doi:10.19562/j.chinasae.qcgc.2023.ep.002

智能网联汽车车载CAN网络入侵检测方法综述*

关宇昕[1],冀浩杰[2],崔 哲[1],李 贺[1],陈丽文[1]
(1. 华北理工大学机械工程学院,唐山 063210;2. 北京航空航天大学合肥创新研究院,合肥 230012)

[摘要] 智能汽车与车联网技术不断融合,汽车正朝着智能化和网联化方向发展。随着车载网络(例如:CAN网络)的复杂性以及车辆与外界相连的方式增加,汽车面临的网络安全风险大幅上升。入侵检测系统作为保护车载网络安全的重要屏障,可以有效检测外部入侵和车辆异常行为。首先,介绍了车载网络的安全属性,并分析了智能网联汽车的网络安全问题以及车载CAN网络的脆弱性和对其的攻击方式。其次,总结了近几年车载CAN网络入侵检测方法的研究现状。最后,对未来车载网络入侵检测系统的发展提出几项开放性问题。

关键词:智能网联汽车;网络安全;车载CAN网络;异常行为;入侵检测系统

An Overview of Intrusion Detection Methods for In-Vehicle CAN Network of Intelligent Networked Vehicles

Guan Yuxin[1], Ji Haojie[2], Cui Zhe[1], Li He[1] & Chen Liwen[1]
1. *School of Mechanical Engineering, North China University of Science and Technology, Tangshan* 063210;
2. *Hefei Innovation Research Institute, Beihang University, Hefei* 230012

[**Abstract**] With the continuous integration of intelligent vehicle and vehicle networking technology, vehicles are developing towards intelligence and networking. As the complexity of in-vehicle network (e.g. CAN network) increases and the way in which vehicles are connected to the outside world increases, the cyber security risks faced by automobiles have risen dramatically. As an important barrier to protect vehicle network security, intrusion detection system can effectively detect external intrusion and abnormal vehicle behavior. Firstly, the security properties of the in-vehicle network are introduced, and the network security issues of the ICV, the vulnerability of the in-vehicle CAN network and the attack modes on it are analyzed. Secondly, the status quo of research on vehicle CAN network intrusion detection methods in recent years is summarized. Finally, several open questions are proposed for the future development of the in-vehicle network intrusion detection system.

Keywords: intelligent and connected vehicle; network security; in-vehicle CAN network; abnormal behavior; intrusion detection system

前言

如今的汽车正朝着智能化、电动化、共享化、网联化——新四化方向发展[1]。随着智能汽车与车联网技术的不断融合,智能网联汽车(intelligent and connected vehicle,ICV)作为万物互联时期的新产物,已经成为全球众多国家的战略发展方向。汽车制造商为使汽车变得更为智能,向其内部增加了越来越多的电子控制单元(electronic control unit,ECU)、传感器和执行器等[2]。网联化的升级增加了车端信息与外界的互联互通,导致智能网联汽车信息安全风险不断增加。其中,车载无线通信技术(vehicle to everything,V2X)发展至今,已经成为现代

* 国家自然科学青年基金(52102447)和河北省自然科学基金(E2022209086)资助。
原稿收到日期为2022年09月04日,修改稿收到日期为2022年09月21日。
通信作者:崔哲,高级工程师,博士,E-mail:cuizhe@ncst.edu.cn。

智能汽车广泛应用的技术。该技术可以大幅度降低汽车安全事故的风险并提高驾驶人的舒适性。此外,汽车制造商将蓝牙、Wi-Fi、GPS和蜂窝网络等技术集成到T-box中[3],使车辆能够更多的与外界互联互通。在汽车网联化的同时,ICV信息安全风险不断增加,车辆信息及用户隐私面临着更大的安全考验。

早期的汽车只是独立运行的单元,并不容易受到网络攻击。而ICV具有高复杂性,并与外界互联网相连,很容易使用户的个人隐私泄漏、财产与经济损失,甚至可能给车内人员造成生命安全威胁。目前,已经发生多起对车载网络的攻击事件。 例如,Miller和Valasek使用Wi-Fi开放端口入侵吉普切诺基的车载网络,并重新对ECU编程。使汽车制动系统和发动机失灵,导致140万辆汽车被迫召回[4]。此外,据2020年的一项调查,福特和大众两款汽车也发现严重的网络安全漏洞[5]。车载GPS系统和娱乐服务系统等需要车外网络支持的服务均可受到来自黑客的攻击。在未来,ICV会暴露出愈来愈多的网络安全问题。因此,研究对其的网络安全防护势在必行。

现有车载网络信息安全增强手段有数据加密技术、消息认证技术和入侵检测技术[1]。但在车载网络这种计算资源紧张且实时性要求高的环境中,数据加密和消息认证技术往往起不到较好效果。入侵检测系统(intrusion detection system,IDS)是一种主动的安全防护技术,它可以检测出对车载网络的攻击以及车辆的异常行为。虽然最近几年一些文章对车载网络的安全问题和车载网络IDS进行了总结和分析[6-8],但车载网络安全问题和对其的入侵检测方法是实时性的问题。随着ICV技术所面临的安全问题日益增加,相关人员研究出许多应用于车载网络的新型IDS。Elkhail等[6]发表了对汽车安全漏洞、恶意软件攻击和防御的调查,介绍了过去几年中的恶意软件检测技术。Gmiden等[7]总结了当前CAN网络协议存在的缺点,以及为解决CAN网络安全问题而设计的各种方法。特别地,他们又对一些密码机制进行概述。Dibaei等[8]首先确定了ICV的主要攻击类型,总结并分析了针对这些攻击类型的防御措施,讨论了对ICV攻击防护的剩余挑战和未来研究方向。此外,Zhang等[9]介绍了物联网体系结构的层次,并且概述了物联网体系结构在不同层面上的安全问题和研究现状。Slevi等[10]重点对物联网范式的新型IDS进行调查。总结了IDS模型、类型和基本细节,主要研究使用深度学习入侵检测方法避免物联网遭受威胁。

本文的其余部分如下。在第二章首先对车载网络进行系统的概述,总结了当今应用在车内各种类型车载网络优缺点。在第三章中,本文分析了黑客对ICV的攻击途径以及车载CAN网络的脆弱性和对其的攻击方式。第四章中本文对车载CAN网络IDS进行归纳和分类,回顾了近几年车载CAN网络IDS的研究现状。由于在目前研究中,多数以车载CAN网络的IDS为主。因此在文章的最后,本文对未来车载网络IDS提出了几项有待解决的开放性问题。

1 车载网络概述

1.1 车载网络介绍

ICV是相对复杂的系统,其内部约有70-100个ECU[4],每个ECU之间的通信通过车载网络来实现。由于每种车载网络的带宽、成本和容错性等不同,被应用在车上不同的位置。图1为车载网络结构图。

1.2 车载网络的分类

由于ICV每个电控系统中通信实时性的要求不同,可以按通信速度将车载网络分为高速、中速和低速网络。根据汽车工程学会(Society of Automotive Engineers,SAE)的标准,可将车载网络分为5类。分别为A类低速网络、B类中速网络、C类高速网络、D类多媒体网络以及E类安全应用网络,如表1所示。ICV通信系统中有5种常用的车载网络,分别为控制器局域网络(controller area network,CAN)、局域互联网(local interconnect network,LIN)、FlexRay、MOST和车内以太网[6]。表2为它们的功能属性对比。

CAN是近30年以来发展起来的技术。由德国Robert Bosch公司在1983年首先提出,并最终成为国际标准[11]。CAN网络以低成本、高容错及稳定性较高等优点,在全球众多国家已经成为汽车计算机控制系统的标准,受到了诸多汽车制造商的青睐。CAN网络协议是一种串行数据通信协议,具有总线型拓扑结构,CAN网络中的ECU节点均可向其他ECU(一个或多个)发送报文[12]。CAN网络具有非破坏性仲裁机制,当多个节点同时发送数据时,其优先级由报文ID决定,ID越小优先级越高[13]。消息格式为短帧结构,数据的出错率较低,并且当数据出错时可自动关闭节点,图2为CAN网络数据帧结构图。

