车联网威胁分析和入侵检测关键技术

Key Technologies of Threat Analysis and Intrusion Detection of Internet of Vehicles

★ 朱鹏程，涂江健，招志才，尚文利，曹忠，浣沙，张曼 广州大学

摘要： 汽车产业为追求更佳的舒适性、便捷性、安全性等其他特性，正不断向智能化和网联化快速转变。车联网高速发展的同时，其自身的安全问题也日渐突出。本文阐述了车联网安全架构，并分析架构各层级面临的主要安全威胁。针对主要安全威胁，总结国内外车联网入侵检测技术的研究现状。最后，分析了当前入侵检测的关键技术，提出了未来研究方向和思路，为我国车联网安全的发展提供理论和技术参考。

关键词： 车联网安全；车载网络；安全威胁；入侵检测

Abstract: The automotive industry is rapidly changing towards intelligence and connectivity in pursuit of better comfort, convenience, safety and other features. The rapid development of Telematics is accompanied by its own security issues. This paper describes the security architecture of telematics and analyses the main security threats faced by each level of the architecture. To address the main security threats, the research status of domestic and international Telematics intrusion detection technologies is summarized. Finally, the key technologies of current intrusion detection are analyzed, and future research directions and ideas are proposed to provide theoretical and technical references for the development of Internet of vehicles security in China.

Key words: Internet of vehicles security; Vehicle network; Security threats; Intrusion detection

1 引言

当前，物联网被视作继互联网之后的又一次信息技术革命浪潮，万物互联将是未来社会的发展趋势。汽车产业作为“万物互联”中的重要板块，为追求更佳的舒适性、便捷性、安全性等其他特性，正不断向智能化、网联化、数字化快速转变。汽车互联网的诞生，借助了新一代移动通信技术，实现车与人、车与车、车与路、车与云等全方位的网络连接，提升用户驾驶体验的同时，极大地提高交通运行效率及交通服务的智能化水平。

日本早在20世纪60年代，首先开启了车内网络的研究。美国在2010年发布了《智能交通战略研究计划》，为车联网技术的发展进行了详细的规划和部署。如今，我国的智能网联汽车的发展也已提升至国家战略高度，国务院和工业信息化部、交通运输部、科学技术部、发展改革委、公安部等部委均出台一系列规划及政策推动我国智能网联汽车产业发展。

在车联网高速发展的同时，车载网络开放性不断提高，面临的信息安全威胁也随之增大，车联网安全事故不断涌现。本文介绍了车载网络安全的架构，从架构出发，分析各结构主要安全威胁。总结了国内外车联网入侵检测的研究现状，并结合前沿技术，指出车联网入侵检测关键技术创新点，为我国车联网安全的发展提供理论和技术参考。

2 车联网架构

典型的车联网定义是指汽车结合高精度、高可靠性且低时延的传感器技术与新一代的移动通信技术，实现车辆内部与车辆外部人、车、路、云、端全方位的网络连接。从车联网安全威胁角度，李兴华等人在《车联网安全综述》中将车联网架构划分为车外网通信层、车内平台网络层和车内组件层[1]。

（1）车外网通信层：由车-车、车-人、车-路、车-云之间通信组成的网络层。其中包括了智能网联汽车相互之间通过LTE-V2X、DSRC（Dedicated Short Range Communication）的通信，车与路基设施之间通过LTE-V2X、DSRC、射频技术的通

信，以及车与人之间通过Wi-Fi、蓝牙或蜂窝网的通信。V2X网络通信中，首先T-BOX作为无线网关，通过4G远程无线通讯、GPS卫星定位、加速度传感和CAN（Controller Area Network）通讯等功能，为整车提供远程通讯接口，包括了行车数据采集、行驶轨迹记录、车辆故障监控、车辆远程查询和控制、驾驶行为分析等服务。其次，车辆可以通过IVI从车外网中获取娱乐信息服务，包括三维导航、实时路况、IPTV、辅助驾驶、无线通讯等一系列应用。最后，车辆还可以通过OBD II系统直接与汽车故障诊断仪器相接通，进行信息交换。故T-BOX、IVI或网关作为车内网与车外网通信的关键节点。

