车联网安全综述

李兴华[1], 钟　成[1], 陈　颖[1], 张会林[1], 翁　健[2]

[1] 西安电子科技大学网络与信息安全学院 西安 中国 710071

[2] 暨南大学信息科学技术学院/网络空间安全学院 广州 中国 510632

摘要　随着移动互联网和工业智能化的快速发展, 以智能网联汽车为中心的车联网逐渐深入人们的生活, 在为出行带来便利的同时也暴露出车辆被远程控制、恶意攻击等安全威胁。本文首先总结并分析了当前车联网环境中所遭遇的多个攻击案例, 将车联网的安全问题总结为三个层面, 分别为: 网络级安全、平台级安全和组件级安全。其次将车联网的整体架构进行了划分和介绍, 从这三个层面对车联网目前存在的主要安全威胁进行了分析和总结, 针对性地介绍了目前的研究热点和研究现状。最后对车联网未来的发展方向和研究重点进行了展望。

关键词　车联网; 安全威胁; 网络级; 平台级; 组件级

中图法分类号　U495; TP309　DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.05.02

Survey of Internet of Vehicles Security

LI Xinghua[1], ZHONG Cheng[1], CHEN Ying[1], ZHANG Huilin[1], WENG Jian[2]

[1] School of Cyber Engineering, Xidian University, Xi'an 710071, China

[2] College of Information Science and Technology/College of Cyber Security, Jinan University, Guangzhou 510632, China

Abstract　With the rapid development of mobile Internet and industrial intelligence, the Internet of Vehicles centered on intelligent connected vehicles has gradually penetrated into people's lives. It has brought convenience to travel but exposed security threats such as remote control and malicious attacks as well. This paper first summarizes and analyzes the multiple attack cases encountered in the current Internet of Vehicles environment, and summarizes the security issues of the car network into three levels: network level security, platform level security and component level security. Secondly, the overall architecture of the Internet of Vehicles is divided and introduced. From these three levels, the main security threats existing in the Internet of Vehicles are analyzed and summarized, and the current research hotspots and research status are introduced. Finally, the future development direction and research focus of the Internet of Vehicles are prospected.

Key words　internet of vehicles; security threat; network level; platform level; component level

1　引言

随着移动互联网和工业智能化的快速发展, 汽车产业不断向智能化和网联化快速转变。智能网联汽车通过搭载先进的车载传感器与智能控制系统, 并与现代移动通信技术相结合, 实现了车与人, 车与车、车与路、车与云服务平台之间的信息交换与共享, 为人们的交通出行带来了极大的便利, 同时有助于政府建立智能化的交通体系。因此, 智能网联汽车作为新的发展方向受到了各国政府和企业[1-4]的广泛关注。调查数据显示, 2018 年我国的车联网市场规模将达到千亿, 并且在未来五年将会以21.6%的速度高速增长。然而随着车联网的快速发展, 其存在的安全问题日益突出, 安全事故[5-9]不断涌现。

2015 年 360 网络攻防实验室利用数字射频处理技术, 伪造钥匙发出的原始射频信号控制发动机电子控制单元 ECU(Electronic Control Unit, ECU), 成功入侵特斯拉[5], 实现了无需钥匙开启车辆。同年某国安全研究专家利用 Linux 系统漏洞对克莱斯勒的 Jeep 车型发起攻击[6], 成功对其固件进行修改, 从而获取了车辆的控制权。同时证明该款车型在被物理接触的情况下也能够被攻击者从车载诊断系统 OBD(On-Board Diagnostic, OBD)接口注入指令, 从而控制车辆, 由此可知车辆的系统漏洞和固件漏洞容易成为攻击者的目标。2016 年, 百度成功破解 T-Box(Telematics Box, T-Box), 篡改协议传输数据[7],

通讯作者: 钟成, 硕士研究生, Email: czhongcs@126.com。

本课题得到国家自然科学基金项目(No. U1708262, No. U1736203, No. 61672413, No. 61772173)资助。

收稿日期: 2019-01-03; 修改日期: 2019-04-19; 定稿日期: 2019-05-13

从而修改用户指令或发送伪造命令到 CAN (Controller Area Network, CAN)总线控制器中, 实现了对车辆的本地控制和远程操作控制, 这是因为在当前的 CAN 总线中没有加入加密认证等安全机制, 从而导致了攻击者容易修改 CAN 总线数据并伪造指令对车辆发起攻击。同年, 安全人员在入侵用户手机的情况下, 获取特斯拉 App 账户用户名和密码, 通过登录特斯拉车联网服务平台可以随时对车辆进行定位、追踪, 解锁、启动, 最终导致车辆被盗, 因此与车辆相关的 App 和车联网服务云平台也可能成为攻击者入侵车联网的入口。2017 年, 腾讯科恩实验室再次成功对特斯拉发起无物理接触远程攻击[8], 实现特斯拉多个 ECU 的远程协同操控, 最终入侵特斯拉车内网络实现任意远程操控。2018 年, 英国的一个盗贼仅使用平板电脑捕捉了特斯拉密匙的被动无线信号[9], 在不到两秒钟的时间内使用信号中隐含的密码打开汽车, 并成功盗走。此类攻击说明车联网的网络层面安全也至关重要, 由无线网络攻击而导致的安全问题也频繁出现。

由以上攻击案例可以总结得到, 车联网中主要的安全威胁来自于三个层面: 1) V2X(Vehicle to Everything, 包括: Vehicle-to-Vehicle、Vehicle-to-Road 等多种形式实体间通信统称为 V2X)的网络通信层安全: 攻击者可通过多样的无线网络通信手段, 篡改或伪造攻击信号, 并向汽车注入攻击指令从而达到影响车辆正常状态或者直接控制车辆的目的。另外多种类型的终端设备也成为攻击者入侵车联网体系的入口, 如云服务平台, 汽车远程服务提供商 TSP (Telematics Service Provider, TSP)、移动终端 App 等; 2)智能网联汽车本身的平台安全: 一方面由于 CAN 总线的高速且不加密不认证特性, 其通信矩阵容易被攻击者破解, 因此攻击者可以轻易伪造 CAN 总线报文, 从而影响车辆状态; 造成安全事故或车主的经济损失; 另一方面, 智能网联汽车中含有多种类型的传感器 ECU, 其中保存了车辆或车主的多种敏感数据, 此类数据容易被攻击者非法收集, 导致用户的隐私泄露; 3)车联网组件安全: 车联网架构中包含了大量的系统组件, 如各种功能 ECU, 攻击者能够通过这些组件的系统漏洞发起攻击或在此类组件固件升级过程中植入恶意代码。

因此我们分别定义这三个层面为: 网络级安全、平台级安全和组件级安全。本文将从这三个方面全面地介绍车联网体系中的安全威胁以及安全现状, 并且给出当前车联网安全研究的最新研究成果。同时我们也给出了对于未来车联网安全的研究方向。

本文的其他章节安排如下, 第 2 节主要介绍了车联网的基本组成和基本架构; 第 3 节讨论了车联网安全的主要威胁及安全现状; 第 4 节中我们介绍并分析了现有的最新研究内容与成果; 并在第 5 节给出了未来车联网领域的研究方向预测, 在第 6 节对本文内容进行了总结。