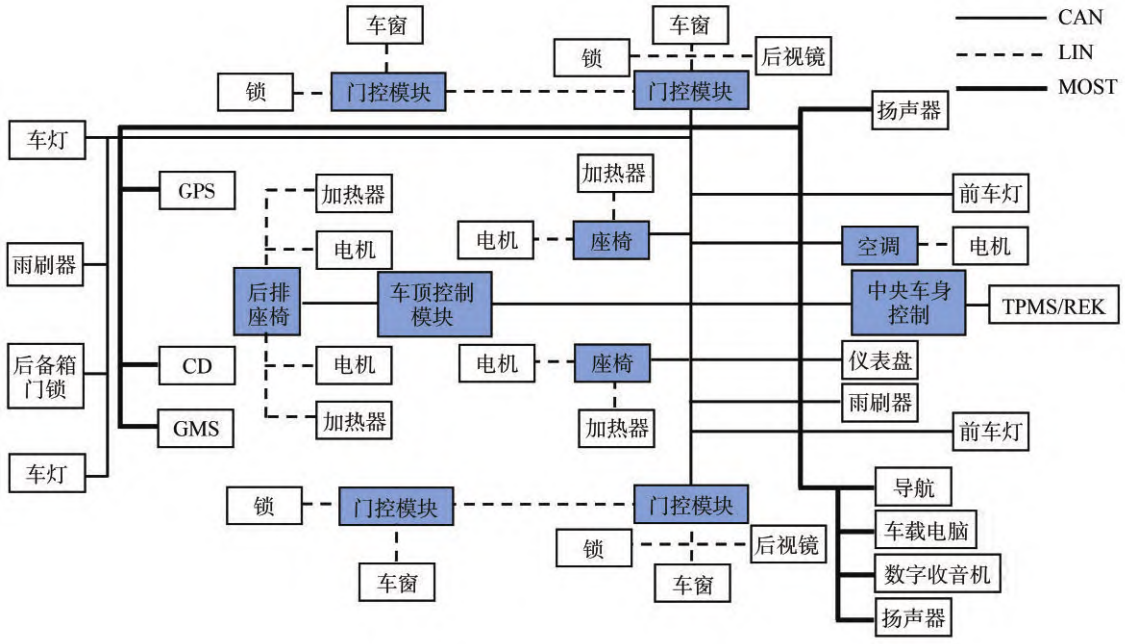

图1 车载网络结构图

CAN网络协议的传输速度最高为1 Mbps,可以满足早期汽车通信需求[14]。然而,随着现代汽车中ECU的增加,导致CAN网络负载逐渐增加,造成消息拥堵、信号传输延迟等,甚至会出现低优先级的报文传输丢失的现象。虽然升级版CAN网络(CAN-FD)的推出一定程度上增加了带宽[15],但还是无法保证能够满足未来车载通信的带宽要求。

LIN的成本和网络安全威胁较低,常用于辅助CAN网络。主要应用在实时性不高的场合(例如雨刮器、车窗升降、仪表盘等部位)。与CAN网络不同的是其结构是由一个主节点和一个或多个从节点组成,最多可以连接15个从节点。消息的时序由主节点决定,容错性较低,且消息的最高传输速度仅有19.2 Kbps。

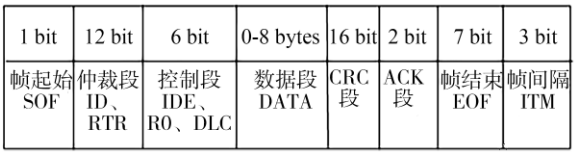

图2 CAN网络数据帧结构图

表1 车载网络分类

网络类别	网络标准	通信速度	成本
A类低速网络	TTP/A、LIN	小于10 Kbps	低
B类中速网络	低速CAN、VAN	10 Kbps-125 Kbps	低
C类高速网络	高速CAN、CAN-FD、TTP/C、FlexRay	125 Kbps-1 Mbps	中
D类多媒体网络	MOST、蓝牙、ZigBee	250 Kbps-100 Mbps	高
E类安全应用网络	Bytelight	10 Mbps	高

表2 常见车载网络的对比

车载网络类型	最大带宽	支持节点个数	拓扑结构	容错性	威胁程度	主要应用部位
CAN	1 Mbps	128	总线型	高	高	发动机、自动变速器、ABS系统、安全气囊、车灯、中央门锁等
LIN	19.2 Kbps	16	总线型(单线)	低	低	车门、车窗升降、灯光、空调等
FlexRay	10 Mbps	大于16	总线型、星型、混合型	高	高	安全雷达、车轮驱动、转向传感器、辅助控制系统等
MOST	150 Mbps	64	环形	高	高	音频模块、导航系统、娱乐系统等
车载以太网	1 Gbps(预计)	未指定	菊花链型、星型、树型	高	高	激光雷达、安全雷达、ECU闪存接口等

FlexRay是由FlexRay联盟开发的一种具备故障容错的高速车载网络。可以通过单通道或双通道进行消息的传输,且单通道消息传输速度最高可达到10 Mbps[16]。主要应用在安全性极高的位置(例如电子制动、电子转向盘等)。另外,当某一个通道出现故障,另一通道仍然可以进行消息的发送,这使得FlexRay具有较高的容错性。但FlexRay的价格比CAN昂贵许多,并不适合大量应用在车载网络中。

MOST是由宝马、DaimlerChrysler、Harman/Becker等公司联合开发的一种用于汽车媒体系统中消息传输的车载网络,采用环形拓扑结构,其最大带宽理论值为150 Mbps[8]。并且采用塑料光纤作为物理层,网络与电磁干扰隔离,防止信息娱乐系统中出现嗡嗡声等问题[8],比CAN更适合媒体系统数据传输。但由于成本较高以及网关的开发难度过大,目前在高端汽车应用较多。

车载以太网的带宽可以达到100 Mbps[8],预计在不久后可增加近1 Gbps,比CAN网络协议的速度快约100倍。然而,由于其成本远高于CAN,很可能无法完全取代CAN网络,而是用于辅助CAN网络更好的改变汽车通信功能。

2　ICV网络安全问题分析

2.1　ICV的攻击途径分析

随着汽车智能化的快速发展以及网联化技术大面积覆盖,越来越多的攻击入口被暴露在外,黑客可以通过这些入口访问车载网络。车载网络受到的网络攻击途径可分为物理访问和无线访问攻击两类,其中物理访问攻击分为直接和间接物理访问攻击两种,而无线访问攻击分为近程和远程无线访问攻击。图3为ICV中潜在攻击途径。

维修人员可通过车载诊断系统(on-board diagnostic,OBD)中的OBD-II端口或OBD加密狗直接访问车辆ECU及车载网络[17]。OBD-II端口可以监测车辆速度、行驶里程来调节车辆的性能[18]。但OBD-II端口缺少身份认证机制,黑客可通过该端口访问车载网络。其次,电动汽车充电桩通过充电电缆与车辆进行信息交换,黑客可以攻击充电桩等基础设施,进而攻击任何连接到充电桩的汽车[19]。另外,汽车内部的信息娱乐系统也很容易遭到非法入侵。Checkoway等[20]证明了黑客可以通过OBD-II端口、CD播放器、USB等入口点访问车载网络并注入攻击报文。腾讯敏锐安全实验室的研究人员对雷克萨斯汽车进行安全实验评估时发现车载蓝牙和OBD系统存在安全漏洞,利用这些漏洞他们可以进入汽车信息娱乐系统,将攻击数据包注入到CAN网络中[21]。Zingbox的研究人员将恶意制作的USB设备连接到信息娱乐系统中,一旦与驾驶员的手机配对,信息娱乐系统中的恶意软件就会利用手机的短信服务等手段来访问个人信息[22]。