（2）车内平台网络层：车内平台的网络架构是通过总线通讯协议将ECU（Electronic Control Unit）节点连接起来，从而构成车内总线网络。ECU作为智能网联汽车的核心电子元件，也是车内基本通讯单元，相互之间通过总线协议连接。车内总线协议主要包括CAN、LIN、FlexRay、MOST等，如图1所示。而在众多总线协议中，CAN作为目前运用最广泛的车内总线协议，是车联网安全领域研究的重点。

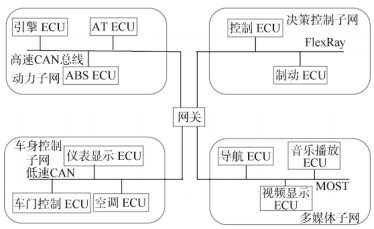

图1 车内总线协议

（3）车内组件层：随着车辆智能化程度越来越高，智能网联汽车内部部署的高性能传感器和ECU数量也随之不断增长。ECU作为汽车每个子系统的“大脑”，通过独有的软硬件系统，单独或多个ECU组合控制着不同的功能。而车内数量庞大的传感器和ECU共同构成了车内的组件层，通过实时通信控制着整车。

3 车联网威胁分析

具有典型性和先进性的车联网相较于传统的互联网，应用环境相较特殊，组网更加复杂，管理更具困难，安全威胁也更为严峻。存在车辆被远程攻击、恶意控制、个人信息泄露等威胁。其影响程度从车内娱乐系统的播放到车辆被恶意操控造成重大交通安全事故，甚至到泄露出行信息、道路信息、地图信息等对国家安全造成威胁。本文从车外网通信层、车内平台网络层、车内组件层三个方面分析车联网存在的主要信息安全威胁。

（1）车外网通信层威胁

由于V2X通信网络采用无线通信方式，故通信过程中存在网络入侵，消息篡改、伪造，通信协议破解，身份认证等威胁。车与人或云端之间传递的信息往往蕴含大量驾驶人员隐私，车辆注册、状态、轨迹信息等，因此车外网络通信层中数据的安全尤为重要。李馥娟等人在《车联网安全威胁综述》中提出，车辆通信数据具有体量大、模态多和实时性高的特点[2]。数据内容本身具有敏感性，同时必须保障通信数据的实时性与真实性。在确保网络通信质量的前提下，谨防数据被篡改。

入侵者攻击通信层的方式多种多样，车外网通信层主要存在的攻击面有：蓝牙车钥匙、OBD口、Wi-Fi、TSP、移动端应用App、车联网云端及相互通信的信道等。攻击手段主要通过对通信协议的先验知识，伪造报文对车辆进行入侵。而高效且匿名的身份认证技术是关键，但由于实时性、算力的限制，传统基于椭圆曲线公钥密码学认证等方法应用于车联网存在较大困难。此外，由于车辆的高速移动，其网络拓扑结构为动态变化，车外网络中未知攻击的入侵检测亦面临较大困难。

（2）车内平台网络层威胁分析

CAN总线是由国际标准化组织（International Organization for Standardization，ISO）定义的串行通信总线，是一种广播式车辆总线，用高总线和低总线连接电子控制单元。近年随着车辆上的联网设备越来越丰富，CAN总线规模不断扩大，车内平台网络层的入侵主要集中在CAN总线上。但是，在最初设计CAN总线时，汽车是一个独立的工具，没有考虑到车与车、车与路、车与云之间的连接与通讯，故CAN总线的设计并没有信息安全方面的防御设计，因此CAN总线

具有如下特性:

· 明文传输：CAN总线在通讯时是采用明文传输的，使得攻击者能够较容易获取CAN总线上传输的数据，并且较容易地读懂其内所包含的信息，借此可以对CAN总线进行消息注入甚至从而控制车辆。

· 无认证机制：CAN总线的消息帧数据量很小，缺乏帧溯源，消息帧内不含任何发送节点的相关信息亦不存在任何签名机制，故在接收到CAN总线传来的数据时，无法对消息帧进行溯源，即使知道某段消息是恶意注入的，也没法因此判断出攻击在何处发生。

