车载网络入侵检测技术综述

童一帆，陈 涛，陈宇鹏

（中国汽车工程研究院股份有限公司，重庆 401122）

摘　要：智能网联汽车促进了交通运输的革新与发展，同时也伴生了网络安全问题，给用户的生命、财产造成了巨大的威胁。入侵检测技术作为一种轻量化的防御技术，能够通过建立的特征对攻击进行有效检测，从而完成对攻击的进一步分析与防御。从广泛使用的车载网络出发，调研了近年来针对常见攻击所提出的入侵检测技术，并对这些技术的特征与方法进行了划分，体现了不同技术之间的先进性与局限性，为车载网络入侵检测技术的研发提供了借鉴。

关键词：入侵检测；车载网络；流量；负载；深度学习

中图分类号：TP309；TP393　　**文献标志码：**A　　**DOI：**10.3969/j.issn.2095-1469.2022.05.01

Review on Intrusion Detection Technologies for Vehicular Networks

TONG Yifan，CHEN Tao，CHEN Yupeng

（China Automotive Engineering Research Institute Co.，Ltd.，Chongqing 401122，China）

Abstract: Intelligent connected vehicles have promoted the innovation and development of transportation; however, ICVs are challenged by network security issues. The intrusion detection technology, as a lightweight defense technology, includes effective detection based on the established features of attacks, further analysis and defense of the attack. This paper investigates the intrusion detection technologies to prevent common in-vehicle network attacks in recent years, classifies these technologies based on shared characteristics and methods, and compares the advantages and limitations of different technologies. The paper provides a reference for the research and development of in-vehicle network intrusion detection.

Keywords: intrusion detection; vehicular network; flow; payload; deep learning

现代汽车是由传感器、电子控制单元（Electronic Control Unit，ECU）和执行器组成的复杂系统，通过不同类型的车内网络连接来控制和监测车辆的状态。随着智能化、网联化的发展，汽车搭载了更多的ECU和外部通信接口，为用户提供智能网联服务和网络安全[1-3]。然而，随着汽车的复杂性和互联性的不断提高，且现有车载网络设计缺乏网络安全考虑，汽车的安全风险也日益突出。

网络安全问题正在成为车载网络系统的主要关注点[4-7]。数以百万计的汽车面临各种安全风险[8-10]，如2015年MILLER等[10]使用Wi-Fi开放端口侵入Jeep Cherokee的车载网络系统，并通过

收稿日期：2022-07-01　改稿日期：2022-08-10　网络首发日期：2022-09-09

参考文献引用格式：

童一帆，陈涛，陈宇鹏．车载网络入侵检测技术综述[J]．汽车工程学报，2022，12(5)：557-566.

TONG Yifan，CHEN Tao，CHEN Yupeng.Review on Intrusion Detection Technologies for Vehicular Networks[J].Chinese Journal of Automotive Engineering，2022，12(5)：557-566.(in Chinese)

重新编程 ECU 的固件成功控制了该车的核心功能（如禁用制动和停止发动机），导致 140 万辆汽车被召回。相关汽车攻击案例引发了对汽车网络安全的广泛研究。

目前，行业内各整车制造公司未普遍采用有效的安全技术手段来应对汽车安全风险。该现状对于黑客入侵行为无法进行有效的防护，从而导致车辆隐私数据或敏感数据的丢失，同时也会导致车辆行驶功能受到远程控制或破坏，对行车安全造成重大影响。入侵检测技术是应对这一情况的有效解决方案，该技术可以识别非法入侵行为，对车主或整车制造厂进行快速预警，车主或整车制造厂根据预警信息进行应急响应，将安全风险降到最低。

对车载网络的保护通常分为以下 3 类：（1）将消息帧进行加密确保其机密性和完整性[11]；（2）使用防火墙对潜在的危险接口进行监控[12]；（3）搭建车载网络入侵检测系统（Intrusion Detection System，IDS）[13]。

在上述分类中，不同的方法具有不同的优缺点。加密和认证的方式虽能有效保护车载网络的信息传输，但现有车载网络由于其自身在计算能力、带宽等方面的局限性[14]，导致这些方法无法被部署。例如，在计算机领域，对于通信连接普遍采用 3 次握手协议，握手成功后才进行有效信息传递。如果 CAN 总线引入该机制，对动力系统等发送实时性高的报文（10 ms）会造成重大延误，在车辆激烈驾驶过程中势必会引发功能安全问题，因此 CAN 总线不适合引入重安全机制。此外，车载网络的攻击入口分布在车机、网关、车身控制器等多个控制器上，且各控制器编译环境不同，有的控制器还采用了汽车专用操作系统，所以无法通过部署一套计算机领域常用的防火墙来完全隔离威胁和各种攻击源。

IDS 可部署在车载网络流量集中的控制器上，通过对车载网络报文的实时检测，能够有效识别异常报文和冗余报文，对车主和整车厂进行实时预警，车主和整车厂根据预警信息的程度，采取相应的应急解决措施，同时整车厂可根据预警信息，对未被入侵的车辆采取有效的补救方案，因此，IDS 技术的应用能够有效解决车载网络信息安全风险。