2 车联网体系架构

车联网是指借助新一代的移动通信技术, 实现车辆内部, 车与人、车与车、车与路、车与服务平台的全方位网络连接, 从而提升汽车智能化水平和自动驾驶能力, 构建汽车和交通服务新业态, 从而提高交通效率, 改善汽车驾乘感受, 为用户提供智能、舒适、安全、节能、高效的综合服务。其中车联网系统按照由外而内主要结构图如下图 1 所示: 其中主要包括车联网服务平台、智能网联汽车以及移动智能终端、路边基础设施等在内的网络级平台和终端、智能网联车汽车平台以及车内网络及车内 ECU 组件。其中各个部分通过形式多样的无线网络通信技术如 WiFi、蓝牙、2 G /3 G /4G、专用短程通信技术 DSRC(Dedicated Short Range Communications, DSRC)以及车内总线网络等, 实现车-云通信、车-车通信、车-路通信、车-人通信和车内通信五种通信场景。

2.1 车外网通信体系

车辆与多终端的无线通信是车联网中非常重要的组成部分, 其中主要包括车-车、车-路和车-人通信。车-车通信指智能网联汽车通过 LTE-V2X、DSRC 与交通网络中的其他车辆进行信息传递, 如车辆在行驶过程中报告当前位置的交通拥堵状况、交通事故等, 以帮助其他车辆做好路线规划或者提醒其他车辆注意行车安全, 从而改善整体的交通状况, 减少事故发生率。车-路通信主要指智能网联汽车通过 LTE-V2X、DSRC、射频通信等技术实现车辆与路基设施的协同以辅助建立高效安全的智能交通体系。车-人通信指用户通过 WiFi、蓝牙或蜂窝移动通信网络技术实现与智能网联汽车的信息传递, 如车主通过手机对车辆进行控制, 进行打开车门、音乐播放操作等。

车联网服务平台是提供智能网联汽车管理和交通、车辆信息内容服务的云端平台, 其提供了导航、娱乐、资讯、安防、车辆及道路基础设施设备信息汇聚、计算和监控管理, 并提供智能化交通管控、车辆远程诊断、交通救援等车辆服务, 比如车辆通过 T-Box 和云服务平台交互, 实现远程控制功能、远程

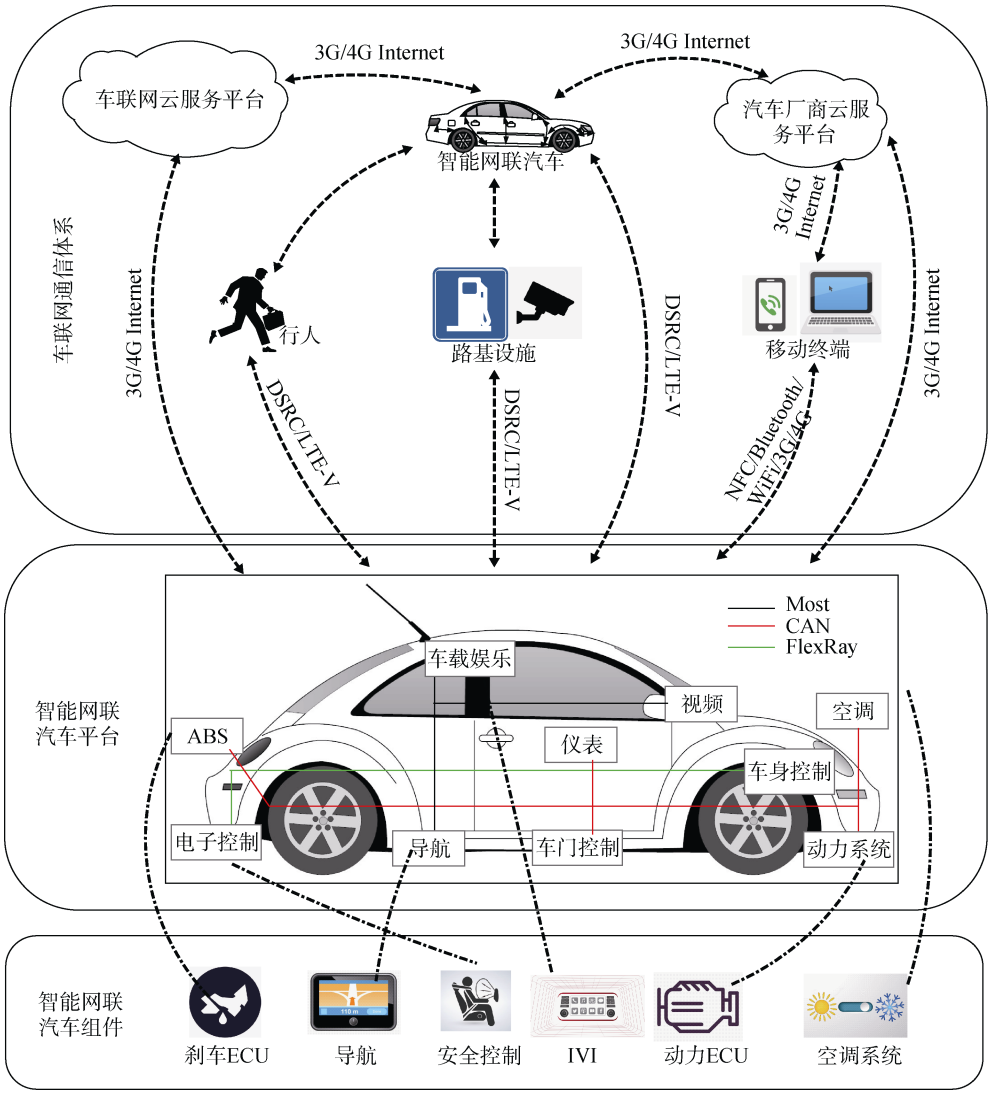

图 1　车联网基本架构

Figure 1　Basic Structure of Internet of Vehicles

查询功能、安防服务功能; 车辆通过 IVI(In-Vehicle Infotainment, IVI)从云服务平台获取娱乐信息服务, 包括三维导航、实时路况、IPTV、辅助驾驶、移动办公、无线通讯、基于在线的娱乐功能等一系列应用。

2.2　智能网联车平台网络架构

车内总线网络架构是通过总线通讯协议将 ECU 节点连接起来, 从而构成车内总线网络, 如图 2 所示。其中, ECU 是智能网联汽车的核心电子元件, 也是车内基本通讯单元。ECU 节点根据传感器和总线上的报文信息,完成预定的控制功能和指令动作, 如灯光的开闭、电机启停等。而不同 ECU 节点之间的通讯是通过车内总线协议来实现。其中, 车内总线协议主要包括 CAN, LIN(Local Interconnect Network, LIN), FlexRay, MOST 等。CAN 总线是一种串行数据通信协议, 负责车内各个子系统间通信。各个 ECU 节点竞争向总线发送数据, 根据报文标识符确定各节点的总线访问控制优先权, 优先级高的 ECU 节点可以向总线发送数据, 其余节点等待总线空闲再次竞争。这种逐位仲裁、明文广播的方式, 提高了数据通信的实时性, 故 CAN 总线是目前最广泛应用的车内总线协议。LIN 总线, 即低速串行总线, 也称低速 CAN, 采用单线传输, 传输速率在 10 到 125kb/s, 大多应用在车门, 空调等车身子系统。FlexRay 总线基于时间触发机制, 具有高带宽、容错性能好等特点, 最大数据传输率达到 10Mbps。目前主要应用于安全相关的线控系统和动力系统。MOST 总线采用环形结构, 在环形总线内只能朝着一个方向传输数据, 是一种专门应用于车内多媒体应用的数据总线技术。在众多总线协议中, CAN 作为目前最广泛使用的车内总线系统, 是学术界和工业界研究的重点。