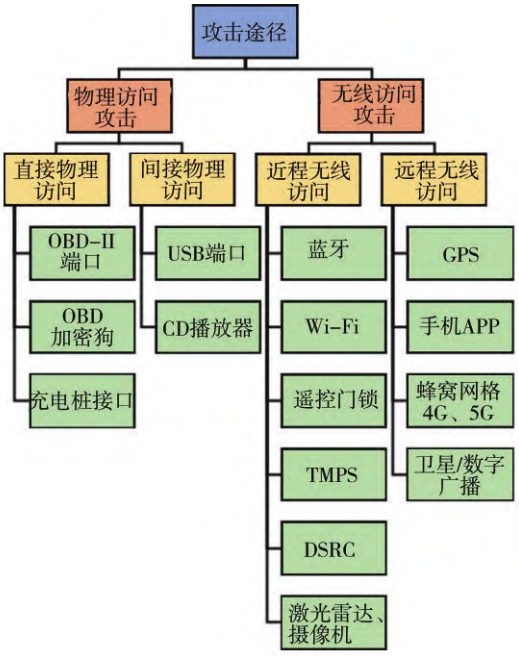

图3　ICV中潜在攻击途径示意图

目前大部分汽车中都装有车载蓝牙设备,黑客可利用蓝牙设备中的漏洞访问车载网络。2018年赛尔黑客新闻报道出几个汽车品牌的信息娱乐系统中发现了一个新的被称为“CarsBlues”的大规模网络漏洞,黑客能通过该蓝牙漏洞将车主手机同步到汽车的个人身份信息窃取[23]。腾讯敏锐安全团队将汽车连接到恶意Wi-Fi热点,使用网络浏览访问网络来控制车辆,并在视频中展示了对汽车的攻击[24]。Vanhoef等[25]研究了受保护的Wi-Fi仍有受到拒绝服务攻击(denial of service,DoS)的可能。胎压检测系统(tire pressure monitoring system,TPMS)是保障行车安全的报警装置,Rouf等[26]分析了TPMS通信协议,并表明该系统可能受到攻击而出现故障。同样,车辆中的车载雷达、专用短程通信技术(dedicated short range communications,DSRC)、遥控门锁系统等均存在安全威胁[19]。Woo等[27]演示了使用手机恶意APP在汽车联网的环境下对车辆进行无

线攻击,并设计了一种应用于车载环境的安全协议。车载GPS系统可以给汽车提供驾驶辅助和定位,但黑客能向该系统提供的接口注入恶意数据攻击车辆[28]。同时,汽车中的远程通信单元允许车辆与蜂窝网络进行通信,黑客可通过蜂窝网络对车辆实施恶意行为[20]。另外,黑客也可以通过车载广播等途径攻击车辆,但黑客通过这种攻击途径取得成功的可能性很低[19]。

2.2 车载CAN网络脆弱性分析

车载网络中CAN网络的威胁程度最高,通常是黑客的主要攻击目标。黑客一旦获得CAN网络的访问权限,就能通过易受攻击的接口(USB、Wi-Fi、CD播放器等)读取ECU内部数据,将攻击报文注入到CAN网络中[20]。车载CAN网络在最初设计时存在的缺陷如下。

仲裁机制的缺陷:CAN网络具有仲裁机制,网络中的节点通过报文ID来确定优先级。假如入侵者一直发送高优先级报文,导致CAN网络一直被占用,其他的节点无法发送报文[6]。

广播传输特性的缺陷:CAN报文以广播形式传输,网络中的所有ECU均可监听CAN网络中的消息。一旦黑客控制任意节点,就可通过该节点读取消息内容。

缺少消息检验及认证机制:CAN网络缺乏身份认证机制[29],无法判断消息是否存在异常。当黑客破解CAN网络协议后,可直接向网络中发送伪造的报文。例如,高速行驶的汽车收到伪造的熄火命令,但ECU无法识别消息的真伪,会导致车辆的突然熄火,引发交通事故。

缺少信息安全及加密机制:CAN报文在CAN网络中以明文形式传输。由于缺乏加密机制,黑客可以轻松读取并破解其中的数据。CAN网络中信息的完整性无法得到保障,存在信息泄露的风险。

2.3 车载CAN网络攻击方式分析

ICV容易受到不同程度的网络攻击,黑客可以通过多种途径点访问CAN网络。对于车载CAN网络的攻击类型可以分为被动和主动两类,常见的攻击方式对比如表3所示。

嗅探攻击:当黑客成功入侵CAN网络后,可监听网络内部的报文并对其进行逆向工程,以便攻击车辆上的特定部件。如图4(a)所示。

DoS攻击:由于CAN网络的仲裁机制,黑客可向网络中发送大量高优先级的攻击报文,导致其它节点无法向网络中发送消息,严重的甚至可能导致车载网络的崩溃。如图4(b)所示。

重放攻击:当黑客捕获到ECU发送的报文后不对其做任何处理,再次将报文重放到网络中,可能导致车内正常通信受到干扰。如图4(c)所示。

篡改攻击:当黑客捕获到网络中的报文后,首先对报文的内容进行修改,再将其发送到CAN网络中。其中,修改的部位可能是报文ID或数据段的信息,以上两种篡改方式均会造成或多或少的影响。如图4(d)所示。

消息注入攻击:当黑客成功入侵CAN网络后,可直接向其内部注入恶意报文,可能会给汽车安全带来严重威胁。如图4(e)所示。

欺骗攻击:当黑客掌握网络中CAN数据帧的详细信息后,便可将欺骗性的报文对网络实施特定的攻击。这些报文中包含错误的信息,可能会误导相应的ECU。如图4(f)所示。

丢弃攻击:当黑客成功入侵车载网络中的某一节点或者网关后,可以删除网络中的报文,导致某些重要的报文无法被其他节点接收,使汽车某些重要的功能出现异常。如图4(g)所示。

模糊攻击:黑客使用某些变异算法将合法数据转换成随机数据,再将随机数据注入到CAN网络

表3 车载CAN网络常见攻击方式对比

攻击方式	威胁程度	防护难度	攻击结果
嗅探攻击	中	高	用户隐私信息和车辆信息泄露
DoS攻击	高	低	大量高优先级报文占用CAN网络,造成通信故障甚至车载的网络崩溃
重放攻击	高	中	未作修改的报文重放CAN网络中,使网络负载率和ID熵增加,影响通信功能
篡改攻击	高	中	将CAN网络中报文的内容修改,产生错误帧和信号,影响通信功能
消息注入攻击	高	中	直接向CAN网络中注入恶意报文,网络负载率和ID熵增加,使汽车内部功能紊乱甚至导致汽车瘫痪
欺骗攻击	高	中	将欺骗性报文注入到CAN网络,使网络负载率和ID熵增加,导致汽车突然失控
丢弃攻击	高	高	直接删除CAN网络中的报文,ID熵降低,可能使汽车某些重要功能失效
模糊攻击	高	高	将变异算法转换的随机数据注入到CAN网络中,使网络负载率和ID熵增加
伪装攻击	高	中	模拟节点向车载网络发送伪造的报文,使网络负载率和ID熵增加

