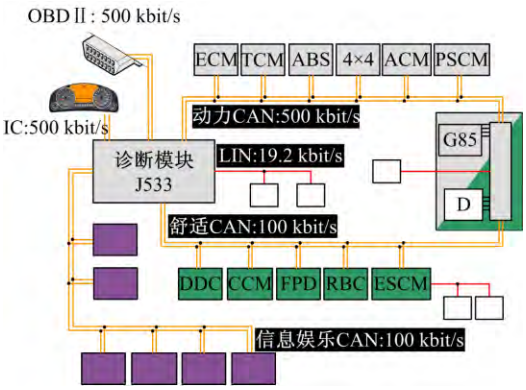


图3 车载CAN总线网络

Fig. 3 In-vehicle CAN bus

## 3 车载CAN总线网络安全问题

### 3.1 目标漏洞

基于上述CAN总线协议定义、电气特性及车载网络结构,结合当前CAN总线网络漏洞研究[18],车载CAN总线安全漏洞主要可归纳为以下几个方面:

(1)缺乏足够的安全保护。目前CAN总线缺乏必要的安全保护,以确保信息的保密性、完整性、可用性、真实性和不可抵赖性。CAN总线上的消息可以被总线上任意节点读取,并且没有任何消息认证码(MAC)或数字签名保护。

(2)弱认证。对ECU进行固件修改时使用口令(Password)等弱认证技术。

(3)CAN协议滥用。拒绝服务攻击(DoS)可

以通过总线仲裁机制进行，如果攻击者使用最高优先级发送数据，那么其他 ECU 将无法使用总线。还有形成恶意的错误帧消息，也可以使 ECU 从总线上断开。

(4)消息泄露。通过常规诊断接口，如 OBD Ⅱ、K 线或 L 线即可掌握车辆运行时的信息。随意使用 OBD 软件也存在潜在的安全隐患，OBD 模块通常会存储访问控制 ECU 的指令。

目前 OBD 应用的安全风险尤其值得关注。OBDⅡ的标准诊断接口中，CAN 总线引脚定义非常明确，黑客很容易找到切入车载 CAN 总线网络的入口。通常汽车制造商会通过登陆密钥、隐瞒接口、请求验证等方式严格限制 OBD 口写入命令，但这些手段仍属于弱认证，并不能保证网络信息的安全性。国内 OBD 应用和车联网方案近年来的发展超出预期，OBD 应用的安全性也受到质疑。这些 OBD 应用的功能从可以实现自动升窗、落锁的简单功能，到可以实时监测车辆信息，分析后通过手机 APP 以图形化的形式展示给驾驶员，甚至直接将车辆信息实时同步到云端存储。而 OBD 应用这种类型的第三方改装设备的安全性不能得到保障，很容易出现软硬件漏洞。

### 3.2　攻击方式

针对车载 CAN 总线网络，攻击者可以丢弃、修改和读取发送至总线上的信息，在源节点和目标节点间进行欺骗攻击，此外还可以进行洪泛、重放攻击。

(1)丢弃(Drop)：可用性攻击。例如一个控制了车载总线中某个网关的入侵者可以删除或不转发某些消息，致使 ECU 一些功能失效。

(2)修改(Modify)：通过入侵或截断总线中某个网关，可以修改从该网关转发的消息。

(3)读取(Read)：任何连接到总线的节点都可以读取总线消息，可以是一个独立的监听装置，也可能是一个被入侵的节点。一旦有密钥或私人信息在总线上发出，就会被入侵者读取。

(4)欺骗(Spoof)：任何被入侵的节点都可以发送错误消息、诊断信息，使总线上 ECU 对事件进行响应，消耗 ECU 的处理器资源。

(5)洪泛(Flood)：入侵者控制任意 ECU 即可向其所在网络发送高速率洪泛消息报文。

(6)重放(Replay)：入侵者控制任意 ECU，任何被记录的消息和消息发起的事件，均可以在任意时间重放到网络中。

### 3.3　应用困难

尽管研究人员在努力尝试保护汽车信息安全，但是其中绝大多数方法并不能立刻应用到实际的车辆当中，主要的障碍有以下几方面：

(1)认证机制推广阻力大。认证协议对 CAN 协议包格式进行了重新定义，这意味着对几乎所有车辆底层系统进行修改，而 OEM 对这种改变十分谨慎。并且大部分的研究显示[8,13]，对 CAN 总线通信进行加密后会产生延时，从而无法满足原有总线的实时需求。