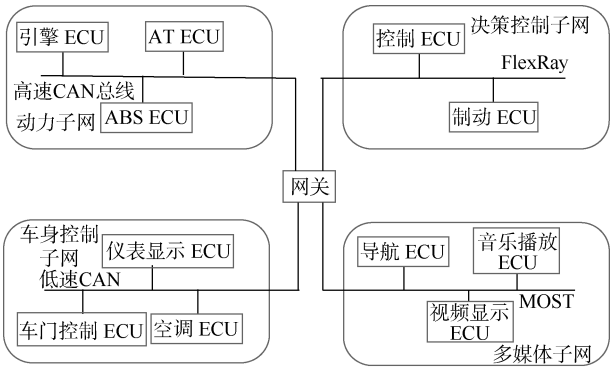

图 2　智能网联汽车平台架构示意图

Figure 2　Schematic Diagram of the Intelligent Vehicle Network Platform

智能网联汽车的车内传感器网络由众多的传感器, 执行器和控制器构成。在车辆运行过程中, 不同的传感器节点感知行车相关信息, 如车内机油温度传感器感知机油温度, 转速传感器采集转速信息等, 并将光, 电, 温度, 压力等信息转换成电信号, 传送给控制器节点。控制器节点对信息进行分析处理后向执行器节点发送控制指令, 由执行器节点完成指令动作。众多节点构成车内传感器网络, 根据通信协议, 协同工作, 例如车内的超声波传感器节点发射超声波信号, 遇到障碍物后返回, 控制器节点根据发射信号和接收信号的时间差可以推算出发射位置与障碍物之间的距离, 若小于安全距离, 将相关刹车制动指令发送给执行器节点。这一场景被广泛应用于自动驾驶或辅助驾驶等。

2.3　智能网联汽车组件

ECU 是汽车专用微机控制器, 类似单片机, 由微处理器(CPU)、存储器(ROM、RAM)、输入/输出接口(I/O)、模数转换器(A/D)以及整形、驱动等大规模集成电路组成[10]。每个 ECU 组件相当于汽车各个子系统的大脑, 包含自己独有的固件和软件系统, 其固件不但提供硬件初始化、加载操作系统、同时为上层软件使用硬件资源提供接口[11], 而软件系统对传感器输入的信息进行运算、处理、判断, 然后输出指令。随着车辆智能化程度的提高, 智能网联汽车内部部署的 ECU 的数量不断增长, 每个 ECU 控制着不同的功能, 如与动力相关的引擎控制 ECU、刹车 ECU, 与车身控制相关的空调控制 ECU、车灯控制 ECU。而且, 汽车的很多行为不是由一个 ECU 独立完成, 而是由多个 ECU 相互合作完成的。在车内网络中, 近百个 ECU 连成网络, 通过实时通信来控制汽车。

3　车联网安全威胁

虽然随着移动互联网和智能网联汽车的发展, 人们可以利用多种通信技术实现对智能车辆的全面控制, 但这也导致其中存在的安全问题日益严重。如车辆被远程攻击、恶意控制等安全隐患, 甚至可能出现大量网联汽车被批量控制, 造成重大社会安全事件。通过上述分析可知, 车联网中的安全威胁主要可分为三个层级: 网络级、平台级和组件级。

3.1　网络级安全威胁

车联网系统由车辆与云服务平台、人、路基设施等多个组件共同组成 V2X 网络, 其中又包括 WiFi、移动通信网(2G/3G/4G 等)、DSRC 等无线通信手段, 由于此类无线通信方式本身存在的网络安全问题[12-17], 因此 V2X 网络也继承了上述无线网络所面临的安全问题, 如传输安全、身份认证和网络入侵等问题, 同时由于车联网架构中也包括云服务平台、移动终端和路基设施等组成部分, 其平台安全和终端安全威胁也成为网络级安全威胁的一部分, 其中主要安全威胁如图 3 所示。

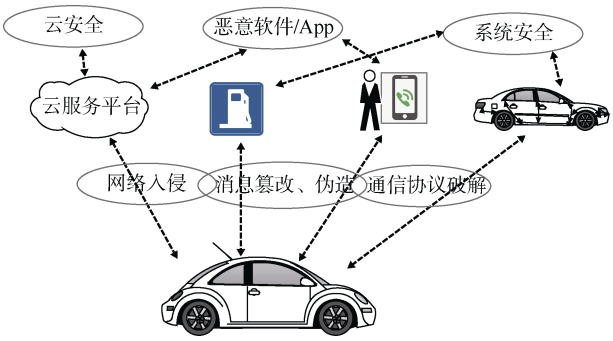

图 3　网络级安全威胁

Figure 3　Network Level Security Threats

1. 网络通信安全

车辆和云服务平台等其他终端传递的消息中传递着大量的用户隐私信息, 此类信息在消息传递的过程中容易受到攻击者窃听, 从而造成车辆或用户的隐私泄露, 同时 V2X 网络消息中包含大量的控制信息和报警信息, 如车-人网络中用户通过移动设备对车辆进行远程控制, 或车-车网络中接收其他车辆发来的报警信息, 如果此类信息遭到攻击者的阻断或者篡改, 则可能影响车辆驾驶员的判断, 从而造成严重的交通事故。另外攻击者可以对车辆进行大量的重复试验, 获得有关通信协议的先验知识, 从而使攻击者可以伪造报文发起对车辆的攻击。因此

在此过程中对所传递消息的加密和实体的认证是不可或缺的。然而在高速移动的车辆网环境中，如何实现多场景且高效的认证同样是具有挑战性的问题。由于车辆的高速移动，车辆需要不断的和新的车辆或者路基设施实现认证，此过程对实时性要求较高，因此传统的基于椭圆曲线等公钥密码学的认证方案[18,19]无法直接应用于车联网环境中。同时，车辆在认证的过程中需要保证用户的隐私安全，车辆如果在无线网络环境中直接使用真实身份 ID 进行认证，那么车辆的位置信息和移动轨迹将会被直接暴露，如果攻击者收集并分析此类数据，那么则可以进一步的推断出车主的个人隐私信息。因此在车联网环境下实现匿名认证是必要的。与此同时，由于车联网系统中车辆不断的高速移动，其所处网络拓扑结构随车辆位置不断变化，如何检测网络中不断出现的未知攻击成为一个亟待解决的问题。虽然基于机器学习的方法[20-22]在传统网络下被广泛使用并且发挥一定的作用，但是车联网环境中的网络结构和流量特征更加复杂多样，并且由于车联网中智能网联汽车本身的存储能力有限，在高速移动的环境中无法获取足够的训练数据完成入侵检测模型的训练过程，这也导致了大多数方案无法适用于车联网环境中。

2. 网络终端安全

云服务平台安全威胁[23-25]：智能网联汽车的云服务平台作为车联网中重要的组成部分同样面临多种安全威胁，并且将云计算平台的安全问题引入车联网中。其作为数据中心和服务中心，本身容易遭受传统的网络攻击，导致数据泄露等问题，同时云服务平台本身的安全性也值得关注，传统的操作系统漏洞威胁和虚拟化技术的大量运用导致虚拟机的调度、管理和维护均成为重要的安全挑战。App 安全威胁[26-28]：车联网中移动终端通过 App 完成对车辆的控制，如门锁、远程启动车辆等功能。而此类 App 因为广泛应用而且易于获取成为了攻击者的攻击入口，例如攻击者可以通过反编译技术获取通信密钥、分析通信协议等，并结合远程控制系统进一步控制车辆。另一方面，Android 或 IOS 系统 App 均存在被攻击者植入恶意代码的风险，当移动终端和车辆进行无线通信时，终端 App 可以作为跳板进一步渗透进入智能汽车内部，从而窃取用户隐私信息或者威胁汽车行驶安全。因此其直接影响到车联网系统的安全。