中,干扰车内正常通信。如图4(h)所示。

伪装攻击:黑客可以模拟节点向网络发送报文,由于CAN网络无消息认证机制,网络中的其他节点无法识别消息的真伪。如图4(i)所示。

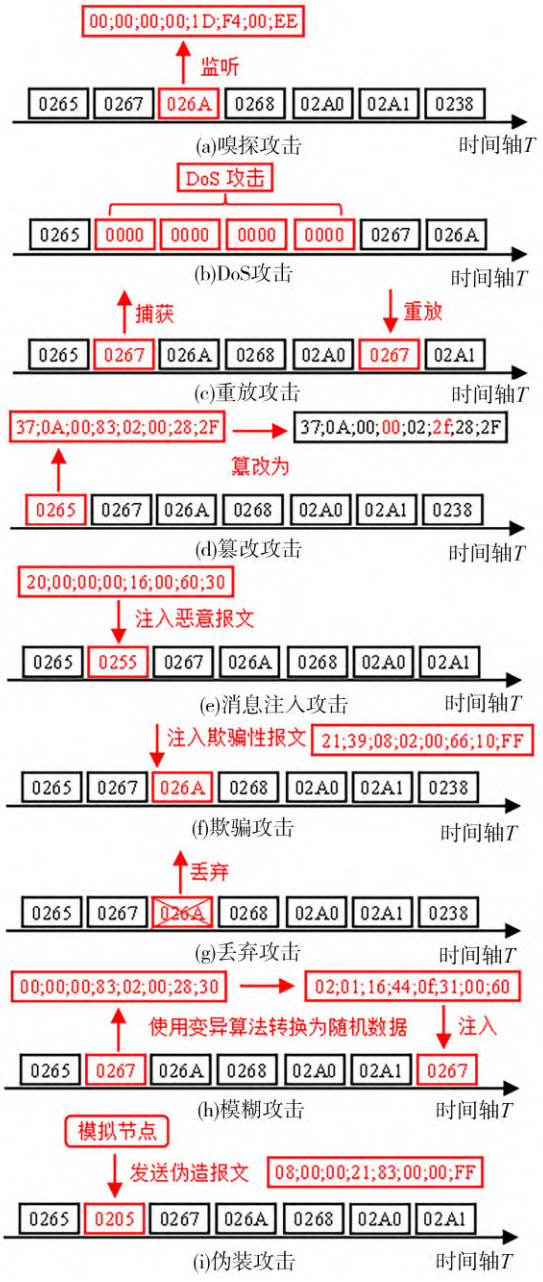

图4　车载CAN网络常见攻击方式示意图

3　车载网络入侵检测系统

入侵检测系统从被提出以来,在保护传统计算机网络的安全性中发挥至关重要的作用。汽车网联化的升级导致汽车信息安全风险加重。随着汽车信息安全概念的提出,关于车载网络IDS的研究备受关注。车载网络IDS作为保护车载网络安全的一种重要方法,它可以检查车载网络中的可疑活动和外部入侵,同时发出入侵警报确保驾驶人能够及时采取相应措施。它不同于其他的信息安全增强方法(例如数据加密、消息认证技术等),入侵检测系统不会占用车载网络内部大量的运算资源,适合车载网络这种资源受限的环境。

入侵检测按照检测技术分为基于签名的入侵检测系统(signature-based intrusion detection system,SIDS)和基于异常的入侵检测系统(anomaly-based intrusion detection system,AIDS)。其中,基于签名的入侵检测系统通过监视预定义的攻击签名列表实现入侵检测[30]。该方法的优点是检测结果出现假阳性的概率较低且检测速度快,但由于该方法的数据库是提前设定好的,无法有效识别新型攻击。当有新型恶意签名出现时,需要人工对数据库进行实时更新。而基于异常的入侵检测系统是通过监测车载网络状态是否偏离正常模式来识别入侵。该方法通过训练大量数据得出检测模型,与车载网络中的数据进行对比来判断系统是否出现异常。这种检测方法的优点是对未知攻击具有预测性,能够检测未知类型的攻击。本文针对车载CAN网络的IDS按照检测技术进行总结和分析。

3.1　基于签名的车载CAN网络入侵检测方法

Studnia等[31]通过对CAN网络特殊性的分析,得出一组禁止的消息序列(即签名)进行入侵检测。他们创建了一个全面的签名库,该签名库可以在汽车的整个生命周期中使用,无需更新。Jin等[32]提出了一种基于签名的轻量级入侵检测系统,该系统所需的计算时间较少,适用于运算资源受限的车载环境中。他们从实际场景中收集数据后进行统计分析,提取检测时所用的签名,并使用CANoe软件对车辆CAN网络进行模拟仿真。试验结果表明,该入侵检测系统可以有效地检测出丢弃攻击和重放攻击,检测率分别为100%和98.2%。但对篡改攻击的检测率仅有66.2%,他们提出利用信号之间的关系可提高篡改攻击的检测率。

虽然基于签名的车载CAN网络IDS对已知攻击有匹配速度快及高精度等优点,但对这种超大型数据库的维护也是一项挑战。另外,黑客对车载网络的攻击方式多种多样,当黑客使用新型恶意签名攻击CAN网络时可能导致基于签名的入侵检测系统

的失效。可将该方法与基于异常的车载CAN网络IDS相结合的设计方式来解决无法检测到未知攻击的问题。

3.2 基于异常的车载CAN网络入侵检测方法

基于异常的入侵检测系统多是通过特征提取或数据统计建立正常特征行为规律,当违反规律时认为入侵行为发生。可将特征分为物理特征和数据特征两类,其中物理特征表示为车载网络通信在物理层存在着诸多规律(如电压波动、时钟偏移),而数据特征主要指传输报文的类别、标识、有效载荷、消息内容等。车载网络在数据特征方面的异常检测研究方法较多,本文对其从几个重要方向进行分类总结,如图5所示。各类检测方法的文献对比如表4~表6所示。

3.2.1 基于物理特征的方法

Murvay等[33]根据CAN网络的物理特性,采用低通滤波、均方误差和卷积等方法对采集物理层信息进行提取和处理,通过实验证明了不同节点的物理特征存在差异,这种差异可以作为节点认证和信息识别的依据。Ning等[34]提出一种基于局部离群因子(local outlier factor,LOF)的入侵检测方法。该方法通过CAN帧电压的物理特征来判断消息是否由合法的ECU发送。通过在两辆车上的大量实验验证可知,该方法平均检测率为98.9%,误检率小于0.5%,并提出可以使用验证机制来降低误报率。

Tian等[35]提出一种基于温度变化指纹技术(temperature-varied fingerprints,TVF)对入侵检测系统。该方法利用了ECU的时钟偏移随温度变化的规律来识别攻击源。证明了ECU的时钟偏移量随温度的变化而变化,并提出分布在发动机附近不同位置的ECU可能由于温度的差异导致时钟偏移的入侵检测方法失效。通过性能评价实验可知,该方法在能有效检测伪装攻击的同时也能够检测出攻击的来源。Zhao等[36]利用ECU的时钟倾斜设计了一种名为ClockIDS的入侵检测方法,该方法根据时钟偏移为每个ECU建立一个独特的指纹。在此基础上,利用经验规则和动态时间扭曲实现了入侵检测和攻击源检测的功能。并用实验证明了所提出的方法的平均检测率为96.77%,并且平均时间成本仅有1.99 ms。

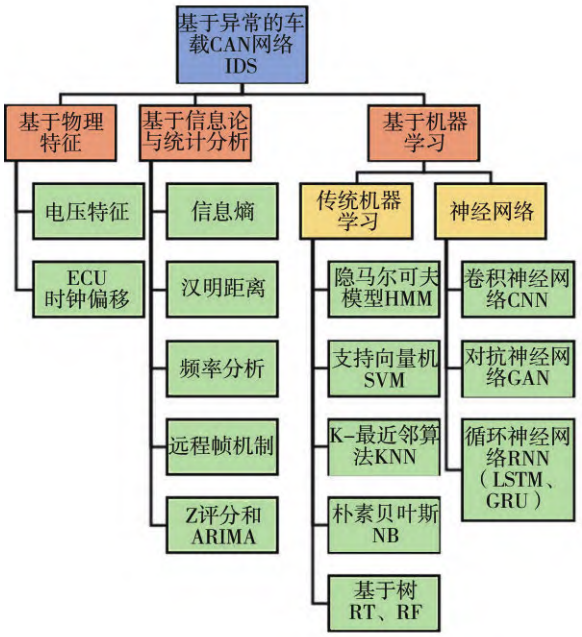

图5 基于异常的车载CAN网络IDS示意图

3.2.2 基于信息论与统计的方法

Muter等[37]首次将基于信息熵的异常检测方法引入到车载网络入侵检测的领域。该作者认为,车载网络中的流量比传统计算机更受限。正常状态下车载网络中的熵值不会发生大的改变,通过分析熵值的变化来判断是否有异常事件的发生。通过向真实车辆CAN网络中实施消息注入、DoS、伪装攻击,实验结果表明,该方法虽能实现对这3种攻击的异常检测,但在处理小规模的攻击模式的能力具有局限性,在识别车辆或用户的正常行为时可能会产生误报。于赫等[38]提出了一种基于信息熵及CAN报文相对距离的方法对车载CAN网络实现入侵检测。