1 车载网络架构概述

现代车辆的典型架构集成了一组网络组件，包括传感器、执行器、ECU 和通信设备[15]。车内网络有助于传感器、ECU 和执行器之间的数据共享，从而实现车辆的运行。在现代车载通信系统中广泛使用的车载网络包括本地互连网络（Local Interconnect Network，LIN）、CAN、FlexRay、以太网和面向媒体的系统传输（Media Oriented System Transport，MOST）。表 1 对上述车载网络的特点进行了概括与比较。

表 1 车内网络类型与特点

网络类型	带宽/（bit·s^{-1}）	容错能力	介质访问控制机制	安全威胁	典型应用
LIN	11.2、19.6 K	低	轮询	低	电池检测、车窗升降等
CAN	125、500 K	低/中	CSMA/CA	高	发动机控制、电子稳定系统等
FlexRay	5、10 M	高	TDMA	中	安全雷达、动态悬架等
Ethernet	100 M	中/高	CSMA/CD	高	激光雷达、娱乐系统等
MOST	25、50、100 M	中	TMD/CSMA	中/高	信息娱乐系统、导航系统等

LIN 提供的低通信速度适用于时间性能要求不高的应用，如电池监控、车窗升降器控制等。如果要适用于对性能和带宽具有较高要求的应用，则需要增加系统成本，FlexRay、MOST 和以太网就是属于此种类型。例如，FlexRay 可用于转向角传感器、安全雷达等，以太网和 MOST 可用于信息娱乐系统[16]。在所有车载网络类型中，CAN 由于其较低成本、较全工具链、一定的抗噪与容错性成为

使用最广泛的车载网，尤其用于汽车动力系统、车身控制系统等[17-18]。然而，由于CAN的安全性不足而易受到安全威胁，本文所提到的大部分入侵检测技术都是基于CAN的。

CAN总线的传输速率可以达到125 Kbit/s及以上，其总线拓扑结构在传输电缆末端带有两个120 Ω的终端电阻。CAN总线上的节点在接收到消息时会与发送节点同步时间，因此不需要同步以规范通信。总线在空闲状态下，其上的每个节点都可以访问总线，并以广播的形式发送所要传输的信息[19]。对于接收消息的节点，其通过消息过滤器根据消息ID决定接收哪个消息。多个节点同时传输消息的情况下，需要通过载波侦听多路访问与冲突避免，以及消息优先级仲裁竞争对总线的访问，ID越小的消息具备的优先级越高。CAN消息帧格式示意如图1所示。

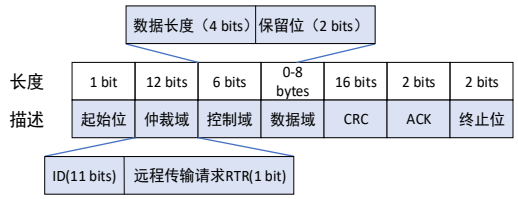

图1　CAN总线消息帧格式[20]

如图1所示，一个CAN帧由以下7个字段组成：

（1）起始位：通知所有节点开始传输的单个显性位。

（2）仲裁域：由2个主要部分组成；表示消息/帧的ID并在仲裁过程中使用的标识符字段，以及根据CAN帧的种类确定的远程传输请求（Remote Transmission Request，RTR）。

（3）控制域：有2个保留位和4个数据长度代码。

（4）数据域：保存传输到其他节点的实际数据。

（5）循环冗余校验（Cyclic Redundancy Check，CRC）：保证消息的有效性。收到消息的所有其他节点都使用此代码验证消息。

（6）确认字符（Acknowledge Character，ACK）：分为ACK部分和分隔符部分。接收到有效消息的节点用显性位（即逻辑0）替换作为隐性位（即逻辑1）的ACK部分。

（7）终止位：7个隐性位组成的标志，指示帧的结束。

2　车载网络攻击

智能网联汽车容易受到多种不同程度的网络攻击，从数据窃听到出行安全，甚至瘫痪整个交通系统[21]。一般来说，网络攻击可以分为两类：被动攻击和主动攻击。被动网络攻击（如窃听）主要违反目标系统安全的保密要求并导致隐私泄露（如对位置信息、对话数据和摄像头记录等隐私数据的访问）[22-23]。主动网络攻击可以通过插入、删除或修改消息来阻碍系统的功能[24]。通过对现有工作的回顾，车载网络的常见网络攻击阐述如下。

2.1　拒绝服务攻击

拒绝服务（Deny of Service，DoS）攻击旨在干扰系统的预期功能[25]。比较常见的DoS中，攻击者可能会发送许多合法请求，超出服务系统的处理能力，致使系统资源耗尽而无法响应其他合理请求。在车联网环境中，攻击者可以向路边单元（Road Side Unit，RSU）发送许多请求消息使RSU过载，这种情况下车辆无法获得该RSU所共享的重要消息，从而导致严重后果。CAN网络中的攻击者可以利用消息仲裁机制，不断发送具有高优先级的消息从而阻断其他ECU节点的消息传输。