(2)新协议能否被 OEM 采用仍是未知，例如使用 CAN-FD(CAN with flexible data rate)协议进行安全认证的方法[19]，CAN-FD 比传统 CAN 协议拥有更高的传输速率，更小的控制位开销，并且每个数据帧可以携带最多 64 个字节的数据。虽然 CAN-FD 优势明显，但是在 OEM 看来离实际商用的距离还远。

(3)认证协议适用的网络节点数量不能达到实际车辆应用要求。即使使用 16 位处理芯片、轻量 32 位 MAC 的加密协议，其在 CAN 总线上实施的开销仍然巨大，而实际车载 CAN 总线网络不论是节点的数量还是网络复杂度都远远超过实验场景。

(4)新协议在旧车型上的应用问题。由于汽车是一种耐用商品，通常一辆汽车的寿命可以达到几十年，这些车辆在出厂时可能没有信息安全方面的防护装置，而在使用过程中，新的总线协议也许无法应用于这些车辆。因此，需要为这些车辆提供一种尽量少依赖于车型的有效的信息安全保护。

## 4　车载 CAN 总线异常检测方法

车载总线异常检测系统以安全组件的形式实施于车载网关中，实时检测潜在的安全威胁并发出预警，提醒驾驶员进行信息安全检测。尽管高级加密认证和数字签名技术具有更高的安全性，但是考虑到汽车较长的使用寿命，车载网络异常检测系统可能更贴合目前的汽车信息安全需求。

针对异常检测，需要对系统的异常有一个定义，即定义系统的正常行为以确定偏离正常行为的攻击。在信息学领域，熵用来衡量一个系统的不确定性。一个系统越是有序，不确定性越小，信息熵就越低；反之，一个系统越是混乱，信息熵就越高[20]。

将一辆从未被入侵的汽车正常驾驶行为时的总线消息集看作一个系统,由于CAN矩阵的定义,这个系统显然是有序的,系统的信息熵值应当是稳定的。向网络注入新的数据报文,或使某个ECU从网络中断开,又或是启动一个数据重放,这些都会影响CAN总线网络的正常行为。这种变化反映在信息熵中就表现为:引入了新的不确定性,系统的信息熵就会发生变化。

此外,在车载CAN总线中,熵的计算与消息出现的概率有关,不涉及标识符的定义,是一种可以应用于不同车型的通用方法。

### 4.1 信息熵

**定义1** 设系统 $X$,其有限个可能的状态集为 $\{x_1,x_2,\cdots,x_M\}$,则系统 $X$ 的信息熵为:

$$H(X)=\sum_{x\in X}P(x_i)\log\frac{1}{P(x_i)} \tag{1}$$

式中:$P(x_i)$ 为系统 $X$ 在状态 $x_i$ 的概率。

**定义2** 设系统 $X$,其有限个可能的状态集为 $\{x_1,x_2,\cdots,x_M\}$,该系统具有相同状态空间的两组不同概率分布 $P(x)$ 和 $Q(x)$,定义 $P(x)$ 和 $Q(x)$ 间的KL距离(Kullback-Leibler divergence)为:

$$D(P\parallel Q)=\sum_{x\in X}P(x)\log\frac{P(x)}{Q(x)} \tag{2}$$

式中:$P(x)$、$Q(x)$ 为系统 $X$ 在状态 $x_i$ 下的概率分布。

### 4.2 基于信息熵的异常检测

针对CAN总线网络周期确定、消息数量稳定的特点,在理想情况下,即不考虑实际网络中数据发送、优先级仲裁、空白域等的影响,定义CAN网络信息系统及熵的理论分析方法。

系统 $\Omega=(E,C,T)$ 表示一段时间为 $T$ 的CAN总线报文集合,其中 $E=\{\varepsilon_1,\varepsilon_2,\cdots,\varepsilon_n\}$ 为 $T$ 时间内出现的 $n$ 种不同CAN标识符的报文,$C=\{c_1,c_2,\cdots,c_n\}$ 为 $T$ 时间内出现的 $n$ 种不同CAN标识符的报文的发送周期。