3.2 平台级安全威胁

平台级的安全威胁主要包括车内 CAN 总线的安全威胁以及车内传感器网络的安全威胁。如图 4 所示。当前的车内总线协议，如 CAN，FlexRay 和 LIN 等均采用发送明文报文，除了简单的校验位之外，未提供任何加密或是认证等安全机制，使得攻击者可通过控制连接到总线上的 ECU 节点读取和修改报文。由于车内总线协议受到的威胁具有相似性，本文主要介绍目前最广泛使用的总线协议—CAN 总线及其受到的安全威胁。

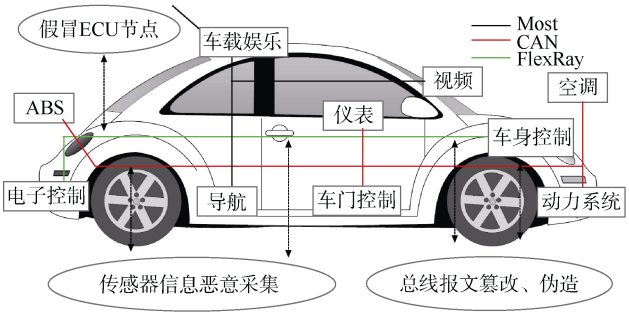

图 4 平台级安全问题

Figure 4 Platform Level Security Threats

CAN 总线在数据链路层采用 CSMA 的方式进行通信，即网络中各节点竞争向总线发送数据，根据报文标识符确定各节点的总线访问控制优先权。发送到总线上的数据帧格式[29]如图 5 所示。

可以看出，报文的数据域最多只有 8 个字节，且不包含发送方地址和目的地址，只提供简单的 CRC 校验位，这种方式在提高 ECU 间节点数据通信的实时性的同时，因其明文广播报文的通信方式，使得攻击者可以根据大量的历史数据帧通过逆向工程、模糊测试等方法获得 CAN 总线的通信矩阵并破解 CAN 总线应用层的通信协议(通信矩阵即 CAN 总线在应用层的，由汽车厂商定义的发送到总线上的数据帧格式以及其对应的实际含义，且对外保密)，进而重放报文或者发送伪造的报文到 CAN 总线。由于无认证机制，ECU 节点认为重放的或者伪造的报文是合法的，进而根据该报文信息完成相关的控制功能和指令动作，威胁行车安全。另外，根据 CAN 总线的报文优先级仲裁机制，攻击者可以持续的发送高优先级的报文抢占总线，中断合法报文的传输，即中断攻击。例如，Koscher[30]等人通过 OBD 接口窃听并分析总线报文，破解 CAN 总线通信矩阵，向总线发送伪造的报文，进而控制车身模块，发动机等，且成功实现了中断攻击。Miller[31]等人实现了利用了吉普的 UConnect 系统中的漏洞，通过连接到车辆的蜂窝网络，经娱乐系统发送伪造报文到 CAN 总线，进而控制转向、制动等车内子系统。

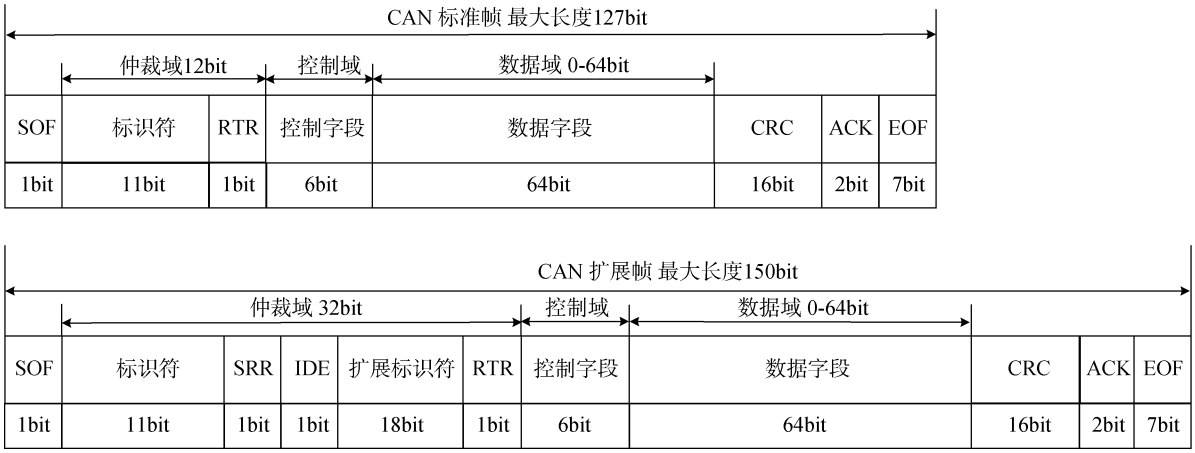

图 5　CAN 总线报文结构

Figure 5　CAN Bus Message Structure

另一方面, 智能网联汽车的车内传感器网络的传感器、控制器、执行器等众多节点根据通信协议, 协同工作。但通信过程中可能存在攻击者恶意采集传感器信息, 收集行车相关数据, 或者根据车内传感器的特点, 通过干扰传感器设备的通信, 危及行车安全。例如超声波传感器通过发射仪发射信号, 遇到障碍物后返回, 根据发射信号和接收信号的时间差可以推算出发射位置与障碍物之间的距离。但会存在这样的问题: 如果环境中存在其他超声波设备发送相同频率的超声波, 则会严重影响接收端的信噪比。利用这一弱点, 可以对其进行噪声攻击。实质上是利用超声波发射仪播放强度更大的同样频率的超声波信号, 这样就使超声波感应器无法回收自己发送的信号, 从而无法检测车身周围的物体。除此之外, 由于超声波传感器主要用于检测与车身最近的障碍物, 只有第一个超声波返回信号会被接收处理。只要让噪声源在合适的时机播放适当频率和强度的超声波即可实现对超声波传感器的欺骗攻击。另外, 由于超声波可以被超声波吸附材料吸收, 攻击者可以利用这一特点, 吸收超声波信号, 导致并未有超声波返回。如国内 360 团队成功扰乱了特斯拉自动驾驶系统的超声波传感器, 实现了针对超声波传感器的噪声攻击和欺骗攻击[32]。再例如, 网联车的汽车无钥匙进入系统 PKE(Passive Keyless Enter, PKE)采用了 RFID 无线射频技术, 钥匙和车身模块包含无线通信的传感器, 车身模块不断发出加密后的消息, 若钥匙模块处于无线信号可接收的范围内, 则会响应并解密, 以打开车门。PKE 系统通常会定时更新密钥, 以防止无线信号重放攻击。但仍存在攻击者通过干扰无线电发射信号, 挖掘漏洞并破解, 最终达到非授权控制汽车的目的。例如, 2016 年 360 团队通过对无线信号的录制, 对信号进行了逆向设计, 更低的频率逐位发送分解的信号, 使得无线信号的传输距离更长, 以实现远距离打开车门等操作。2018 年 KU Leuven[33]发现 Tesla Model S 的 PKE 系统仅用 40bit 的弱密码加密与密钥相关的代码, 一旦从任何给定的钥匙模块中获得两个代码, 就可以通过穷举获得汽车密码。攻击者可以读取附近 Tesla 的无线信号, 计算产生加密密钥, 窃取汽车。