2.2　消息注入和重放攻击

消息注入（MI）攻击的主要原理是在网络中注入伪造的消息，重放攻击是将之前的消息重新注入到网络中。在CAN网络中，攻击者可以控制某个ECU，并通过它将伪造的消息发送到CAN总线上；而重放攻击中则需要首先对之前的消息进行存储，然后再在某个时间点将原来的消息发送到CAN总线。例如，攻击者可以存储车速表读数并稍后将其再次广播到网络。

2.3　消息操纵

这种攻击通过更改/修改或删除消息来影响数

据的完整性。例如，攻击者可以修改消息的内容。攻击者可能会修改消息的内容而不影响其发送与接收时间。字段修改和删除攻击是消息操纵攻击的典型类型。在删除攻击中，攻击者先删除受感染的ECU并输出缓冲区中的消息，然后再将它们传输到CAN总线上。

2.4 伪装攻击

要发起伪装攻击，攻击者需要渗透两个ECU（A和B）。攻击者首先监视CAN总线以了解A以什么频率发送了哪些消息，然后停止A的传输并利用B代表A[26]制造和注入消息。

2.5 恶意软件攻击

恶意软件可能以病毒、蠕虫、间谍软件等多种形式存在，攻击者可以将它们利用通信接口的漏洞注入系统。例如，将恶意软件加入到多媒体文件中，并利用其多媒体系统固件输入漏洞实现恶意软件的运行，从而将恶意消息发送到CAN总线上[27]，以实现消息注入攻击、重放攻击、DoS等特定类型的攻击。

3 车载CAN网络IDS类型

近年来，汽车恶意攻击的数量有所增加。因此，车载网络安全问题越来越受到关注[28-29]。入侵检测技术作为一种网络安全增强方法，成本低，部署方便。

入侵检测依赖于观测的数据，在车载网络中主要是各节点（如ECU）之间交换的数据。例如，1条CAN消息，其具有固定的格式，包括消息ID、数据内容、校验码等，表示某个事件或过程。消息的时间戳或者数据范围都可以作为特征成为区分消息是否正常的依据，从而实现入侵检测。

一般而言，可以将数据集的特征分为两种类型：物理特征和网络特征。物理特征是指描述系统物理状态的特征（如速度、发动机转速），而网络特征是指描述系统通信和数据方面的特征（如消息数量、数据序列）。为了强化学习算法的辨别能力，需要剔除不相关的特征，所以精确地选择合理的特征不仅能够降低计算成本，对提高学习算法的泛化能力也具有重要意义。

通常将传统的IDS分为两类：基于签名的IDS和基于异常的IDS[30]。基于签名的IDS需要对已有攻击模式进行匹配[31]，如黑名单就是一种常见的基于签名的IDS。当观察到匹配的攻击模式时则报告入侵。由于基于签名的IDS只对已知的攻击进行报告，所以具有较低的误报率，但检测新攻击（如0-day攻击）的能力有限。为了能够抵御新型攻击，签名数据库需要保持最新。此外，存储大型签名数据库并对其执行模式匹配，对CPU、内存等资源的要求都比较高[32]。

基于异常的IDS对正常的系统行为进行建模，并将与正常系统行为有显著偏差的行为视为入侵[33]。该方法不必每次存储最新的攻击模式，且能够识别新型攻击，但是如果对正常系统的行为建模不精确容易产生误报。此外，正常系统行为的建模依赖于不受攻击的数据，而这些“纯净”数据在现实世界中并不一定能够获得。与基于签名的IDS相比，基于异常的IDS由于不需要存储签名，所以需要更少的内存即可满足要求[15]。

近年来，针对车载网络的入侵检测技术进行了大量研究[34-38]。从车载网络IDS设计的角度来看，其可以分为基于流量的IDS、基于负载的IDS和混合IDS。基于流量的IDS监控车辆的内部网络，并从中提取不同的特征（如消息频率和间隔）[39]。然后使用提取的特征来识别入侵或异常行为，而无需检查消息的有效负载；基于负载的IDS检查消息的负载以识别入侵；混合IDS是前两个类别的组合。针对上述分类，典型的车载网络入侵检测技术阐述如下。

3.1 基于流量的IDS技术

HOPPE等[40]通过分析车载网络的实际攻击案例，提出了基于异常的IDS跟踪特定目标消息类型的所有CAN消息，并评估当前的消息频率和之前的是否一致。此外，建议在检测到攻击时，在考虑周围环境条件的同时，所提出的系统能够自适应地

通过车辆的多媒体设备向驾驶员报告安全事件。

LING Congli 和 FENG Dongqin 基于 CAN 总线上传输的消息 ID 与其可中断的发生频率提出了一种 CAN 入侵检测算法 [41]。对于给定消息类型（即 ID），该算法会计算其连续消息的数量。如果可中断序列中的消息计数大于预定阈值，则算法会发出可能攻击的警报。该算法在检测操纵消息内容的同时保持其频率的攻击方面能力有限。