#### 4.2.1 CAN总线信息熵

假设CAN网络在时间 $T$ 内的负载适中,所有消息都能在规定时间内发送完成,那么,$T$ 时间内CAN总线消息的数量 $total$ 可以由报文周期和时间长度得到,其熵值计算可以变为如下形式:

$$H(E)=\sum_{\varepsilon\in E}P(\varepsilon)\log\frac{1}{P(\varepsilon)} \tag{3}$$

$$\underset{T}{total}=\left(\frac{T}{c_1}+\frac{T}{c_2}+\cdots+\frac{T}{c_n}\right)=T\sum_{i=1}^{n}\frac{1}{c_i} \tag{4}$$

定义第 $i$ 种报文 $\varepsilon_i$ 出现的个数 $n_i=T/c_i$,则第 $i$ 种报文在时间 $T$ 内出现的概率 $P(\varepsilon_i)$ 可表示为:

$$P(\varepsilon_i)=\frac{n_i}{\underset{T}{total}}=\frac{T}{c_i}\times\frac{1}{T\sum_{i=1}^{n}\frac{1}{c_i}}=\frac{1}{c_i\sum_{i=1}^{n}\frac{1}{c_i}} \tag{5}$$

显然有 $\sum_{i=1}^{n}P(\varepsilon_i)=1$,$P(\varepsilon_i)>0(i=1,2,\cdots,n)$。

定义第 $i$ 种消息的不确定性为消息 $i$ 的自信息 $I(\varepsilon_i)$:

$$I(\varepsilon_i)=\log\frac{1}{P(\varepsilon_i)}=\log c_i\sum_{i=1}^{n}\frac{1}{c_i} \tag{6}$$

则在时间 $T$ 内CAN总线的信息熵定义为消息的平均不确定性,即为自信息的数学期望:

$$H(E)=\mathrm{E}[I(\varepsilon_i)]=\sum_{i=1}^{n}H_i \tag{7}$$

$$H_i=p(\varepsilon_i)I(\varepsilon_i)=\frac{\log c_i\sum_{i=1}^{n}\frac{1}{c_i}}{c_i\sum_{i=1}^{n}\frac{1}{c_i}} \tag{8}$$

令 $x=c_i\sum_{i=1}^{n}\frac{1}{c_i}$,因为函数 $f(x)=\log(x)/x$ 在 $x>0$ 时为单调递增函数,当CAN网络中出现新的报文消息时有:

$$\Delta x=c_i\left(\sum_{i=1}^{n+1}\frac{1}{c_i}-\sum_{i=1}^{n}\frac{1}{c_i}\right)=\frac{c_i}{c_{n+1}}>0$$

所以函数 $f(x)$ 值增加,$H_i$ 增加,$H(E)=\sum_{i=1}^{n}H_i$ 增加。

#### 4.2.2 CAN总线报文相对距离

参考KL距离的定义,定义第 $i$ 种报文在两个相邻 $T$ 时间段消息集合的相对距离 $d_i(Q\parallel P)$:

$$d_i(Q\parallel P)=Q(\varepsilon_i')\log\frac{Q(\varepsilon_i')}{P(\varepsilon_i)} \tag{9}$$

在重放攻击场景下,假设第 $i$ 种报文在 $T$ 时间长度内以周期 $c_i$ 进行发送,那么 $T$ 时间长度内第 $i$ 种报文 $\varepsilon_i$ 出现的概率 $P(\varepsilon_i)$ 可由式(5)得到。当在下一个 $T$ 时间长度内,该报文被恶意节点重放,则在这一个 $T$ 时间长度内,该报文的频率变高,平均周期将变小,把被攻击时间段内的第 $i$ 种报文记作 $\varepsilon_i'$,平均周期定义为 $c_i'$,显然有 $c_i'<c_i$,则在该时间段内 $\varepsilon'_i$ 出现的概率可表示为:

$$Q(\varepsilon_i') = \frac{1}{c_i' \sum_{i=1}^{n} \frac{1}{c_i'}} \tag{10}$$

在理想假设下，由于没有被重放的报文消息出现的概率不会发生变化，即 $Q(\varepsilon_i) = P(\varepsilon_i)$，因为 $\log 1 = 0$，则没有被重放攻击的报文消息的相对熵会趋于 0，那么只需考查被重放报文消息的相对熵。