3.3　组件级安全威胁

ECU 本质上是单片机, 其计算资源和存储能力都较弱, 安全性一般较差, 攻击者可以通过软件攻击、电子探测攻击、探针技术、远程升级[34]等手段, 获取 ECU 的关键信息, 甚至破解和控制 ECU。因此 ECU 面临其本身的漏洞安全问题, 如固件漏洞、软件漏洞、通信协议漏洞等; 同时, ECU 大都支持远程升级和固件重新刷写, 以实现功能更新或者漏洞修补, 因此, ECU 还面临远程升级带来的安全问题, 如升级包篡改。其中主要安全威胁如下图 6 所示。

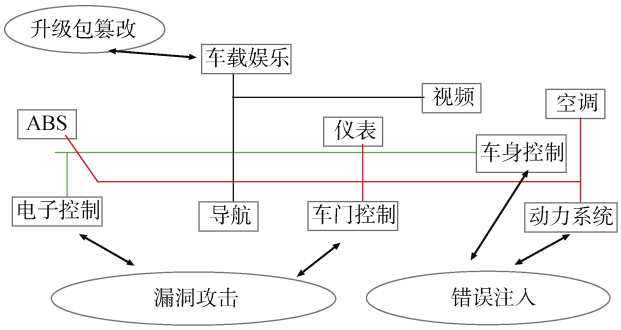

图 6　组件级安全问题

Figure 6　Component Level Security Threats

1 ECU 的安全漏洞: ECU 中的漏洞既有软件漏

洞, 也有固件漏洞。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[35]的机会。攻击者利用这些漏洞, 扰乱 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, 打乱了系统的执行流程。而对于固件漏洞, 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 固件的漏洞。固件读取时, 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。

2 ECU 固件升级: 攻击者可以通过 OBD 口, 或者将 ECU 拆解下来, 并利用辅助设备, 将含有恶意代码的固件刷入 ECU, 进而干扰/控制 ECU 和车内网络。同时, 攻击者可以通过升级包篡改等手段远程升级 ECU 固件, 将篡改后的恶意升级包或者未认证的第三方升级包刷写入 ECU, 实现对 ECU 的干扰和控制。

综上所述, 智能网联汽车内部的 ECU 存在安全漏洞问题以及固件安全升级问题。由于汽车内部的 ECU 数量庞大, 种类众多, 不同 ECU 的具体安全问题不尽相同, 如对引擎 ECU 的攻击手段不一定适用于刹车 ECU, 然而任何一个安全问题都会影响到同型号的多辆汽车, 可能造成严重的后果, 这导致了车内组件的安全问题庞大而复杂。

4 车联网安全保护措施

车联网的快速发展以及安全问题的日益突出引起了国内外安全组织和研究机构的广泛关注, 各研究组织通过发布白皮书、设立车联网项目以及各种科研项目奖励[11,35,36]等方式开展车联网安全研究并推广车联网的安全标准以解决车联网中出现的各种安全问题。

4.1 网络级安全防护

1. 通信层安全防护

车联网环境中的车辆不再是独立的封闭系统, 而是依赖各种对外接口和通信手段与外界实体进行通信, 如上述图中所示。因此提供完善的对外通信策略对车辆与外界的连接和通信安全是至关重要的。车辆对外通信安全是整车防御的第一层防御保障, 目前已有一些学者提出了车外部网络安全通信解决方案, DSRC[37]是欧洲较早提出的 V2X 通信标准, 安全和隐私部分主要是基于公钥架构 PKI(Public Key Infrastructure, PKI), 但这种基于 PKI 架构的安全方案每次通信必须传递证书, 并验证证书, 增加了网络负载, 文献[38,39]等在通信层面对 DSRC 协议进行了优化和增强, 进一步提高了车联网环境中通信的效率。同时为了实现车联网环境中高效认证并且保护车辆的隐私信息, 众多学者将批量认证技术和匿名认证技术[40,41]引入到车联网环境中, 以保证车辆的通信安全和隐私安全。文献[40]提出了一种高效的匿名批量认证方案, 该方案首先将区域划分为若干部分, 其中 RSU 以本地化的方式管理车辆。然后, 使用假名实现隐私保护, 并使用基于身份的签名实现批量认证。最后, 使用 HMAC 来避免耗时的证书撤销列表检查, 并确保在以前的批量认证中可能丢失的消息的完整性。而文献[41]采用了群签名的方式完成车辆的批量认证, 在验证群组成员身份的过程中, 采用组员的身份有效期来代替证书撤销列表检查操作, 使得认证过程更加高效。考虑车联网中大多是计算能力和存储能力受限的移动设备, 基于共享密钥的轻量级匿名认证方案[42-45]相继被研究者提出, 此类方案主要将认证设备的共享密钥进行 HMAC 或 CRC 校验, 然后发送服务器进行校验, 这样省去了公钥密码体制复杂的计算过程, 并且通过可以通过 k-匿名[44]或组标志[45]等手段高效的完成匿名认证。

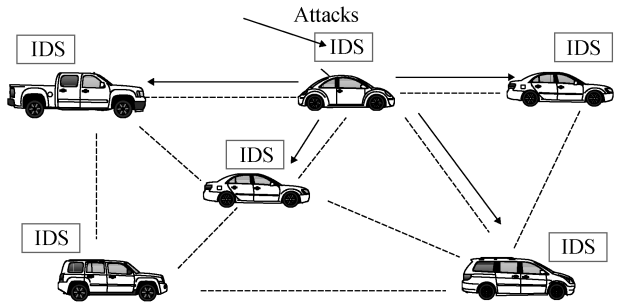

图 7 分布式入侵检测架构

Figure 7 Distributed Intrusion Detection Framework

由于车联网通信方式多样性和车辆的移动性特点, 车辆所处的网络环境更加复杂, 如何进行有效的网络入侵行为检测成为一项挑战。目前已有许多关于无线网络场景下的入侵检测方案[46,47], 其中文献[48-50]提出基于Ad-hoc网络中的入侵检测方案, 其主要架构如图7所示, 此类方案基于分布式合作的方式由簇头节点作为入侵响应的监视节点负责整个区域节点行为监视, 同时所有的监视节点又相互合作负责整个网络的入侵检测任务, 此类方案虽然可以通过监视节点节省网络资源的开销, 但是随着车辆的移动, 需要不断地建立分组离开分组, 同时车辆间需要非常强的信任关系以保证车辆自身不受组

内车辆的攻击，从而保证入侵检测系统能够正常有效的工作，显然对于快速移动的车辆来说并不适用。由于基于机器学习深度学习的智能化算法在处理大数据上具有优势，越来越多的研究者将此类技术应用于入侵检测领域并且取得了较好的效果[20-22]。此类方法的主要思想是通过提取底层网络流量特征进行分析，并根据已有数据建立检测模型，对未知的网络流量进行检测，从而检测出网络中的攻击行为。文献[20-22]分别采用了机器学习中不同的算法进行建模，以建立可靠的入侵检测模型。考虑单一模型在检测准确率等方面的局限性，基于集成学习[51,52]的入侵检测方案相继被提出，此类方案主要依靠多种或多个检测模型结果的融合得到最终的检测结果，显著的提高了入侵检测效果，其中融合方案主要有投票法，加权投票法等。但是，由于车联网环境下车辆的存储能力有限，在移动环境中如何保证充足的训练数据集成为一个关键问题，因此文献[53,54]中考虑了网络入侵检测中数据缺乏的问题，首先采用了半监督学习(Semi-Supervised Learning)通过少量的标记数据对大量的未标记数据进行标记，从而基于少量数据的情况下建立了可靠的入侵检测模型。如图8所示，文献[54]中在k-NN算法中通过未标记数据周围k个已标记数据的投票，逐渐对未标记数据进行投票，将投票结果的多数作为数据的label(正常或异常)，然后成功构造了大量的标记数据集D，进而采用改进的随机森林算法建立可靠的入侵检测模型。