SONG 等 [42] 提出了一种基于 CAN 消息时间间隔统计分析的轻量级 IDS，主要原理是根据消息频率分析异常流量，从而用于检测注入攻击。在正常运行条件下，ECU 生成的消息有自己的固定频率或间隔。当车辆受到消息注入攻击时，这些频率或间隔会意外更改。试验表明，受到注入攻击的消息频率比正常情况高出 20～100 倍。

CHO 和 SHIN 构建了一个基于时钟的入侵检测系统（Clock-based Intrusion Detection System，CIDS），其可以检测包括伪装攻击在内的各种类型的攻击 [26]。由于 CAN 协议没有在 CAN 消息中提供发送器的身份，所以利用消息周期性来提取和估计发射器的时钟偏差，从而用于对发射 ECU 进行指纹识别。累计时钟偏移是通过将平均时钟偏移的绝对值相加得到的，根据定义，其斜率表示时钟偏移且是恒定的。这使所提出的 CIDS 能够根据到达时间戳估计时钟偏差，从而对消息发送器进行指纹识别以便进行入侵检测。

AVATEFIPOUR [43] 提出了一种基于机器学习的模型，该模型通过学习接收到的数据包的物理信号属性，将 CAN 数据包与其发送源进行“绑定”。所提取的物理信号特征向量由 11 个时域和频域统计信号属性组成，包括高阶矩、频谱合度、最小值、最大值和不规则性等属性，然后用于基于神经网络的分类器。试验结果表明，该模型对通道和 ECU 分类的正确检测率分别为 95.2% 和 98.3%。

基于熵的信息论方法也可以用来检测车载网络的消息注入、DoS 等攻击 [44-45]。相比于传统的计算机网络，车载网络中的流量更受限制，因为每条消息及其内容都是在传输之前指定的。这意味着正常网络操作中数据的熵（即不确定性）几乎是固定的并且相对较低。因此，通过观察熵值可以很容易地检测到改变数据熵的入侵。例如，MI 攻击会降低熵值，因为特定消息的数量会增加。因此，IDS 可以通过检测熵的变化来判断是否存在攻击的指标。

由上文可知，基于流量型的 IDS 技术可有效识别特定数据包和频率的异常情况，对于传统 CAN 总线网络适用性更强，同时实时性好。但是对于面向服务的车载网络，由于服务信号可以根据服务需求进行变更，那么基于流量型的 IDS 技术则很难对新增的服务信号做出响应，也无法发现新增服务信号的篡改等风险，所以该技术有其局限性。

3.2　基于负载的 IDS 技术

BEZEMSKIJ 等 [46] 通过监控车辆的不同车载资源（如传感器、网络和处理）的实时网络和物理特征实现入侵检测，分为学习阶段和检测阶段。在学习阶段，将车辆学习特征的正常值范围作为正常行为配置文件。在检测阶段，如果某个特征的观察值超出其正常范围，则检测机制会报告攻击。所提出的机制能够检测信息注入攻击和伪装攻击。

MARKOVITZ 等 [47] 通过一个分类器将 CAN 消息拆分为字段并识别字段类型及其边界，而无需事先了解消息格式。由此可知存在 3 类场：常数场、多值场和计数器或传感器场。然后，检测系统根据从分类器获得的 ECU 消息的特征（即字段类型和边界）为每个 ECU 构建模型。该模型基于三元内容可寻址存储器（Ternary Content Address Memory，TCAM）对 ECU 发送的消息进行匹配，任何与 TCAM 不匹配的消息都被标记为异常。

STABILI 等 [48] 基于不同 ID 类别的连续有效载荷之间的汉明距离提出了一种入侵检测算法。在学习阶段，为提出的算法建立了一个正常范围的有效汉明距离。然后，它分析通过 CAN 总线传输的所有消息的有效载荷序列，并将相同 ID 的连续有效载荷之间的汉明距离与有效汉明距离的正常范围进行比较。试验结果表明，所提出的算法在检测消息注入攻击时效果较好。

KANG 等[49]提出了一种基于深度神经网络（Deep Neural Networks，DNN）的 IDS。检测模型是基于从 ECU 之间交换的车载网络数据包的比特流中提取的高维特征进行训练。一旦特征被训练并存储在分析模块中，所提出的系统就会检查车辆网络中交换的数据包，以确定系统是否受到攻击。由于神经网络的前向计算模式简单且固定，所以所提出的系统在检测异常时具有较低的延迟。

由上文可知，基于负载的 IDS 技术普遍引入机器学习机制来完成正常样本的识别，该技术的普适性较强，无需对适配车型进行定制化开发。但是其存在机器学习的普遍问题，即正常样本和异常样本采集问题，特别是异常样本数量巨大，学习难度较高。因此，该技术如何获取大量样本来进行学习是应用该技术的门槛。