考虑上文的场景，第 $i$ 种报文的相对距离，用 $d_i(\varepsilon_i' \| \varepsilon_i)$ 表示：

$$d_i(\varepsilon_i' \| \varepsilon_i) = Q(\varepsilon_i') \log \frac{Q(\varepsilon_i')}{P(\varepsilon_i)} = \frac{1}{c_i' \sum_{i=1}^{n} \frac{1}{c_i'}} \log \left( \frac{c_i \sum_{i=1}^{n} \frac{1}{c_i}}{c_i' \sum_{i=1}^{n} \frac{1}{c_i'}} \right) \tag{11}$$

由于周期 $c' > 0$，则 $c_i' \sum_{i=1}^{n} \frac{1}{c_i'} > 0$，又有 $\log 1 = 0$，$f(x) = \log x$ 在 $x > 0$ 处单调递增，那么 $d_i(\varepsilon'_i \| \varepsilon_i)$ 的变化趋势仅需考虑式(11)对数运算符内的表达式是否大于 1，那么：

$$\frac{c_i \sum_{i=1}^{n} \frac{1}{c_i}}{c_i' \sum_{i=1}^{n} \frac{1}{c_i'}} - 1 = \frac{c_i \sum_{i=1}^{n} \frac{1}{c_i} - c_i' \sum_{i=1}^{n} \frac{1}{c_i'}}{c_i' \sum_{i=1}^{n} \frac{1}{c_i'}} \tag{12}$$

由 $c_i' \sum_{i=1}^{n} \frac{1}{c_i'} > 0$，只需考虑式(12)分子是否大于零，情景假设中其他报文消息没有被重放，其他报文消息的周期不变，则：

$$\begin{aligned} c_i \sum_{i=1}^{n} \frac{1}{c_i} - c_i' \sum_{i=1}^{n} \frac{1}{c_i'} &= \frac{c_i}{c_1} + \frac{c_i}{c_2} + \cdots + \frac{c_i}{c_i} + \cdots + \frac{c_i}{c_n} - \left( \frac{c_i'}{c_1} + \frac{c_i'}{c_2} + \cdots + \frac{c_i'}{c_i} + \cdots + \frac{c_i'}{c_n} \right) = \\ &\frac{1}{c_1}(c_i - c_i') + \cdots + \frac{1}{c_{i-1}}(c_i - c_i') + \\ &\frac{1}{c_{i+1}}(c_i - c_i') + \cdots + \frac{1}{c_n}(c_i - c_i') \end{aligned} \tag{13}$$

被重放的报文消息 $c_i' < c_i$，$c_i - c_i' > 0$，因此式(13)、式(12)大于零，式(11)对数运算符内的表达式大于 1，可得 $d_i(\varepsilon_i' \| \varepsilon_i) > 0$，这样就得到被重放攻击的消息相对距离的变化趋势。同理可证，当攻击消失时，没有攻击的时间段与混有攻击时间段的相对距离将会得到负值的变化趋势，$d_i(\varepsilon_i \| \varepsilon_i') < 0$。

### 4.3　实验环境

本文实验的系统环境为 Windows 7，使用 Vector 公司 CANoe(Version 8.1 SP)模拟车载 CAN 总线网络环境，使用 USB-CAN-Ⅱ模拟一个被入侵的 ECU 节点对总线网络进行攻击，如图 4 所示。模拟的车载网络包含 power_train 和 comfort 两个子网，由一个网关连接，两个子网的速率均为 500 kbit/s。包含 9 个 ECU，共 17 种不同周期和数据长度的消息报文。