表4 基于物理特征的车载CAN网络入侵检测方法

文献	年份	检测技术	检测的攻击方式	存在的问题	数据集来源	数据集是否开源
[33]	2014	低通滤波、均方误差和卷积	未说明	没有实际攻击实验检测方法的可行性	实车数据	否
[34]	2019	CAN帧电压的物理特征	未说明	未给出检测的具体是何种攻击类型	实车数据	否
[35]	2019	ECU的时钟偏移随温度变化的规律	伪装攻击	无法检测到非周期性的ID	实车数据	否
[36]	2022	ECU时钟偏移	欺骗、丢弃、伪装攻击	无法检测到非周期性的ID	实车数据	否

使用CANoe软件模拟CAN网络环境,对3种攻击场景实验分析表明,该方法可有效检测到重放和DoS攻击。Marchetti等[39]提出了一种基于熵计算的异常检测算法。通过分析车载CAN网络交换消息的熵水平,观察到熵值非常稳定,分布类似于正态分布。若熵值过大偏离平均熵值,则报告异常。为了反映真实道路的交通状况,对高速公路上驾驶过程中收集的数小时CAN消息进行实验评估,该算法只能检测出包含大量伪装消息的攻击。对于少量伪装消息的攻击,该方法需要多个异常检测器(每个ID一个)并行执行,但这种方法对于在正常条件下熵表现出很大变化的一小部分ID也是无效的。Wu等[40]对CAN网络特点分析后,优化了以前的基于信息熵的入侵检测方法。使用具有固定消息数量的最佳滑动窗口大小来提高IDS的检测精度和响应时间。他们所提出的方法可以检测到所有DoS攻击,对于消息注入攻击的检测率也达到92.3%,显著提高了检测精度,并且未发生误报。Ohira等[41]发现了一种称为熵操纵攻击的新型DoS攻击,提出一种基于两个滑动窗口相似性的DoS攻击检测方法。其中的一个滑动窗口由实际接收的CAN ID(窗口ID:WIDs)组成,另一个滑动窗口由普通CAN ID(标准ID:CIDs)组成。该方法使用辛普森系数计算WIDs和CIDs中的相似性。通过从真实车辆上采集的CAN消息进行实验,所提出的系统可以检测所有类型的DoS攻击,且检测时间与基于熵的入侵检测系统相比缩短了93.33%。此外,为促进针对DoS攻击对策的研究,该作者公布了源代码。Islam等[42]提出一种基于图形的CAN网络入侵检测方法,该方法借助图形理论、统计分析和卡方检验来检测异常的CAN消息。首先将非攻击数据定义为基本假设,并将其定义为基本分布。然后使用其他分布与基本分布相比较。可以明显观察到分布的差异。实验测试表明,该方法比文献[39]中方法的准确性提高13.73%。Ling和Feng[43]为检测CAN网络中的恶意消息提出了一种算法。该算法利用消息的ID与其可中断发生的频率相结合,通过计算输入消息ID的连续数量,如果ID计数器超过给定阈值,IDS会发出警报。使用CANoe和CAPL仿真实验结果表明,该算法可以检测到DoS攻击和消息注入攻击。Lee等[44]基于CAN网络中远程帧的“请求和应答”机制,通过分析远程帧对有攻击和无攻击场景下的应答行为,提出一种基于远程帧的车载网络入侵检测系统OTIDS。他们使用实车采集的远程帧应答数据提出窗口偏移量与时间间隔、及时响应、丢失响应4种特征构建的正常行为检测模型。通过实验测试,OTIDS可快速实现对DoS、模糊攻击和伪装攻击的检测,并公布了研究所用的数据集[47]。

表5　基于信息论与统计分析的车载CAN网络入侵检测方法

文献	时间	检测技术	检测的攻击方式	存在的问题	数据集来源	数据集是否开源
[37]	2011	信息熵、相对熵	DoS、伪装和消息注入攻击	检测小规模攻击模式的能力有限	实车数据	否
[38]	2016	信息熵 、CAN报文相对距离	DoS和重放攻击	检测技术的灵敏性不足	软件模拟数据	否
[39]	2016	信息熵、熵值偏离程度	消息注入和模糊攻击	检测小量伪装攻击消息的能力有限	实车数据	否
[40]	2018	信息熵、模拟退火算法优化滑动窗口	DoS和消息注入攻击	需考虑车辆运行状态对信息熵的影响	实车数据	[47]
[41]	2022	图形论、卡方检验、统计分析	DoS、欺骗、模糊和重放攻击	检测所用图形属性较单一	实车数据	否
[42]	2020	信息熵、滑动窗口相似性	DoS攻击	检测系统的功能较单一	实车数据	[47]
[43]	2012	检测异常CAN ID和频率	DoS和消息注入攻击	检测小规模攻击模式的能力有限	软件模拟数据	否
[44]	2017	远程帧请求与响应之间的偏移率和时间间隔	DoS和模糊攻击	未给出该系统的检测精度和其他性能指标	实车数据	[47]
[45]	2017	ID相同且连续的CAN消息有效载荷之间的汉明距离	欺骗和消息注入攻击	对重放攻击的检测能力有限	实车数据	否
[46]	2018	时间序列算法、检查CAN ID广播间隔的变化	重放和消息注入攻击	需优化阈值、模型因子和参数来提高性能	实车数据	否

表6 基于机器学习的车载CAN网络入侵检测方法

文献	年份	检测技术	检测的攻击方式	存在的问题	数据集来源	数据集是否开源
[48]	2016	HMM	消息注入攻击	需进一步研究如何处理罕见异常状态以及如何确定最佳阈值	实车数据	否
[49]	2018	HMM、回归模型	添加噪声攻击	该研究没有提供检测模型的训练时间和检测延迟	软件模拟数据	否
[50]	2019	改进的BAT算法、OCSVM	DoS攻击	该研究没有提供检测模型的训练时间	实车数据	否
[51]	2020	RT、RF、SGD和NB	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	该研究没有提供检测模型的训练时间	实车数据	[47][54]
[52]	2021	KNN、RF、SVM和MLP	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	该研究没有提供检测模型的训练时间	实车数据	[47][54]
[53]	2018	GAN	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	无法准确区分流量异常是电子元件故障引起的还是黑客恶意攻击引起的	实车数据	[54]
[55]	2021	GAN	DoS、消息注入、伪装和篡改攻击	需优化GAN模型以减少运算资源,将其轻量化	实车数据	否
[56]	2016	LSTM	DoS攻击	该方法将每个ID的数据序列视为相互独立的	实车数据	否
[57]	2021	LSTM	重放和篡改攻击	计算速度较慢,未来需要将其轻量化	实车数据	[63]
[58]	2022	LSTM	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	该研究没有提供检测模型的训练时间和检测延迟	实车数据	[54]
[59]	2020	DCNN	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	需进一步研究如何将其在线应用在汽车中	实车数据	[54]
[60]	2022	CNN	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	只能检测到干扰CAN数据包正常序列的攻击	实车数据	[54]
[61]	2022	CNN、LSTM	DoS、模糊、欺骗驱动装置和欺骗RPM仪表攻击	该研究没有提供检测模型的训练时间和检测延迟	实车数据	[54]
[62]	2021	CNN、AGRU	DoS、模糊和伪装攻击	该研究没有提供检测模型的训练时间和检测延迟	实车数据	[47]