3.3 混合类型的 IDS 技术

JIN Shiyi 等[50]分别根据流量选择消息 ID、时间间隔作为特征，根据负载选择数据范围以及相关性作为特征，从而提出了一种混合类型的 IDS。该 IDS 作为一种轻量级 IDS 可以直接应用到 ECU 上，避免了车载网络拓扑的更改开销，因此在汽车架构没有发生大规模改变的阶段存在一定的应用前景。

MÜTER 等[51]引入了一组检测传感器：形式传感器、位置传感器、距离传感器、频率传感器、相关传感器、协议传感器、似真性传感器和一致性传感器。这些检测传感器基于明确且可靠的信息，所以在检测异常时不会产生误报。尽管这些传感器可用于检测攻击而不会误报，但并非所有攻击都可以被这些传感器检测到。例如，如果攻击者能够注入完全符合网络正常行为且与先前值合理的消息。此外，当检测到异常时很难确定其是由攻击、错误还是故障引起的。

BERLIN 等[52]引入了一个安全信息和事件管理系统（Security Information and Event Management，SIEM），其使用是基于规则、机器学习、深度学习、基于实时、安全和大数据的算法，通过车辆的数据和其他来源的附加信息（如来自第三方和服务的数据）来识别攻击。

ZHANG Linxi 等[53]提出了一种基于规则和深度学习的两阶段 IDS 来实时检测攻击。在第 1 阶段，轻量级基于规则的 IDS 可以快速检测违反主要 CAN 流量的周期性和规律性的攻击，而基于 DNN 的 IDS 会从基于规则的系统中捕获错过的攻击，试验表明该系统可以检测 5 种类型的攻击，包括消息注入、伪装、重放、删除或丢弃攻击，在增加检测准确性的同时降低了检测时延。

彭海德[54]提出了一种基于 ID 熵和支持向量机–数据关联性的 IDS 检测技术，针对 CAN 周期性消息，建立白名单与熵相结合的检测机制，针对非周期消息，建立了数据域与车辆状态相结合的数据关联检测技术，从而实现对重放、DoS、丢弃（删除）攻击的检测。

KWON 等[55]结合车载网络 IDS 提出了一种减轻入侵危害的方法，其主要是通过将受攻击的 ECU 进行重新配置，或者将检测到的恶意消息通知特定域的 ECU 进行丢弃。

SUDA 等[56]提出了一种基于时间序列特征提取的车载网络入侵检测方法以检测 ID 修改攻击、数据字段修改攻击和洪泛攻击。其主要是将消息 ID、数据字段以及消息帧间隔统一放到递归神经网络中进行训练，从而达到识别异常或者攻击的目的。NAM 等[57]利用类似的思想基于生成式的预训练模型提取面向时间序列的 ID 特征以检测入侵。

HE Yuchu 等[58]基于深度学习方法，在考虑车载网络流量与负载的基础上，增加了临近消息的关系特征并给不同的特征分配相应的权重以增加入侵检测的效率。

混合类型的 IDS 技术融合了基于流量的 IDS 和基于负载的 IDS 的优点，既能对选定的报文进行快速识别，同时又具备学习能力，可以学习新报文。但是受限于车辆整体成本，IDS 部署的控制器算力和存储空间普遍无法支撑混合类型的 IDS 技术，如何降低混合类型的 IDS 技术资源使用，是该技术能够进行广泛使用的前提条件。

4 结论

随着汽车智能化与网联化的发展，车载网络在功能运转、信息交互、状态显示等方面发挥着巨大作用，随之而来的网络安全威胁更加突出。入侵检测技术作为一种被动防御技术，具有低开销、应用广等特点，能够有效收集并检测潜在的车载网络安全攻击。从对车载网络入侵检测技术的调研来看，车载网络入侵检测技术主要分为基于流量的和基于负载的两大类，不同类型的技术在成本开销、应用场景以及效果等方面具有较大差异，因此需要根据实际情况设计车载网络入侵检测系统。特别是随着入侵检测技术不断成熟，可以在原有技术的基础上增加隔离措施，不仅仅局限于预警，提前将相关物理功能进行区域化管制，及时处置风险，这是入侵检测技术的新发展方向。

参考文献（References）

[1] LIU Chunhua，CHAU K T ，WU Diyun，et al .Opportunities and Challenges of Vehicle-to-Home，Vehicle-to-Vehicle，and Vehicle-to-Grid Technologies[J]. Proceedings of the IEEE ，2013 ，101(11)：2409-2427.

[2] 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.

[3] LIU Jizheng，WANG Zhenpo，ZhANG Lei. Integrated Vehicle-Following Control for Four-Wheel-Independent-Drive Electric Vehicles Against Non-Ideal V2X Communication [J]. IEEE Transactions on Vehicular Technology，2022，71(4)：3648-3659.

[4] KOSCHER K，CZESKIS A，ROESNER F，et al. Experimental Security Analysis of a Modern Automobile [C]//2010 IEEE Symposium on Security and Privacy，May 16-19，2010 ，Oakland，CA，USA. Piscataway NJ：IEEE，c2010：447-462.