· 广播传输：CAN总线采用广播传输的方式进行通信，即假若攻击者对其中一个节点进行入侵，便可轻松获取全部的CAN总线信息。

· 消息优先级仲裁机制：当多个ECU发送消息到CAN总线时，CAN总线会对其优先级进行判断，优先执行优先级更高的指令。所以攻击者可以通过向CAN总线发送大量高优先级的消息，使原本的系统功能完全瘫痪。

（3）车内组件层威胁分析

车内组件层的威胁主要来自于ECU的安全漏洞，ECU中的漏洞包括软件漏洞和固件漏洞。ECU的软件漏洞可以导致系统崩溃、重启或执行非预期功能。其中一些漏洞提供了缓冲区溢出攻击的机会。攻击者利用这些软件漏洞，干扰ECU的正常工作，导致ECU崩溃或者执行攻击者提供的恶意代码，打乱系统的执行流程。对于固件漏洞来说，攻击者可以通过外部设备对ECU的固件进行逆向分析，获得其指令集代码、更改ECU相关参数、挖掘ECU固件漏洞。当读取固件时，可以通过二进制数据中的字符串得到ECU的类型，进而知道ECU采用的指令集类型。通过一些工具如banal、Windows等可以得到一些关键函数和MAP表，并实现MAP数据的编辑和校验。不同种类的ECU会带来不同的漏洞安全问题。

4　国内外车联网入侵检测技术研究现状

（1）车外网通信层入侵检测技术研究现状

车外网的通信与传统无线通信较为相似，但由于车辆的高速移动，网络拓扑存在动态变化的特点。车辆与外部车辆、TSP、路基设备等需要不断建立网络、离开网络，分组网络中具备强信任关系的同时保障不受组内攻击。故基于传统互联网的入侵检测技术应用于车联网时需针对性改进。当前主要思想仍是基于深度学习的算法对网络中各节点的流量特征进行分析，基于大量训练集监控当前网络流量，判断入侵行为。

通过采用不同的机器学习模型，以建立可靠的入侵检测模型。Aburomman等人在文献中提出对常用基于机器学习入侵检测的集成、混合技术[3]。考虑同质与异构类型的集成方法，同时训练多个分类器来解决相同的问题，然后结合它们的输出来提高准确率。而Ashfaq等人在文献中提出基于模糊半监督学习的入侵检测系统，以解决少量数据的问题[4]。其主要思想为利用无标记样本辅助监督学习算法来提高IDS分类器的性能。训练单隐层前馈神经网络输出模糊隶属度向量，利用模糊量对未标记样本进行分类（低、中、高模糊类别）。分类器在将每个类别分别合并到原始训练集中后再进行训练。将此技术运用至车联网当中，亦能显著提高入侵检测结果。

（2）车内平台网络层入侵检测技术研究现状

对于CAN总线的入侵检测，一些研究者尝试通过修改CAN总线的协议来增加相对应的校验机制或对CAN总线传输的消息进行加密处理。但是由于CAN总线消息中数据字段的长度不足，会大大增加计算负载，而车辆通信对速率要求极高。如果入侵检测系统过于复杂就会带来很大的时间延迟，对行车安全造成威胁，甚至造成车毁人亡的后果，所以基于车辆的入侵检测系统不宜设计得过于复杂。基于此，Song等人提出了一种基于CAN报文时间间隔分析的车载网络轻量级入侵检测算法，虽然能很好地发现CAN中某些周期报文的异常，但是不能检测报文中数据被修改的情况[5]。Müter等人提出基于典型车辆网络CAN的特性，引入了一组异常检测传感器，允许在车辆运行期间识别攻击而不会导致误报，但是没有具体实施，只是做了算法上的研究[6]。张子健提出了一种可以检测异常帧的CAN总线的异常检测算法，但是这种单独对每条报文的检测无法检测出不同数据报文间的关系[7]。例如修改左右车轮

的转速使其不一致且都处在正常的范围内，虽然不会发生警报但会对行车安全造成巨大危害。Taylor等人提出了一种基于长短时记忆神经网络的异常检测器来检测CAN总线攻击[8]。检测器通过学习，预测来自总线上每个发送器的下一个数据来工作，实际下一个数据中与正常情况偏差较大的部分被标记为异常。