Stabili等[45]提出一种CAN网络入侵检测算法,该算法通过计算ID的CAN报文有效载荷序列的汉明距离与离线训练阶段建立的有效汉明距离的参考范围进行比较,分别对消息注入攻击和重放攻击两种入侵行为实施检测。对福特汽车未经修改的CAN流量跟踪进行的实验评估表明,该模型能够有效检测到消息注入攻击,并且该算法具有较低的计算开销(约为几百字节),适合用于车辆ECU中。但这种方法并不适合检测重放攻击。Tomlinson等[46]对CAN广播进行了分析,并将时间定义的窗口方法与Z评分和自回归综合移动方法(autoregressive integrated moving average model,ARIMA)相结合。将所提出的方法与平均时间间隔监督的方法进行了比较,并测试了这些方法是否能够触发丢弃数据包和插入数据包的高优先级。测试结果显示,无监督方法具有高优先级。另外还强调了确保最佳阈值的重要性,阈值设置的高低均会降低检测方法的灵敏度和特异性。

3.2.3 基于机器学习的方法

Narayanan等[48]收集不同车辆的CAN消息,生成了一个用于预测车辆异常状态的隐马尔可夫模型(hidden Markov model,HMM)。该模型不但可以检测攻击状态,还能检测到车辆中不安全的行为(例如在200英里/h的车速下打开车门是不安全的)。他们通过观察速度传感器和发动机速度传感器的值是否突然变化实现对车辆异常状态的检测。类似的,Levi等[49]提出一种基于时间的检测技术,该技术使用HMM和回归模型来检测车辆异常。他们应用HMM模型学习车辆正常行为并计算模型似然分数,然后基于时间特征建立回归模型并使用回归模型预测时间间隔似然分数。通过比较两个模型的似然分数来检测相关异常。

Avatefipour等[50]提出一种改进的机器学习异常检测模型,使用基于改进的单类支持向量机构建所提出的模型,并利用改进的蝙蝠算法进行优化。为证明所提出模型的性能,他们使用传统的一类支持向量机(support vector machines,SVM)和隔离森林(isolation forest,IF)算法与该模型进行评估。相比之下,所提出的方法具有更高的检测率,并且可以表现出很高的搜索能力和收敛性。

Minawi等[51]和Alfardus等[52]分别提出两种基于机器学习的CAN网络入侵检测系统,所提出的系统可以直接插入车辆中的OBD端口。以上两种系统模型均由CAN报文输入层、威胁检测层和警报层这3层组成。其中,文献[51]中的威胁检测层包含随机树(random tree,RT)、随机森林(random forest,RF)、带铰链损失的随机梯度下降(stochastic gradient descent,SGD)和朴素贝叶斯(naive Bayes,NB)4种算法,而文献[52]中威胁检测层包含K-最近邻网络(k-nearest neighbor,KNN)、RF、SVM和多层感知器(multilayer perceptron,MLP)4种算法。他们使用相同的数据集对各自所提出的算法进行评估。结果表明,文献[51]中的系统使用朴素贝叶斯算法和随机树算法来检测DoS攻击,实现了100%的准确率。另外,随机树算法在模糊攻击中的准确率也达到了99.99%。文献[52]中的系统对伪装和DoS攻击的检测率达到100%,并且对模糊攻击的检测率也高达99%。

Seo等[53]提出一种生成对抗网络(generative adversarial networks,GAN)的车载IDS模型(GIDS),并公布了该研究所用数据集[54]。首先使用one-hot编码将CAN ID转换为图像,第1鉴别器接收CAN图像并输出一个0到1的值,若输出结果低于阈值则报告异常(检测出已知攻击)。若高于阈值则图像由第2鉴别器接收并输出一个0到1之间的值,输出低于阈值,则报告异常(检测出未知攻击)。实验表明,GIDS对4种攻击方式的平均检测率大于98%,但GIDS无法区分CAN流量异常是由电子元件故障引起的还是黑客恶意攻击引起的。Xie等[55]分析了CAN网络的安全威胁,提出了一种增强深度学习GAN模型的入侵检测技术。他们引入汽车CAN通信矩阵,将同一发送方的所有消息分组到数据块作为入侵检测系统的输出。通过实验评估结果显示,所提出的模型可以有效抵御DoS、消息注入、伪装和篡改攻击。

Taylor等[56]提出使用(long short-term memory,LSTM)神经网络检测汽车CAN网络中序列数据的异常。所提出的方法无需对数据信息解码,并且具有检测未知攻击的能力。但该方法将每个ID的数据序列视为独立的序列,并没有考虑不同消息类型之间相互依赖的关系。类似地,Longari等[57]为车载网络专门设计了一种LSTM的入侵检测系统CANnolo。该系统采用无监督学习模式,在训练阶段自动分析数据,无需知道消息的语义。运行时利用经过训练的CAN消息并预测后续序列。然后,根据真实数据和预测数据之间的重建误差检测异常。该方法优于文献[56]中所提出的方法。但此方法的计算速度较慢,需将其轻量化。Ding等[58]利用CAN报文之间的时间相关性提出一种基于双向长短期记忆网络(Bi-LSTM)的入侵检测系统,并设计出一种滑动窗口策略,对实车采集的数据集进行时间序列线性回归。在通过确定的滑动窗口构造二维输入数据样本集,利用Bi-LSTM网络学习二维数据特征训练分类器实现入侵检测。为验证入侵检测模型的性能,使用数据集[54]进行实验。实验中,Bi-LSTM模型由输入层、两个连续层中16个单元的隐藏层和一个完全连接的输出层组成。结果显示,Bi-LSTM模型高于其他网络模型精度。除DoS攻击数据集外,其他3种攻击数据集的检测准确率均达到100%。与现有研究方法相比,对4种数据集的检测准确率平均提高了5.3%、3.8%、2%和3.3%。

Song等[59]提出一种基于深度卷积神经网络(deep convolutional neural networks,DCNN)的入侵检测系统。并提出一个名为frame builder的新模块,能使CAN通信量直接输入所提出的模型中,无需对数据预处理。为测试该系统的可行性,使用数据集[54]对该系统进行实验。结果表明,所提出的系统可以有效检测DoS、模糊、欺骗驱动装置和欺骗RPM仪表这4种攻击模式。他们还比较了其他著名的机器学习算法的性能,评估结果表明DCNN模型要明显优于其他的机器学习技术。

Arai等[60]提出一种通过递归图生成的图像来训练卷积神经网络(convolutional neural networks,CNN)模型对车载网络进行入侵检测。在这项研究中,他们使用CAN数据包的时间戳和仲裁ID来训练模型。但时间戳不直接用于训练,仅用于保持数据包的优先级。提取数据集的仲裁ID并将其编码为介于0和N之间的值(N表示唯一仲裁ID的总数)。随后,仲裁ID的编码序列使用RP转换为

CNN的输入图像。在从RP中的平方矩阵中生成训练图像。最后,CNN模型将车载网络攻击分类为二元或多类分类。

Lo等[61]提出一种基于CNN和LSTM所组成的车载入侵检测系统HyDL-IDS。该IDS主要由CAN流量预处理器和HyDL检测器组成。CAN流量预处理器首先将捕获到的CAN流量转换为统一尺度,再将处理好的数据输入到HyDL模块中。HyDL检测器相当于整个系统的大脑,从网络流量中提取空间和时间特征,在使用上述两种深度学习方法对流量分类。他们使用数据集[54]将该系统与传统机器学习方法和神经网络方法进行比较,HyDL-IDS在检测精度和误报率方面都有显著提升。Javed等[62]将CNN与基于注意力的门控单元(attention-based gated recurrent unit, AGRU)相结合,提出一种名为CANintelliIDS的入侵检测方法。检测模型由3个AGRU层和两个CNN层组成,首先将数据点转换为向量序列并输入到CNN层中,CNN再将输入序列中的重要特征提取到AGRU模型中。AGRU根据数据点的关系方面和上下文信息学习序列,以调整其权重。注意力机制根据数据点序列的显著性为其分配权重分数,在将数据点的权重分数与相应的向量相乘,并生成上下文向量来预测目标标签。使用数据集[47]将所提出的方法与现有方法进行比较,结果显示,所提出的方法比现有方法提升10.79%的性能。