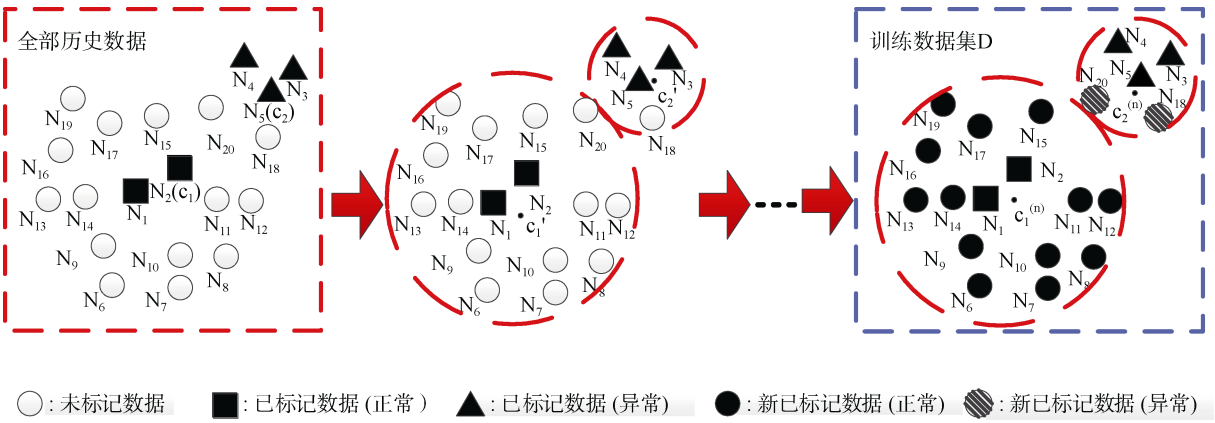

图 8　半监督学习过程

Figure 8　Semi-supervised Learning Process

2. 终端层安全防护

云服务平台：数据安全是云服务平台最重要的问题，如何保证云服务平台中数据不被滥用和泄露成为研究的热点内容。文献[55,56]中详细分析了云服务平台中的数据安全保护措施，如云数据加密技术、数据访问控制技术以及对应的完整性保护、数据存在与可用性证明等安全问题。另外云服务平台本身系统安全性也成为另一个重要问题，如虚拟化的安全技术、虚拟机映像文件安全、以及云资源调度访问安全等。终端层另一个非常重要的问题就是移动终端的应用安全防护机制，主要包括了恶意代码识别、恶意软件识别等，除了基于传统的沙箱检测、代码分析和软件行为分析[57]等技术，新兴的基于人工智能的方法成为目前研究的热点[58,59]。此类研究不作为本文重点，因此本文不作赘述。

4.2　平台级安全防护

CAN 总线作为目前最广泛使用的车内总线通信协议，作为攻击者入侵车内网络的关键一步，是目前研究的重点。目前关于 CAN 总线的安全研究主要集中在 CAN 总线的报文认证机制、报文加密机制和 CAN 总线的异常检测机制。

CAN 总线的报文认证机制主要是验证报文的完整性以及数据源认证。报文认证机制可以抵抗攻击者的重放，伪造报文。为实现 CAN 总线认证机制，需考虑两个方面的问题：一是 CAN 总线的数据帧的数据域最多只有 8byte，难以增加额外的认证数据，且数据帧格式多由厂商确定，若修改数据帧格式，需硬件方面的支持；二是 CAN 总线数据帧不包含发送方和目的方地址，若要实现报文的源认证，需对 ECU 节点进行标识。目前的研究[60-69]大多集中在 CAN 总线的报文认证，如表 1 所示，主要从以下三个方面：第一类是主要从物理层方面进行改进。一方面可以利用增加 CAN 收发器中物理层的电子讯号的采样频率来实现嵌入认证信息，但此方法需要修改 CAN 收发器硬件设计，增加了制造商成本，如文献[61-62]。另一方面利用 CAN 上的物理信号特性来

表 1 CAN 总线认证方案对比

Table 1 CAN bus authentication scheme comparison

技术分类	协议	特点及优势	局限性和缺点
利用 CAN 总线物理层特性	Groza 等人[60]方案	1. 有效的使用对称密钥用于时间同步; 2. 已成功的在传感器网络中使用。	1. 认证时延不可避免; 2. 延迟密钥公开时存在与其他数据帧冲突的可能。
	Van 等人[61]方案	1. 根据 CAN 特性, 将密钥与 message ID 相关联; 2. 无认证延迟。	1. 无法实现源认证; 2. 密钥数量随报文数增加而增加。
	Murvay 等人[63]方案	1. 利用物理信号特性来区分发送方; 2. 只需安装一个监测单元, 成本较小。	在实际环境中可能受到干扰, 导致较高的错误率;
基于密码学生成 MAC	Nilsson 等人[65]方案	1. 将 MAC 分成四部分, 占用随后发送报文的 CRC 位; 2. 不增加总线负载。	1. 认证延迟不可避免; 2. 占用 CRC 导致无法校验传输过程的错误。
	Woo 等人[66]方案	1. 将 MAC 截断为 32 bit, 占用扩展标识符字段和 CRC; 2. 不增加总线负载, 无认证延迟。	1. 有限长度 MAC 难以提供足够的安全性; 2. 无法校验传输过程的错误。
	Radu 等人[67]方案	1. 将生成的 MAC 额外的报文传输; 2. 64bit 的 MAC 安全性较高。	成倍的增加总线负载。
其他方案	CaCAN[68]	1. 中央监视节点对其他节点进行身份认证; 2. 其余节点无需进行计算。	1. 安全性依赖于中央节点; 2. 修改 CAN 控制器, 成本较高。

区分发送方节点, 通过对电信号特征求均方误差或卷积, 可以成功地区分 ECU 节点, 如文献[63-64]所提方案。第二类主要基于密码学的方式生成 MAC 认证报文, 如在 CAN 总线上传输与该报文相应的等长的认证信息, 即需要传输两条报文: 原本的报文以及该报文的认证信息。但这种方式需要两倍的传输成本以及两倍的报文标识符使用空间。再比如将认证信息嵌入其数据域中, 即使用数据域的一部分用来表示认证信息。这种方式压缩了数据域所承载的信息容量, 但无须额外分配报文标识符, 例如复合的 MAC 方案[65]和 Woo [66]等人提出方案。第三类由中央监视节点对网络中的其他节点进行身份验证。一旦发现未授权的报文传输, 中央监视节点实时传输更高优先级的错误帧来阻止非法报文的传输。但这种方法需要修改 CAN 控制器。并且若监视器节点受到损害或被移除, 整个网络安全也会受到影响, 如 CaCAN[68]。