[5] MILLER C，VALASEK C.A Survey of Remote Automotive Attack Surfaces [J]. Black Hat USA，2014，2014：1-94.

[6] FRÖSCHLE S，StüHRING A. Analyzing the Capabilities of the CAN Attacker [C]// European Symposium on Research in Computer Security. Springer，Cham，2017：464-482.

[7] 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，2014，16(2)：993-1006.

[8] PETIT J，SHLADOVER S E. Potential Cyberattacks on Automated Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems，2014，16(2)：546-556.

[9] SINGH M，KIM S. Security Analysis of Intelligent Vehicles：Challenges and Scope [C]// 2017 International SoC Design Conference (ISOCC). IEEE，2017：13-14.

[10] MILLER C，VALASEK C. Remote Exploitation of an Unaltered Passenger Vehicle [J]. Black Hat USA，2015，2015：1-91.

[11] BULCK J V，MÜHLBERG J T，PIESSENS F. VulCAN：Efficient Component Authentication and Software Isolation for Automotive Control Networks [C]//Proceedings of the 33rd Annual Computer Security Applications Conference. 2017：225-237.

[12] MACHER G，SPORER H，BRENNER E，et al. An Automotive Signal-Layer Security and Trust-Boundary Identification Approach [J]. Procedia Computer Science，2017，109：490-497.

[13] QIU Bin，CHEN Ke，HE Kexun，et al. Research on Vehicle Network Intrusion Detection Technology Based on Dynamic Data Set [C]//2021 IEEE 3rd International Conference on Frontiers Technology of Information and Computer (ICFTIC)，Nov. 12-14，2021，Greenville，SC，USA. Piscataway NJ：IEEE，c2021：386-390.

[14] CHAKRABORTY S，AL FARUQUE M A，CHANG Wanli，et al. Automotive Cyber-Physical Systems：A Tutorial Introduction [J]. IEEE Design & Test，2016，33(4)：92-108.

[15] HAN Song，XIE Miao，CHEN H H，et al. Intrusion Detection in Cyber-Physical Systems：Techniques and Challenges [J]. IEEE Systems Journal，2014，8(4)：1052-1062.

[16] ZENG Weiying，KHALID M A S，CHOWDHURY S. In-Vehicle Networks Outlook：Achievements and Challenges [J]. IEEE Communications Surveys & Tutorials，2016，18(3)：1552-1571.

[17] SUN H，LEE S Y，JOO K，et al. Catch ID if You CAN：Dynamic ID Virtualization Mechanism for the Controller

Area Network［J］. IEEE Access，2019，7：158237-158249.

［18］YE Jin，GUO Lulu，YANG Bowen，et al. Cyber-Physical Security of Powertrain Systems in Modern Electric Vehicles：Vulnerabilities，Challenges，and Future Visions［J］. IEEE Journal of Emerging and Selected Topics in Power Electronics，2020，9(4)：4639-4657.

［19］HAFEEZ A，TOPOLOVEC K，AWAD S.ECU Fingerprinting Through Parametric Signal Modeling and Artificial Neural Networks for In-Vehicle Security Against Spoofing Attacks［C］// 2019 15th International Computer Engineering Conference（ICENCO），Dec. 29-30，2019，Cairo，Egypt. Piscataway NJ：IEEE，c2019：29-38.

［20］崔晓通，陈宇鹏，张亮，等. 车载以太网类型及测试［J］. 西安：西安邮电大学学报，2020，25(4)：90-96.
CUI Xiaotong，CHEN Yupeng，ZHANG Liang，et al. A Survey on Automotive Ethernet Testing Framework and Technologies［J］. Xi'an：Journal of Xi'an University of Posts and Telecommunications，2020，25(4)：90-96.（in Chinese）

［21］ELKHAIL A A，REFAT R U D，HABRE R，et al. Vehicle Security：A Survey of Security Issues and Vulnerabilities，Malware Attacks and Defenses［J］. IEEE Access，2021，9：162401-162437.

［22］KLEBERGER P，OLOVSSON T，JONSSON E. Security Aspects of the In-Vehicle Network in the Connected Car［C］// 2011 IEEE Intelligent Vehicles Symposium（IV），June 5-9，2011，Baden-Baden，Germany. Piscataway NJ：IEEE，c2011：528-533.

［23］SCHWEPPE H，ROUDIER Y. Security and Privacy for In-Vehicle Networks［C］//2012 IEEE 1st International Workshop on Vehicular Communications，Sensing，and Computing（VCSC），June 18，2012，Seoul，Korea（South）. Piscataway NJ：IEEE，c2012：12-17.

［24］KANG D M，YOON S H，SHIN D K，et al. A Study on Attack Pattern Generation and Hybrid MR-IDS for In-Vehicle Network［C］//2021 International Conference on Artificial Intelligence in Information and Communication（ICAIIC）. IEEE，c2021：291-294.