4 车载网络入侵检测技术发展趋势

智能网联技术的发展,使现代汽车能够更多地连接到互联网之中,汽车的信息安全所面临的风险显著增加。车载IDS作为一种主动防御技术,不仅可以识别外部入侵,还能检测车载网络内部系统异常,是现阶段车端最有效的安全防护方法。但目前对车载IDS的研究仍有很多不足,结合前文所总结的车载IDS研究现状,本文对未来车载IDS提出了几项有待解决的开放性问题。

4.1 如何提升车载网络IDS检测能力的全面性

在现实场景中,车辆所处的环境以及可能遭受到的网络攻击方式复杂多样。而现有对车载IDS研究多数只是针对车载CAN网络的一种或几种攻击方式进行入侵检测,检测的环境较为单一,并不具备全面的入侵检测能力。然而,车联网是一种复杂的环境,网联化的加重导致黑客对ICV的攻击途径和攻击方式会逐渐变多。因此,在今后车载IDS的研究中,不应仅局限对于车载CAN网络单个方面实现入侵检测,也应考虑如何检测T-Box通信模块、V2X通信协议等或其它车载网络的入侵。

4.2 如何构建基于车载网络IDS评估基准数据集

近年来,对于传统计算机IDS效果的评估,多数研究采用KDD CUP和DARPA等数据集作为评估基准。现阶段对于车载网络IDS的研究,虽然大多项研究使用的数据集据来源于真实的测试车辆,但部分研究所用的数据集并未公开,无法对比检测系统在不同攻击场景下的性能。因此,在未来的研究方向中,如何统一测试数据集来标准化地评估车载网络IDS的检测性能是未来研究中有待解决的问题。

4.3 如何提升车载网络IDS的检测性能

在未来的研究中应考虑如何提升车载网络IDS的检测性能,其中检测性能包括检测精度、检测时间和检测系统的鲁棒性等。目前,基于签名的车载网络IDS的检测精度较高,但该方法只能识别签名库中的已知攻击,需要人工对签名库进行更新。而机器学习算法在入侵检测领域彰显出优越的性能,是未来车载网络IDS研究的重要方向。基于机器学习的车载网络IDS方法通过训练数据所构建的检测模型来识别攻击,该方法可以检测到未知的攻击,对未知的数据有自适应能力。但传统的机器学习算法所占用的运算资源较高,在车载网络这种计算开销受限以及要求检测实时性高的场合中,应考虑如何提高检测算法的计算速度、降低检测响应时间是目前对车载网络IDS研究中亟待解决的重要问题。

5 结论

随着2015年《中国制造2025》的发布,智能网联车在我国将成为未来发展的重点。然而,智能化与网联化在推动汽车技术变革的同时,也带来了相应的网络安全问题。本文在此背景下,首先概述了当今汽车主要应用的车载网络类型,并讨论了现阶段智能网联汽车所面对的网络安全问题以及黑客对车载网络的攻击方式。随后,针对近几年车载CAN网络IDS的研究做了较全面的综述,总结了车载CAN网络入侵检测方法的研究现状。最后,本文对未来车载网络入侵检测方法的发展趋势提出了几项开放性问题。

参考文献

[1] 吴武飞,李仁发,曾刚,等.智能网联车网络安全研究综述[J].通信学报,2020,41(6):161-174.
WU W F, LI R F, ZENG G, et al. A review of the network security research of intelligent networked vehicles [J]. Journal of Communications, 2020, 41(6): 161-174.

[2] HAN S, XIE M, CHEN H H, et al. Intrusion detection in cyber-physical systems: techniques and challenges[J]. IEEE Systems Journal, 2014, 8(4):1049-1059.

[3] 李岩松.复杂网络环境下智能网联汽车安全威胁分析与远程入侵研究[D].西安:西安电子科技大学, 2019.
LI Y S. Security threat analysis and remote intrusion research of intelligent connected vehicles in complex network environment [D]. Xi'an: Xidian University, 2019.

[4] MILLER C, VALASEK C. Remote exploitation of an unaltered passenger vehicle[J]. Black Hat USA, 2015,1-91.

[5] The Institution of Engineering and Technology. Serious cyber-security flaws uncovered in ford and volkswagen Cars[R]. (2020-04-09)[2022-04-15].

[6] ELKHAIL A A, REFAT R U D, HABRE R, et al. Vehicle security: a survey of security issues and vulnerabilities, malware attack and defenses[J]. IEEE Access, 2021, 9: 162401-162437.

[7] GMIDEN M, GMIDEN M H, TRABELSI H. Cryptographic and intrusion detection system for automotive CAN bus: survey and contributions[C]. 2019 16th International Multi-Conference on Systems, Signals & Devices (SSD). Piscataway: IEEE Press, 2019:158-163.

[8] DIBAEI M, ZHENG X, JIANG K, et al. Attacks and defences on intelligent connected vehicles: a survey[J]. Digital Communications and Networks, 2021, 6(4):399-421.

[9] ZHANG J, JIN H, GONG L, et al. Overview of IoT security architecture[C]. 2019 4th International Conference on Data Science in Cyberspace (DSC). Piscataway: IEEE Press, 2019: 338-345.

[10] SLEVI S T, VISALAKSHI P. A survey on deep learning based intrusion detection systems on internet of things[C]. 2021 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC). Piscataway: IEEE Press, 2021: 1488-1496.

[11] ISO. Road vehicle-interchange of digital information-controller area network (CAN) for high-speed communication[S]. ISO 11898, (2015-12-01)[2022-4-15].

[12] KANG T U, SONG H M, JEONG S, et al. Automated reverse engineering and attack for CAN using OBD-II[C]. IEEE 88th Vehicular Technology Conference (VTC-Fall). Piscataway: IEEE Press, 2018:1-7.

[13] AVATEFIPOUR O, MALIK H. State-of-the-art survey on in-vehicle network communication "CAN-Bus" security and vulnerabilities[J]. arXiv Preprint, arXiv:1802.01725,2018.

[14] ZHANG C M, ZHOU W, YIN Y T, et al. Deterministic communications for in-vehicle network: overview and challenges[C].2021 2th International Conference on Artificial Intelligence and Information Systems. Association for Computing Machinery. New York: ACM Press, 2021:1-6.

[15] YU T Q, WANG X B. Topology verification enabled intrusion detection for in-vehicle CAN-FD networks[J]. IEEE Communications Letters, 2020, 24(1):227-230.

[16] TUOHY S, GLAVIN M, HUGHES C, et al. Intra-vehicle networks: a review[J]. IEEE Transactions on Intelligent Transportation Systems, 2014, 16(2):534-545.

[17] KOSCHER K, CZESKIS A, ROESNER F, et al. Experimental security analysis of a modern automobile[C].2010 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2010: 447-462.

[18] BHARATI S, PODDER P, MONDAL M R, et al. Threats and countermeasures of cyber security in direct and remote vehicle communication systems[J]. arXiv Preprint, arXiv: 2006.08723, 2020.

[19] 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.
YU H. Research on information security of connected vehicles and CAN bus anomaly detection technology [D]. Changchun: Jilin University, 2016.

[20] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces[C].Usenix Conference on Security. Berkeley: USENIX Association, 2011:6.

[21] Tencent Keen Security Lab. Experimental security assessment on Lexus cars[R].(2020-03-30)[2022-04-16].

[22] REGALADO D, IGLESIAS G, HSU K, et al. Zingbox identifies new cybersecurity threat for cars and drivers at defcon 26[R]. (2018-08-09)[2022-04-16].

[23] Privacy 4 Cars. Carsblues vehicle flaw found affectingmillions of vehicles worldwide[R]. (2018-11-15)[2022-04-16].

[24] Tencent Keen Security Lab. Exploit allowed hackers to take remote control of a tesla model S[R]. (2016-09-21)[2022-04-16].

[25] VANHOEF M, PIESSENS F. Denial-of-service attacks against the 4-way Wi-Fi handshake[C]. in Proc. 9th Int. Conf. Netw. Commun. Secur. Chennai, India: Academy & Industry Research Collaboration Center, 2017:1-10.