近年来兴起许多基于机器学习的入侵检测方案。Zarai等人将递归神经网络和深度神经网络用于入侵检测系统中，使用了四个隐藏层、四十一层输入和两层输出，共有100次迭代[9]。对四种常用的缺陷检测模型架构进行比较，得出DNN3算法性能最佳，使用了三层长短时记忆法（Long Short-Term Memory，LSTM），最后显示三层LSTM有着较高的性能。Wang等人提出了一种基于深度学习的高效网络入侵检测方法，即基于稀疏自动编码器（SAE）和随机森林（RF）的有效网络入侵检测方法，将SAE的特征提取能力与随机森林的分类检测能力相结合，提高了检测效率和准确性[10]。同时为了解决基准数据集的不规则性和不平衡性，采用了ANASYN过采样技术，所提出的SAE-RF模型比传统的方法具有更好的性能。Lv等人提出了一种基于混合核函数极限学习机（HKELM）的新型准确有效的误用入侵检测系统[11]。该系统依赖于特定的攻击特征来区分正常和恶意活动，使用了主成分分析（Principal Component Analysis，PCA）算法，能够将计算量大大缩减，很好地处理线性关系，但对于一些非线性关系不太适应。因此又引入了核主成分分析（Kernal Principal Component Analysis，KPCA）算法，首先通过核函数将原始数据映射到高维空间，将一些不可分离的数据分离开来，然后再利用PCA算法进行降维和特征提取。Zhang等人提出了一种基于改进遗传算法（GA）和深度信任网络（DBN）的入侵检测模型[12]。针对不同类型的攻击，通过遗传算法的多次迭代，自适应地生成最优的隐层数和每层神经元数，使得基于DBN的入侵检测模型具有结构紧凑、检测率高的特点，可以有效提高入侵攻击的识别率，降低神经网络结构的复杂度。Ravi等人提出了一种新的SDRK（SSML DFNNRRS-K-means）机器学习算法来检测入侵[13]。SDRK利用有监督的深层神经网络（DNN）和无监督聚类技术，较大提高了算法的准确率。

（3）车内组件层入侵检测技术研究现状

对ECU的攻击一般可以分为针对ECU之间通信的攻击，即通过OBD-II接口的攻击，以及针对MCU内部内存与外部内存之间数据传输的攻击。Yu等人在文献中针对这两种形式的攻击提出了不同的对策[14]。

· 通过OBD-II接口进行代码认证：为了防止代码被篡改，需要通过身份验证来保证数据的完整性。例如，当一个ECU系统向远程主机发送一个请求移动代码的请求时。主机在传输的代码中包含一个身份验证器，可用于同时验证代码的真实性和完整性。身份验证器结合了加密和加密哈希函数。对代码应用密码哈希函数会输出一个短值，该值包含关于代码的足够冗余信息，以显示任何篡改，称为摘要。然后，可以通过使用主机的私钥加密摘要来获得身份验证器。主机加密的连接使用ECU接收器的公钥的代码和身份验证器的国家，并将其发送给目标ECU。在接收端，ECU计算消息的代码摘要，并将其与解密的消息摘要进行比较。如果它们是平等的，那么该消息确实来自其所谓的主机，并且没有被篡改。

· 实时解密：在单片机内部内存和外部存储器之间。但是，MCU不能直接解释加密的数据，实时解密从加密的代码中提取程序。在将代码加载到主存中时，就会进行解密。要实现实时解密，解密器必须以明文的形式存储在内部内存中。必须使用锁位、硬件硬化和温度保护进行保护。主程序被加密并存储在一组外部内存块中，因为它通常比内部内存大得多。对称加密用于程序的机密性。使用加密和实时解密的ECU重编程过程。

5 车联网安全新思路

随着“万物互联”时代的到来，车内暴露面数量激增，车联网行业迅猛发展的同时攻击手段愈发复杂多样，多步攻击已成为当前网络攻击行为的主要特征之一。多步攻击的威胁已引起广泛关注，防范多步攻击迫在眉睫。传统的无线网络入侵检测系

统在建立模型时，往往只考虑了当前攻击行为所涉及的网络节点的路径，因此无法详细分析网络的脆弱性。对攻击意图、路径的预测以及对攻击事件实时监控、分析将是进一步的研究方向。