［25］JAVED A R，UR REHMAN S，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.

［26］CHO K T，SHIN K G. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection［C］// 25th USENIX Security Symposium（USENIX Security 16）. 2016：911-927.

［27］LUO Qian，LIU Jiajia. Wireless Telematics Systems in Emerging Intelligent and Connected Vehicles：Threats and Solutions［J］. IEEE Wireless Communications，2018，25(6)：113-119.

［28］ZHANG Yanyan，LIU Tianyu，ZHAO Hao，et al. Risk Analysis of CAN Bus and Ethernet Communication Security for Intelligent Connected Vehicles［C］//2021 IEEE International Conference on Artificial Intelligence and Industrial Design（AIID），May 28-30，2021，Guangzhou，China. Piscataway NJ：IEEE，c2021：291-295.

［29］谢浒. 基于机器学习的车载CAN网络入侵检测研究［D］. 天津：天津理工大学，2021.
XIE Hu. Research on Intrusion Detection of In-Vehicle CAN Network Based on Machine Learning［D］. Tianjin：Tianjin University of Technology，2021.（in Chinese）

［30］MITCHELL R，CHEN I R. A Survey of Intrusion Detection Techniques for Cyber-Physical Systems［J］. ACM Computing Surveys（CSUR），2014，46(4)：1-29.

［31］TIAN Miaoqing，JIANG Ruobing，XING Chaoqun，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）. IEEE，2019：1-8.

［32］ALDWAIRI M，ABU-DALO A M，JARRAH M. Pattern Matching of Signature-Based IDS Using Myers Algorithm Under MapReduce Framework［J］. EURASIP Journal on Information Security，2017(1)：1-11.

［33］CHEN Mingqiang，ZHAO Qingling，JIANG Zhe，et al. Intrusion Detection for In-Vehicle CAN Networks Based on Auxiliary Classifier GANs［C］//2021 International Conference on High Performance Big Data and Intelligent Systems（HPBD&IS），Dec. 5-7，2021，Macau，China. Piscataway NJ：IEEE，c2021：186-191.

［34］GMIDEN M，GMIDEN M H，TRABELSI H. An Intrusion Detection Method for Securing In-Vehicle CAN Bus［C］//2016 17th International Conference on Sciences and Techniques of Automatic Control and Computer Engineering（STA），Dec. 19-21，2016，Sousse，Tunisia.

Piscataway NJ：IEEE，c2016：176−180.

[35] CHENG Anyu，PENG Yibo，YAN Hao，et al. An Intrusion Detection Method for the In-Vehicle Network [C]//2021 33rd Chinese Control and Decision Conference（CCDC），May 22−24，2021，Kunming，China. Piscataway NJ：IEEE，c2021：4893−4899.

[36] DING Defeng，ZHU Lu，XIE Jjiaying，et al. In-Vehicle Network Intrusion Detection System Based on Bi-LSTM [C]// 2022 7th International Conference on Intelligent Computing and Signal Processing（ICSP），April 15−17，2022，Xi'an，China. Piscataway NJ：IEEE，c2022：580−583.

[37] ALFARDUS A，RAWAT D B.Intrusion Detection System for CAN Bus In-Vehicle Network Based on Machine Learning Algorithms [C]//2021 IEEE 12th Annual Ubiquitous Computing，Electronics & Mobile Communication Conference（UEMCON），Dec. 1−4，2021，New York，NY，USA.Piscataway NJ：IEEE，c2021：944−949.

[38] 彭一波. 入侵检测系统在车载CAN网络中的设计与实现 [D]. 重庆：重庆邮电大学，2021.
PENG Yibo. Design and Implementation of Intrusion Detection System for In-Vehicle CAN Network [D]. Chongqing：Chongqing University of Posts and Telecommunications，2021.（in Chinese）

[39] BALDINI G. Intrusion Detection Systems in In-vehicle Networks Based on Bag-of-Words [C]// 2021 5th Cyber Security in Networking Conference（CSNet），Oct. 12−14，2021，Abu Dhabi，United Arab Emirates. Piscataway NJ：IEEE，c2021：41−48.

[40] HOPPE T，KILTZ S，DITTMANN J. Applying Intrusion Detection to Automotive It—Early Insights and Remaining Challenges [J]. Journal of Information Assurance and Security（JIAS），2009，4(6)：226−235.

[41] LING Congli，FENG Dongqin. 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.

[42] SONG H M，KIM H R，KIM H K. Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In-Vehicle Network [C]// 2016 International Conference on Information Networking（ICOIN），Jan. 13−15，2016，Kota Kinabalu，Malaysia. Piscataway NJ：IEEE，c2016：63−68.

[43] AVATEFIPOUR O. Physical-Fingerprinting of Electronic Control Unit（ECU）Based on Machine Learning Algorithm for In-Vehicle Network Communication Protocol "CAN-BUS" [D]. Michigan，USA：The University of Michigan-Dearborn，2017.