[26] ROUF I, MILLER R, MUSTAFA H, et al. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study[C]. 19th Usenix Security Symposium. Berkeley: USENIX Association, 2010: 11-13.

[27] 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 System, 2015, 16(2): 993-1006.

[28] ORUGANTI P S, APPEL M, AHMED Q. Hardware-in-loop based automotive embedded systems cybersecurity evaluation test-

bed[C]. Proceedings of the ACM Workshop on Automotive Cybersecurity. New York:ACM Press, 2019:41-44.

[29] BOZDAL M, SAMIE M, JENNISON I. A survey on CAN bus protocol: attacks, challenges, and potential solutions[C]. International Conference on Computing, Electronics & Communications Engineering. Piscataway: IEEE Press, 2018:201-205.

[30] NAVAZ A S S, SANGEETHA V, PRABHADEVI C. Entropy based anomaly detection system to prevent DDoS attacks in cloud [J]. arXiv Preprint, arXiv:1308.6745,2013.

[31] STUDNIA I, ALATA E, NICOMETTE V, et al. A language-based intrusion detection approach for automotive embedded networks[J]. International Journal of Embedded Systems, 2018, 10(1):1-12.

[32] JIN S Y, CHUNG J G, XU Y N. Signature-based intrusion detection system (IDS) for in-vehicle CAN bus network[C]. IEEE International Symposium on Circuits and Systems. Piscataway: IEEE Press, 2021:1-5.

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

[34] NING J, LIU J. An experimental study towards attacker identification in automotive networks[C].2019 IEEE Global Communications Conference. Piscataway: IEEE Press, 2019: 1-6.

[35] TIAN M Q, JIANG R B, XING C Q, et al. Exploiting temperature-varied ecu fingerprints for source identification in in-vehicle network intrusion detection [C]. 2019 IEEE 38th International Performance Computing and Communications Conference (IPCCC). Piscataway: IEEE Press, 2019:1-8.

[36] ZHAO Y L, XUN Y J, LIU J J. ClockIDS: a real-time vehicle intrusion detection system based on clock skew[J]. IEEE Internet of Things Journal. 2022, 9(17): 15593-15606.

[37] MUTER M, ASAJ N. Entropy-based anomaly detection for in-vehicle networks[C].IEEE Intelligent Vehicles Symposium. Piscataway: IEEE Press, 2011: 1110-1115.

[38] 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 H, QIN G H, SUN M H, et al. Vehicle CAN bus network security issues and anomaly detection methods [J]. Journal of Jilin University (Engineering Edition), 2016,46(4):1246-1253.

[39] MARCHETTI M, STABILI D, GUIDO A, et al. Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms[C].IEEE International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow. Piscataway: IEEE Press, 2016: 1-6.

[40] WU W F, HUANG Y, KURACHI R, et al. Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks[J]. IEEE Access, 2018, (6): 45233-45245.

[41] OHIRA S, DESTA A, ARAI I, et al. Normal and malicious sliding windows similarity analysis method for fast and accurate IDS against DoS attacks on in-vehicle networks[J]. IEEE Access, 2020, 8:42422-42435.

[42] ISLAM R, REFAT R U D, YERRAM S M, et al. Graph-Based intrusion detection system for controller area networks[J]. IEEE Transactions on Intelligent Transportation System, 2022, 23(3): 1727-1736.

[43] LING C L, FENG D Q. An algorithm for detection of malicious messages on CAN buses [C].Proceedings of 2012 National Conference on Information Technology and Computer Science. France: Atlantis Press, 2012, 10:124-127.

[44] LEE H, JEONG S, KIM H K, et al. OTIDS: a novel intrusion detection system for in-vehicle network by using remote frame[C]. Conference on Privacy Security and Trust. Piscataway: IEEE Press, 2017:57-66.

[45] STABILI D, MARCHETTI M, COLAJANNI M. Detecting attacks to internal vehicle networks through hamming distance[C]. AEIT International Annual Conference. Piscataway: IEEE Press, 2017: 1-6.

[46] TOMLINSON A, BRYANS J, SHAIKH S A, et al. Detection of automotive CAN cyber-attacks by identifying packet timing anomalies in time windows[C].48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks Workshops, Piscataway: IEEE Press, 2018:231-238.

[47] Hacking and Countermeasure Research Lab. CAN-intrusion-dataset (OTIDS)—Hacking and Countermeasure Research Lab[R]. (2017)[2022-05-21].

[48] NARAYANAN S N, MITTAL S, JOSHI A. OBD_securealert: an anomaly detection system for vehicles [C]. IEEE International Conference on Smart Computing. Piscataway: IEEE Press, 2016: 1-6.

[49] LEVI M, ALLOUCHE Y, KONTOROVICH A. Advanced analytics for connected car cybersecurity [C]. IEEE 87th Vehicular Technology Conference, Piscataway: IEEE Press. 2018:1-7.

[50] AVATEFIPOUR O, AL-SUMAITI A S, EL-SHERBEENY A M, et al. An intelligent secured framework for cyberattack detection in electric vehicles' CAN bus using machine learning[J]. IEEE Access, 2019, 7:127580-127592.

[51] MINAWI O, WHELAN J, ALMEHMADI A, et al. Machine learning-based intrusion detection system for controller area networks[C]. Proceedings of the 10th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications. New York:ACM Press, 2020:41-47.

[52] ALFARDUS A, RAWAT D B. Intrusion detection system for CAN bus in-vehicle network based on machine learning algorithms[C]. IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference. Piscataway: IEEE Press, 2021:0944-0949.

[53] SEO E, SONG H M, KIM H K, et al. GIDS: GAN based intrusion detection system for in-vehicle network[C]. Annual Conference on Privacy, Security and Trust, Piscataway: IEEE Press, 2018:1-6.

[54] Hacking and Countermeasure Research Lab. Car-Hacking dataset—hacking and countermeasure research Lab [R]. (2018) [2022-05-21].

[55] XIE G Q, YANG L T, LUO H B, et al. Threat analysis for automotive CAN networks: a GAN model-based intrusion detection technique [J]. IEEE Transactions on Intelligent Transportation Systems, 2021, 22(7):4467-4477.

[56] TAYLOR A, LEBLANC S, JAPKOWICZ N, et al. Anomaly detection in automobile control network data with long short-term memory networks[C]. IEEE International Conference on Data Science and Advanced Analytics. Piscataway: IEEE Press, 2016: 130-139.

[57] LONGARI S, VALCARCEL D H N, ZAGO M, et al. CANnolo: an anomaly detection system based on LSTM autoencoders for controller area network[J]. IEEE Transactions on Network and Service Management, 2021, 18(2):1913-1924.

[58] DING D F, ZHU L, XIE J Y, et al. In-vehicle network intrusion detection system based on Bi-LSTM[C]. 2022 7th International Conference on Intelligent Computing and Signal Processing (ICSP). Piscataway: IEEE Press, 2022:580-583.

[59] SONG H M, WOO J Y, KIM H K, et al. In-vehicle network intrusion detection using deep convolutional neural network[J]. Vehicular Communications, 2020, 21:100198.

[60] ARAI I, OHIRA S, FUJIKAWA K, et al. Rec-CNN: In-vehicle networks intrusion detection using convolutional neural networks trained on recurrence plots [J]. Vehicular Communications, 2022, 35:100470.

[61] LO W, ALQAHTANI H, THAKUR K, et al. A hybrid deep learning based intrusion detection system using spatial-temporal representation of in-vehicle network traffic[J]. Vehicular Communications, 2022, 35:100471.

[62] JAVED A R, REHMAN S U, KHAN M U, et al. CANintelliIDS: detecting in-vehicle intrusion attacks on a controller area network using CNN and attention-based GRU[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2):1456-1466.

[63] ZAGO M, LONGARI S, TRICARICO A, et al. ReCAN - dataset for reverse engineering of controller area net-works [J]. Data in Brief, 2020,29:105149.