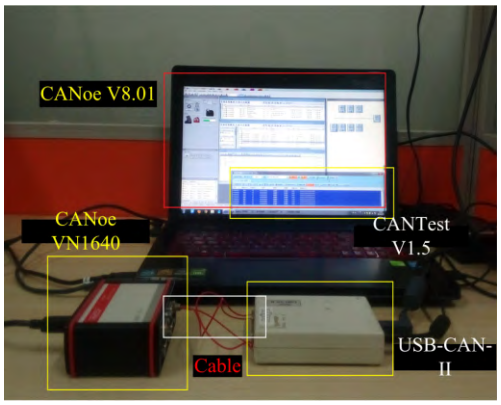


图 4　实验环境

Fig. 4　Performance evaluation environment

### 4.4　验证及讨论

攻击场景 1 为在上文所述实验环境下，攻击者在一个整段时间间隔 $T$，向 power_train 子网中发送周期为 0.05 s、帧 ID 为 0x00、数据域长度为 8 个字节的攻击报文，表 1 为 power_train 子网信息熵的变化情况。实验结果显示：在攻击者向网络中发送一个新 ID 的报文使得 power_train 子网的信息熵增加。

在攻击场景 1 中，攻击者的开始和结束均在时间间隔 $T$ 的整数时刻，但是在实际攻击场景中，攻击可以在任意时刻开始，它完全可能跨越两个时间周期，因此在攻击场景 2 中，攻击者跨越两个整段时间间隔 $T$，在 4～16 s 向 power_train 子网中发送周期为 0.05 s、帧 ID 为 0x00、数据域长度为 8 个字节的攻击报文，表 2 为 power_train 子网信息熵的变化情况。实验结果显示：在两段时间间隔 $T$ 内 power_train 子网的信息熵均增加，但是后一个时间间隔的增幅不明显。

值得注意的是，当 CAN 总线网络受到以极高频率发送的高优先级报文(如帧 ID 为 0x00)攻击时，这时 CAN 总线网络中的其他消息将难以获得总线发送权。总线上的报文消息的数量会大大下降，甚至在短时间内仅存在一种报文消息，那么这种 CAN 总线网络的不确定性大大降低(仅

有一种消息的网络系统是确定的,其熵为0),其在信息熵上的表现为系统熵值大幅度下降。

表1 攻击者在$T$时间段发送标识符为0x00的报文消息

Table 1 Attacker sent CAN identifier 0x00 during $T$ period

| 标识符 | 描述 | 周期/s | 数据大小/byte | $H_i$(无攻击) | $H_i$(有攻击) |
|---|---|---|---|---|---|
| 0x67 | Ignition_Info(点火) | 0.02 | 2 | 0.5307 | 0.5277 |
| 0x64 | EngineData(发动机) | 0.05 | 8 | 0.4088 | 0.3848 |
| 0x66 | EngineDataIEEE(发动机) | 0.05 | 8 | 0.4088 | 0.3848 |
| 0x3FC | GearBoxInfo(变速箱) | 0.05 | 1 | 0.4088 | 0.3848 |
| 0xC9 | ABSdata(ABS) | 0.05 | 6 | 0.4088 | 0.3848 |
| 0x51A | NM_Gateway_PowerTrain(传动网关) | 0.6 | 4 | 0.0816 | 0.0741 |
| 0x51B | NM_Engine(发动机) | 0.6 | 4 | 0.0789 | 0.0717 |
| 0x00 | Attacker(攻击者) | 0.05 | 8 | | 0.3590 |
| $H(E)$ | | | | 2.3264 | 2.5717 |

注:$H(E)=\mathrm{sum}(H_i)$,$T=15$ s。

表2 攻击者在4~16 s发送标识符为0x00的报文消息

Table 2 Attacker sent CAN identifier 0x00 during 4~16 s

| 时间间隔($T$=15 s) | 00:00.00~00:14.99 | 00:15.00~00:29.99 | 00:30.00~00:44.99 | 00:45.00~00:59.99 |
|---|---|---|---|---|
| 无攻击 $H(E)$ | 2.3836 | 2.3289 | 2.3309 | 2.3316 |
| 有攻击 $H(E)$ | 2.6299 | 2.3334 | 2.3309 | 2.3316 |