CAN 报文加密机制是指对 ECU 节点分配密钥, 并使用相应的密钥加密报文的数据域。只有拥有密钥的 ECU 节点可以解密报文, 以保证报文的机密性。报文加密传输可以在攻击者多重步骤的初期就阻拦该攻击。另一方面, 由于车内 ECU 节点的计算存储能力有限, 且车内 CAN 总线对实时性的需求高, 计算开销大的加密算法并不适用于车内 CAN 总线网络。因此, 轻量级的加密算法更受到学术界和工业界的认可。LCAP[70]方法采用了 AES 分组加密, 分组长度为 16 字节。由于 CAN 总线数据域只有 8 个字节, 至少需要对每两条数据帧分组加密, 这也意味着通信时延的增加。而若采用流密码[71]的方式对每一位加密, 在减少时延的同时, 如何更新加密密钥成为研究的难点。工业界的 Trillium[72] 公司提出 SecureCAN 方案用于实时加密 CAN 总线(和 LIN 总线)报文, 其针对每一个 CAN 报文使用不同的加密密钥, 且加密方法可以针对最大 8byte 的数据进行处理, 但该加密算法并未公开, 其安全性并没有经过安全专家以及信息安全社群的检验。

CAN 总线报文异常检测机制主要分为基于统计的异常检测和基于机器学习的异常检测。其中, 基于统计的异常检测是通过统计大量的历史报文记录, 分析报文的信息熵, 时间间隔, 时间序列等, 检测异常的 CAN 总线报文, 并及时反馈。这里将总线上的信息熵定义为一个时间窗口内 CAN 总线上不同 ID 的报文频率, 而当攻击者向 CAN 总线注入大量报文时, 总线上信息熵的变化不同于正常情况。根据信息熵的变化情况, 对总线上的报文进行异常检测, 但此类基于信息熵变化的检测方案对于少量报文注入引起的信息熵的变化和任务触发型报文引起的信息熵的变化难以区分, 准确率低, 如文献[73]。另外, 总线上的某些报文具有周期性。针对周期性的报文, 如果同一 ID 的报文连续出现的时间间隔高于或低于阈值, 则认为是异常。但这种方法对非周期性报文并不适用, 如文献[74,75]。在文献[75]中, 根据报文标识符和部分数据字段, 利用 Bloom 滤波来检测报文的周期性, 从而发现潜在的重放或伪造攻击。该滤波机制是直接适用于任何其他时间触发的车内总线, 如 FlexRay。除此之外, 研究者还提出基于报文序列和

基于时钟偏斜的异常检测方法等。报文序列是指根据报文 ID 出现的序列来建立转移矩阵, 对于没有出现过的报文序列就视为异常。但此类方案无法定位异常报文, 误报率较高, 如文献[76-77]。而基于时钟的入侵检测方式将周期性报文的时间间隔作为发送 ECU 的指纹, 对其建模, 分析并检测入侵, 如文献[78], 该方案在入侵检测中具有较低的假阳率, 且在检测到攻击时, 可以定位是哪个 ECU。但需要时间收集大量的总线报文, 且仅适用于周期性报文。另一方面, 基于机器学习的异常检测方法将大量的标记好的正常数据和异常数据提取特征向量, 训练模型, 用于车内网络的异常检测。例如, 可以通过收集车辆状态来建立隐马尔科夫模型, 与观测到的车辆状态对比来判断是否有异常发生; 可以通过用报文内容, 网络状态等车内网络数据提取特征向量, 来训练神经网络, 并根据神经网络预测下一条报文的内容, 当接收到的报文与预测结果差别大于阈值时, 就识别为异常, 如文献[79-82]。相比于基于统计的异常检测, 基于机器学习的异常检测方法准确率高且更具有普适性, 但计算和存储开销较大。

另外, 对于 LIN, FlexRay 和 MOST 总线, 现有研究较少, 且与 CAN 总线的安全方案具有相似性, 主要通过以下三个方面: (1)对发送方进行认证, 以确保只有合法节点才能通信。对于来自未经授权节点的报文, 立即丢弃。如文献[83], 通过数字证书来验证发送方的身份。证书由节点标识符 ID、公钥、认证信息组成。网关安全保存所有认证过的设备制造商的公钥。每个发送节点的数字证书由制造商使用其私钥进行签名。网关使用相应的公钥来验证节点证书的有效性。如果认证过程成功, 则将相应的节点添加到网关的有效节点列表中; (2)加密传输报文, 对 ECU 节点分发密钥并将报文加密传输, 只有拥有密钥的合法节点可解密, 以保证报文的机密性; (3)在网关节点实现防火墙功能[84-86], 只有合法的获得授权的节点才能向某些与行车安全高度相关的节点发送有效的消息。比如 LIN 总线通常应被禁止向高度安全需求的总线, 如FlexRay发送报文。此外, 在正常驾驶中, 防火墙应该禁用车载诊断功能读取或者发送报文。

4.3 组件级安全防护

由上节的安全威胁分析可知, 智能汽车中 ECU 组件面临的安全问题可分为两类: 漏洞检测问题和固件安全问题。

表 2 漏洞检测方法及其优缺点

Table 2 The advantages and disadvantages of vulnerability detection methods

检测方法	优点	缺点
静态分析文献[87-89]	1. 无需运行被测程序 2. 自动化程度高 3. 容易定位问题	1. 需要源代码 2. 依赖特征库和规则库
符号执行文献[90-93]	利用符号的可变性, 尽可能地遍历程序的每一条路径	1. 约束求解困难 2. 路径爆炸问题
模糊测试文献[94-96]	1. 无需源代码 2. 不关心被测对象的内部实现细节 3. 测试用例的可复用性好	无法识别访问控制漏洞和多点触发漏洞
机器学习文献[97-100]	1. 从大量数据中自动提取漏洞特征 2. 适用于大规模数据	依赖数据集的数量与质量, 无法发现未知模式的漏洞

1 漏洞检测: 智能汽车中, ECU 本质上是一种嵌入式设备, 因此针对嵌入式设备的漏洞检测方法仍然可以用于 ECU 的漏洞检测。现有的嵌入式设备的漏洞检测方法有静态分析[87-89]、符号执行[90-93]、模糊测试[94-96]、机器学习[97-100]等, 如表 2 所示。静态分析是一种静态漏洞检测技术, 不需要运行软件程序, 通过语法分析、数据流分析等对程序源代码进行扫描并与其规则库进行比对, 就可分析程序中可能存在的漏洞并定位漏洞在源代码中的位置。常用的静态分析工具有 FaultMiner [87]、ITS4[88], 二者都是针对源代码的分析工具, 主要检测不符合安全规范的函数调用。FaultMiner 结合了数据挖掘和静态分析, 而 ITS4 仅支持对 C/C++语言的语法分析。静态分析依赖其规则库的质量。Costin[99]等提出的框架进行大规模的固件收集、过滤、解包和静态分析, 并实现了集中有效的静态分析技术, 通过从互联网上收集的 32356 个固件镜像, 发现 693 个固件镜像有至少一个漏洞, 并报告 38 个新的漏洞, 展示了对固件安全更广泛的看法。符号执行是一种通过计算符号状态来实现程序分析的方法, 它能够确定是什么输入导致程序每个部分的执行, 在理论上可以发现程序中的所有漏洞。现有的符号执行引擎具有自动分析程序中所有可能路径的能力, 遍历程序的执行空间, 支持对二进制文件的分析, 并找出漏洞, 如 FIE[90]、