目前追踪和发现攻击行为的主要方法包括直接基于网络流量进行特征建模和基于样本代码特征进行建模，但原始流量数据量往往过大，噪声特征占据非常大比例，导致直接基于原始流量构建的特征模型的鲁棒性欠佳，且此类方法通常需要耗费较多的人工成本，某些情况只能基于离线的历史数据进行分析，无法满足实时分析和追踪的需求。

当前，许多研究者将知识图谱技术与网络安全相结合，以面对网络攻击形势的复杂多变。安全知识图谱技术可有效解决动态攻击类型的监控与预测问题。《安全知识图谱技术白皮书》中提出运用安全知识图谱基于上下文感知计算框架的攻击追踪方法。定义以攻击行为为核心的本体结构，通过海量的多源异构威胁情报（包括开源威胁情报、设备产生的告警日志等）进行采集，生成领域安全知识库以分析其网络脆弱性。因攻击者进行实际的入侵活动时往往不只利用一种攻击手段，而是在更广的时间域利用一系列相互关联的攻击方法进行攻击，故在进行攻击行为监测和追踪时，将更大时间攻击行为进行关联检测。利用图谱对攻击行为关联检测流程图如图2所示。

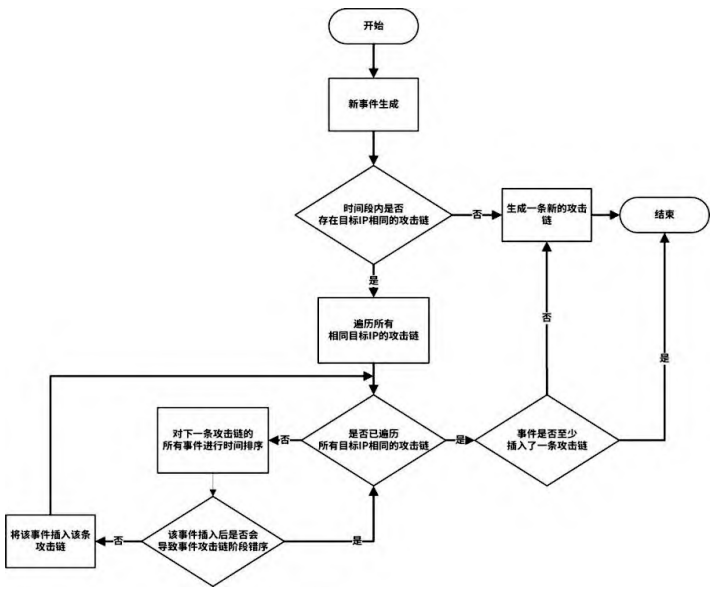

图2 利用图谱对攻击行为关联检测

第三代人工智能-认知智能技术可有效突破仅依赖数据驱动模型的入侵检测系统的瓶颈，构建车联网安全领域知识图谱是车联网安全由感知智能迈向认知智能、决策智能的必由之路。通过将安全知识图谱应用到车联网领域，能够实现对威胁的攻击建模、路径预判和智能实时防护等，大幅提升入侵威胁检测、态势感知、应急处理和追踪溯源等能力。当然，安全知识图谱在车联网入侵检测的应用实践仍处于早期阶段，在理论方法、标准制定等方面需要进一步研究与探索。

6 总结与展望

全球车联网市场规模从2015年的2454.2亿元，增长至2020年的6434.4亿元，预计2025年将超过1.5万亿元，2020~2025年全球车联网行业市场规模复合增长率将超过15%。车联网将会是物联网最大的驱动力之一，物联网正在重新定义汽车。本文从车联网安全威胁角度，分析了V2X通信安全、CAN总线安全与ECU安全，整理了车联网入侵检测技术现状。随着车联网入侵检测技术的日趋成熟，将会出现更为具体的安全需求与更加新颖的检测手段，如将基于认知智能的深度学习模型运用于车联网入侵检测系统等，皆需要研究者们进一步研究和探索。AP