攻击场景3为攻击者在某一时间间隔$T$重放某一种报文消息,实验时被重放的消息并不会告知检测者。而检测者要检测是否有报文被重放,需要计算网络内所有不同种报文消息在相邻时间间隔的相对距离。实验网络的17种报文的周期、数据域长度如表3所示。实验共进行了11个时间间隔$T$($T$=15 s),对每种报文计算10个相对距离$d_i(\varepsilon_i \| \varepsilon_i')$,实验结果如图5所示。图中$x$、$y$、$z$坐标轴分别对应CAN总线报文ID(17个),计算相对距离的数量(10组)及相对距离$d_i(\varepsilon_i \| \varepsilon_i')$。图5(a)显示标识符ID为0xC9的消息的第5组相对距离$d_i(\varepsilon_i \| \varepsilon_i')$呈现一个大范围的正值跃变,根据正文4.2.2节的推断,可认为在第6个时间间隔$T$内发生了重放攻击,在0xC9消息接下来的第6组相对距离$d_i(\varepsilon_i \| \varepsilon_i')$出现了负值跃变,说明在第7个时间间隔$T$时重放攻击结束。图5(b)显示报文ID为0xC9的消息自身的相对距离发生很大波动,其变化时刻与通过图5(a)推断的时刻相符,因此可确定报文ID为0xC9的报文在第6个时间间隔$T$被重放,这说明检测结果正确。

表3 实验环境CAN网络报文

Table 3 CAN frame identifier of experimental environment

| 标识符 | 描述 | 周期/s | 数据大小/byte |
|---|---|---|---|
| 110 | Gateway_1(网关1) | 0.1 | 3 |
| 1A0 | Console_1(中控1) | 0.02 | 4 |
| 1F0 | DOOR_l(车门) | 0.02 | 1 |
| 1F1 | DOOR_r(车门) | 0.02 | 1 |
| 67 | Ignition_Info(点火) | 0.02 | 2 |
| 64 | EngineData(发动机) | 0.05 | 8 |
| 66 | EngineDataIEEE(发动机) | 0.05 | 8 |
| 111 | Gateway_2(网关2) | 0.05 | 8 |
| C9 | ABSdata(ABS) | 0.05 | 6 |
| 3FC | GearBoxInfo(变速器) | 0.05 | 1 |
| 41A | NM_Console(中控) | 1.2 | 4 |
| 51A | NM_Gateway_PowerTrain(传动网关) | 0.6 | 4 |
| 41B | NM_DOORleft(车门) | 1.2 | 4 |
| 51B | NM_Engine(发动机) | 0.6 | 4 |
| 41C | NM_DOORright(车门) | 1.2 | 4 |
| 41D | NM_Gateway(网关) | 1.2 | 4 |
| 1A1 | Console_2(中控2) | 0.5 | 2 |