[44] MÜTER M，ASAJ N.Entropy-Based Anomaly Detection for In-Vehicle Networks [C]//2011 IEEE Intelligent Vehicles Symposium（IV），June 5−9，2011，Baden-Baden，Germany. Piscataway NJ：IEEE，c2011：1110−1115.

[45] MARCHETTI M，Stabili D，Guido A，et al. Evaluation of Anomaly Detection for In-Vehicle Networks Through Information-Theoretic Algorithms [C]// 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow（RTSI），Sept. 7−9，2016，Bologna，Italy. Piscataway NJ：IEEE，c2016：1−6.

[46] BEZEMSKIJ A，LOUKAS G，ANTHONY R J，et al. Behaviour-Based Anomaly Detection of Cyber-Physical Attacks on a Robotic Vehicle[C]//2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security（IUCC-CSS），Dec. 14−16，2016，Granada，Spain. Piscataway NJ：IEEE，c2016：61−68.

[47] MARKOVITZ M，WOOL A. Field Classification，Modeling and Anomaly Detection in Unknown CAN Bus Networks[J].Vehicular Communications，2017，9：43−52.

[48] STABILI D，MARCHETTI M，COLAJANNI M. Detecting Attacks to Internal Vehicle Networks Through Hamming Distance [C]//2017 AEIT International Annual Conference，Sept. 20−22，2017，Cagliari，Italy. Piscataway NJ：IEEE，c2017：1−6.

[49] KANG M J，KANG J W. A Novel Intrusion Detection Method Using Deep Neural Network for In-Vehicle Network Security[C]//2016 IEEE 83rd Vehicular Technology Conference（VTC Spring），May 15−18，2016，Nanjing，China. Piscataway NJ：IEEE，c2016：1−5.

[50] JIN Shiyi，CHUNG J G，XU Yinan. Signature-Based Intrusion Detection System（IDS）for In-Vehicle CAN Bus Network [C]// 2021 IEEE International Symposium on Circuits and Systems（ISCAS），May 22−28，2021，Daegu，Korea. Piscataway NJ：IEEE，c2021：1−5.

[51] MÜTER M，GROLL A，FREILING F C. A Structured Approach to Anomaly Detection for In-Vehicle Networks

[C]//2010 Sixth International Conference on Information Assurance and Security, Aug. 23-25, 2010, Atlanta, GA, USA. Piscataway NJ: IEEE, c2010: 92-98.

[52] BERLIN O, HELD A, MATOUSEK M, et al. POSTER: Anomaly-Based Misbehaviour Detection in Connected Car Backends [C]// 2016 IEEE Vehicular Networking Conference (VNC), Dec. 8-10, 2016, Columbus, OH, USA. Piscataway NJ: IEEE, c2016: 1-2.

[53] ZHANG Linxi, SHI L, KAJA N, et al. A Two-Stage Deep Learning Approach for CAN Intrusion Detection [C]// Proceedings of the 2018 Ground Vehicle Systems Engineering and Technology Symposium (GVSETS), Aug. 7-9, 2018, Novi, Michigan. 2018: 1-11.

[54] 彭海德. 汽车CAN网络的入侵检测方法研究 [D]. 大连: 大连理工大学, 2021.
PENG Haide. Research on Intrusion Detection Method of Automobile CAN Network [D]. Dalian: Dalian University of Technology, 2021. (in Chinese)

[55] KWON H, LEE S, CHOI J, et al. Mitigation Mechanism Against In-Vehicle Network Intrusion by Reconfiguring ECU and Disabling Attack Packet [C]//2018 International Conference on Information Technology (InCIT), Oct. 24-26, 2018, Khon Kaen, Thailand. Piscataway NJ: IEEE, c2018: 1-5.

[56] SUDA H, NATSUI M, HANYU T. Systematic Intrusion Detection Technique for an In-Vehicle Network Based on Time-Series Feature Extraction [C]// 2018 IEEE 48th International Symposium on Multiple-Valued Logic (ISMVL), May 16-18, 2018, Linz, Austria. Piscataway NJ: IEEE, c2018: 56-61.

[57] NAM M, PARK S, KIM D S. Intrusion Detection Method Using Bi-Directional GPT for In-Vehicle Controller Area Networks [J]. IEEE Access, 2021, 9: 124931-124944.

[58] HE Yuchu, JIA Zhijuan, HU Mingsheng, et al. The Hybrid Similar Neighborhood Robust Factorization Machine Model for CAN Bus Intrusion Detection in the In-Vehicle Network [J]. IEEE Transactions on Intelligent Transportation Systems, 2021: 1-9.

作者简介

童一帆（1986-），男，湖南长沙人，硕士，主要研究方向为新能源与智能网联汽车安全。
Tel：18618339797
E-mail：tongyifan@caeri.com.cn

通信作者

陈宇鹏（1983-），男，吉林桦甸人，博士，主要研究方向为汽车网络与数据安全，人工智能方向的安全问题。
Tel：13843014675
E-mail：chenyupeng@caeri.com.cn