作者简介

朱鹏程（1998-），男，江西南昌人，硕士，现就读于广州大学电子与通信工程学院，主要从事知识图谱、车联网威胁分析方向研究。

涂江健（1997-），男，广东肇庆人，硕士，现就读于广州大学电子与通信工程学院，主要从事车载CAN总线入侵检测方向的研究。

招志才（1998-），男，广东湛江人，硕士，现就读于广州大学电子与通信工程学院，主要从事车载ECU系统入侵检测方向的研究。

尚文利（1974-），男，黑龙江北安人，教授，博士生导师，现就职于广州大学，主要从事计算

智能与机器学习、工业信息安全、边缘计算方向研究。广州大学“百人计划”学科带头人，国家“十三五”重点研发计划项目首席，IEEE Industrial Electronics Society (IES) Member，第六届全国工业过程测量控制和自动化标准化技术委员会（SAC/TC124/SC5）委员，工业控制系统信息安全产业联盟理事。

曹　忠（1977-），男，安徽黄山人，讲师，博士，现任广州大学电子与通信工程物联网工程系主任，主要从事智能控制、人工智能技术、工业控制系统安全等方向研究。亚洲控制协会会员、中国中文信息学会成员、广州市物联网协会专家库成员。主持和参与国家重点研发课题、国家自然科学基金、广东省自然科学基金等10余项，发表学术论文30余篇，申请发明专利10余项。

浣　沙（1984-），女，讲师，博士，现就职于广州大学，主要研究方向为宽带雷达通信一体化技术、多源融合探测识别技术和雷达抗干扰技术、车联网信息安全防护技术。

张　曼（1984-），女，讲师，博士，现就职于广州大学，主要研究方向为智能图像/信号处理、车联网安全等。

参考文献：

[1] 李兴华, 钟成, 陈颖, 张会林, 翁健. 车联网安全综述[J]. 信息安全学报, 2019, 4 (03) : 17 - 33.

[2] 李馥娟, 王群, 钱焕延. 车联网安全威胁综述[J]. 电子技术应用, 2017, 43 (05) : 29 – 33, 37.

[3] Abdulla Amin Aburomman, Mamun Bin Ibne Reaz. A survey of intrusion detection systems based on ensemble and hybrid classifiers[J]. Computer & Security, 2017 : 135 - 152.

[4] Rana Aamir Raza Ashfaq, Xizhao Wang, Joshua Zhexue Huang, Haider Abbas, Yu-Lin He. Fuzziness based semi-supervised learning approach for intrusion detection system[J]. Information Sciences, 2017 : 484 - 497.

[5] Hyun Min Song, Ha Rang Kim, Huy Kang Kim. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]. International Conference on Information Networking, IEEE, 2016 : 63 - 68.

[6] Michael Müter, André Groll, Felix C. Freiling. A Structured Approach to Anomaly Detection for In-Vehicle Networks[C]. 2010 Sixth International Conference on Information Assurance and Security (IAS), IEEE, 2010 : 92 - 98.

[7] 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, (08) : 92 - 96.

[8] Adrian Taylor, Sylvain Leblanc, Nathalie Japkowicz. Anomaly detection in automobile control network data with long short-term memory networks[C]. 2016 IEEE International Conference on Data Science and Advanced Analytics (DSAA), IEEE, 2016 : 130 - 139.

[9] Rabeb Zarai, Mnaouer Kachout. Recurrent neural networks and deep neural networks based on intrusion detection system[J]. Open Access Library Journal, 2020, 7 (3) : 1 - 11.

[10] Zhihao Wang, Dingde Jiang, Liuwei Huo, Wei Yang. An efficient network intrusion detection approach based on deep learning[J]. Wireless Networks, 2021 : 1 - 14.

[11] Lu Lv, Wenhai Wang, Zeyin Zhang, Xinggao Liu. A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine[J]. Knowledge-Based Systems, 2020, 195 : 105648.

[12] Ying Zhang, Peisong Li, Xinheng Wang. Intrusion detection for IoT based on improved genetic algorithm and deep belief network[J]. IEEE Access, 2019, 7 : 31711 - 31722.

[13] Nagarathna Ravi, S.Mercy Shalinie. Semi-supervised learning based security to detect and mitigate intrusions in IoT network[J]. IEEE Internet of Things Journal, 2020, 7 (11) : 11041 - 11052.

[14] Lu Yu, Juan Deng, Richard R.Brooks, Seok Bae Yun. Automobile ECU Design to Avoid Data Tampering[C]. In Proceedings of the 10th Annual Cyber and Information Security Research Conference (CISR '15), 2015 : 1 - 4.