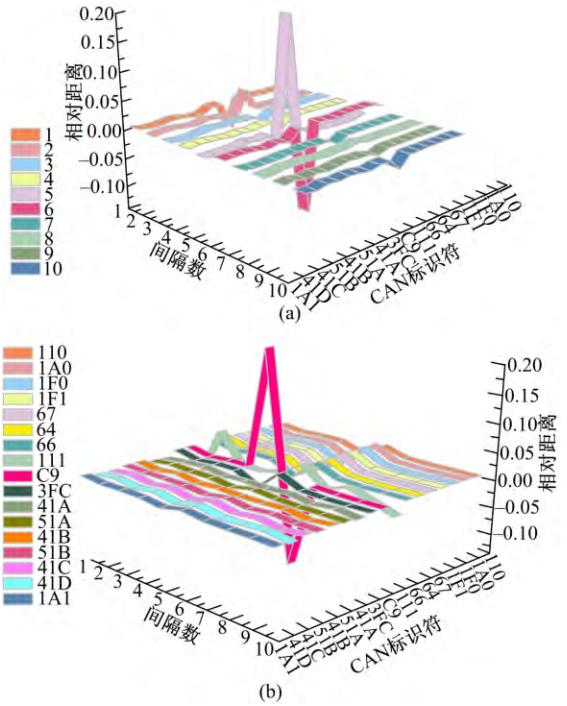


图5 CAN总线消息相对距离对比图

Fig. 5 CAN bus frame relative distance comparison

## 5　结束语

**本文提出的基于信息熵及消息相对距离的方法可用于车载 CAN 总线网络的异常检测。经实验验证，该方法可以用于检测车载 CAN 总线网络的洪泛、重放等攻击。未来的研究工作将进一步完善该方法的灵敏度，及对其他攻击手段检测的适用性。**

**参考文献：**


[1] Miller C, Valasek C. Adventures in automotive networks and control units[C]// DEFCON 21 Hacking Conference, Las Vegas, 2013.

[2] Miller C, Valasek C. A survey of remote automotive attack surfaces[C]// Black Hat, Las Vegas, USA, 2014.

[3] Miller C, Valasek C. Remote Exploitation of an Unaltered Passenger Vehicle[C]// Black Hat, Las Vegas, USA, 2015.

[4] Leinmüller T, Buttyan L, Hubaux J P, et al. Sevecom-secure vehicle communication[C]// IST Mobile and Wireless Communication Summit, Myconos Greece, 2006.

[5] European Commission within the Seventh Framework Programme. E-safety vehicle intrusion protected applications (EVITA) project[OB/OL]. http://www.evitaproject.org.

[6] Groza B, Murvay S. Broadcast Authentication in a Low Speed Controller Area Network[M]. E-Business and Telecommunications: Springer, 2012: 330-344.

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

[8] Groza B, Murvay S, van Herrewege A, et al. Libracan: a Lightweight Broadcast Authentication Protocol for Controller Area Networks[M]. Cryptology and Network Security: Springer, 2012: 185-200.

[9] Murvay P S, Groza B. Source identification using signal characteristics in controller area networks[J]. Signal Processing Letters, 2014, 21(4): 395-399.

[10] Lin Chung-wei, Sangiovanni-Vincentelli A. Cybersecurity for the controller area network (CAN) communication protocol[C]// International Conference on Cyber Security, Washingtong DC, 2012: 1-7.

[11] Schweppe H, Roudier Y. Security and privacy for in-vehicle networks[C]// IEEE 1st International Workshop on Vehicular Communications, Sensing, and Computing (VCSC), Seoul, 2012: 12-17.

[12] Schweppe H, Roudier Y, Weyl B, et al. Car2x communication: securing the last meter-a cost-effective approach for ensuring trust in car2x applications using in-vehicle symmetric cryptography[C]// Vehicular Technology Conference (VTC Fall), San Francisco, 2011: 1-5.

[13] 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): 993-1006.

[14] Yu Lu, Deng Juan, Brooks Richard R, et al. Automobile ECU design to avoid data tampering[C]// Proceedings of the 10th Annual Cyber and Information Security Research Conference, Tennessee, 2015: 10.

[15] 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.

[16] Muter M, Groll A, Freiling F C. A structured approach to anomaly detection for in-vehicle networks[C]// Sixth International Conference on Information Assurance and Security (IAS), Atlanta, 2010: 92-98.

[17] BOSCH. CAN Specification, Version 2.0[S]. 1991.

[18] Kleberger P, Olovsson T, Jonsson E. Security aspects of the in-vehicle network in the connected car[C]// Intelligent Vehicles Symposium (IV), Baden, 2011: 528-533.

[19] Lin C W, Zhu Q, Phung C, et al. Security-aware mapping for CAN-based real-time distributed automotive systems[C]// IEEE/ACM International Conference on Computer-aided Design (ICCAD), San Jose, 2013: 115-121.

[20] **刘衍珩，付枫，朱建启，等. 基于活跃熵的 DoS 攻击检测模型[J]. 吉林大学学报：工学版，2011, 41(4): 1059-1064.**
Liu Yan-hang, Fu Feng, Zhu Jian-qi, et al. DoS detection model base on alive entropy[J]. Journal of Jilin University (Engineering and Technology Edition), 2011, 41(4): 1059-1064.