KLEE[91]、Firmalice[92]、Angr[93]。但是在实际应用过程中, 具有路径爆炸、约束求解困难等问题。路径爆炸是指程序中可能路径的数目随着程序规模的增长而呈指数级增长, 甚至由于失控的循环而趋于无穷。约束求解是指根据最终得到的结果求解输入向量, 如果把结果条件改为漏洞条件, 就能够进行漏洞挖掘。FIE 是基于 KLEE 的一个符号执行引擎, 为自动分析 MSP430 微控制器(现有研究中常用来模拟 ECU 进行实验)的固件漏洞而设计的, 利用状体修剪和内存涂抹来提高代码覆盖率, 并支持分析固件程序中所有可能路径的能力, 同时支持分析内存安全违规和外围滥用错误两种安全问题。模糊测试是基于缺陷注入的自动化漏洞挖掘技术, 基本思想与黑盒测试类似, 不关心程序的内部实现细节。通过向被测程序输入半随机数据并执行程序, 分析程序发生的异常来发现漏洞。半随机数据是指对被测程序来说, 输入数据的格式和大部分数据是合法的, 但是其他部分却属于非法数据。由于被测程序没有考虑对非法输入的处理而触发安全漏洞。模糊测试的用例可以复用于多个同输入类型的被测对象。有研究从网络协议、固件程序和模拟器执行等不同方面进行模糊测试。如黄涛[94]通过分析车内网络的总线技术和协议, 研究模糊测试技术的优缺点, 对车内网络进行威胁建模, 提出了基于模糊测试的车控网络漏洞挖掘方案, 成功发现 ECU 中的漏洞。戴忠华[95]等从漏洞利用的角度分析了固件的攻击面, 然后根据攻击面导出相应的安全规则, 提出了一种针对嵌入式设备的基于污点分析的改进模糊测试方法, 实现漏洞挖掘。Avatar[96]等是一个基于时间的仲裁框架, 通过在嵌入式设备之间注入一个特殊的软件代理, 在模拟器中执行固件的指令, 实现模糊测试等动态分析。机器学习为漏洞检测提供了新的方法, 通过在大量的数据中提取漏洞特征, 并对已标记的数据集建立分类模型, 实现对漏洞的检测, 适用于大数据时代。基于机器学习的方案一般需要建立漏洞的特征数据集, 在特征数据集上采用不同的机器学习算法, 如基于知识匹配[97]、对抗深度学习[98]、神经网络[99-100]。但是, 基于机器学习的模型依赖于漏洞特征数据集, 会导致一定的误报率和漏报率, 同时, 其难以检测数据集中未出现的漏洞类型。此外, 有研究从嵌入式设备的底层硬件入手, 实现漏洞挖掘, 是主流方法的有效补充。如杨世德[101]等通过分析嵌入式系统的底层运行机制, 提出了一种基于嵌入式系统底层硬件漏洞挖掘模型和方法。张鹏辉[102]等通过对固件的软硬件交互机制进行形式建模分析, 提出了基于行为时序逻辑 TLA 的软硬件协同形式验证方法, 发现了固件更新过程中的安全漏洞。李登[103]等通过对设备固件进行分类, 采用二进制差量分析、字符串差量匹配、模糊哈希三种方法分析第三方库同源性, 从而检测同类固件中存在的漏洞。

2 固件安全: 固件安全问题主要是固件反逆向分析和固件安全升级。为防止固件被逆向分析, 一方面选择的 ECU 要支持加密算法、内部有保护寄存器、可以对固件存储器设置只读模式等方法, 以增加读取 ECU 固件的难度; 选择可以通过软件禁用 ECU 的 JTAG、RS232 等调试接口, 减少读取 ECU 固件的入口, 降低固件被读取的风险。另一方面, 尽可能使用自定义的指令集, 尽量避免使用通用开源的指令集, 同时, 在不改变功能逻辑的前提下, 在固件代码中插入混淆指令, 增大逆向分析的难度。对于固件安全升级, 应使用经过汽车生产厂商认证的升级程序, 禁止 ECU 下载安装第三方固件升级程序。同时 ECU 在固件升级时, 要支持固件认证和完整性校验。并且 ECU 要支持回滚机制, 确保升级失败后固件仍可回退到之前的版本, 确保升级的可靠性, 如文献[104]。区块链作为一种分布式账本, 具有数据不可篡改的特性。根据这一特性, 有研究将区块链引入 ECU 的固件更新中, ECU 向区块链网络中的节点请求最新固件来完成更新和确认固件的正确性, 如文献[105]。有研究引入了基于 PKE 的对称加密算法和椭圆曲线算法、RSA 加密算法, 如文献[106-108], 保证 ECU 存储数据的机密性和访问控制。但是 ECU 的计算能力和存储能力均受限, 不是所有的 ECU 都能支持这些加密算法, 同时加解密会降低通信实时性。如今车载设备的固件更新多是通过 OTA(Over the Air, OTA)技术来无线远程更新。OTA 需解决身份认证和数据完整性两个问题, 现有研究通过多个安全签名、生物特征(如虹膜)验证等手段, 来实现固件的安全更新, 如文献[109-111]。

5 发展趋势与展望

5.1 车联网安全发展趋势

移动互联网和智能化设备的快速发展必然驱使车联网向着网络化和智能化发展, 车辆与外界环境的交互将会变得越来越多样性, 而其中存在的安全问题也将不断涌现, 因此, 建立完善的车联网安全防护体系是必要的, 在此前提之下, 网络级、平台级和组件级三大安全层级的研究必将更加广泛和深入。网络级安全中建立高实时性的多场景认证技术

仍然是一个巨大挑战, 同时对于高速移动的车辆所面临的多样化未知攻击问题, 可以借助目前人工智能领域的机器学习、深度学习和自然语言处理等技术, 完成入侵行为的自动化检测与报告。平台级安全中, 为了保证 CAN 总线高速实时性的需求, 考虑内部消息敏感程度的不同, 数据帧容量的限制, 建立差异化的安全策略将会成为一个重要研究方向。而在组件级安全中, 软件安全和云数据安全将成为研究重点, 如软件漏洞检测、云服务平台安全防护、数据隐私保护等。同时随着车辆智能化的发展, 自动驾驶技术将逐步取代人工驾驶, 而其中安全问题则亟待解决。1) 自动驾驶汽车主要通过环境感知系统识别周围环境并做出相应决策, 然而环境感知增加了大量的智能化设备, 如雷达、摄像头、传感器等, 在增加车联网中网络节点数的同时, 也增加了攻击者攻击的入口, 使得攻击者可以通过此类设备的安全漏洞或者干扰物理设备的感知结果引起车载传感器的误判从而引起安全事故; 2)自动驾驶汽车的智能决策过程需要综合考虑大量的声音、图片和视频信息, 此类信息需要经过决策系统的计算完成最终的决策过程, 因此高性能处理器甚至是云计算组件的加入将会成为车联网安全中又一重要威胁; 3)自动驾驶汽车智能控制系统控制着整个车辆的运作, 其本身的安全性成为整个车联网系统的关键, 攻击者一旦成功入侵驾驶控制系统, 也就控制了整个车辆的安全, 甚至影响到整个车联网系统的安全。因此自动驾驶的安全性应该受到更加广泛的重视。

5.2 车联网安全研究展望

在网络级安全范畴中, 除了各种通信协议和认证协议的研究之外, 网络入侵检测是非常重要环节。利用机器学习、深度学习等方法进行自动化的网络入侵检测已经广泛且成熟的应用于传统网络环境中, 但是由于车联网环境中随着车辆的高速移动, 网络拓扑结构和车辆所处外部环境不断变化, 未知的网络攻击将不断涌现, 传统网络中的检测方案主要基于大量的标记训练数据来建立检测模型, 这在资源受限且高速移动的车联网环境中显然无法适用。考虑到车联网的系统架构, 车-车、车-云可以共享数据, 因此可以依靠车联网系统使得训练数据在不同的网络中实现共享, 当车辆进入陌生网络时, 只需要向目标网络中的车辆或者云服务平台请求该网络中的数据集, 并且依靠迁移学习技术高效的完成入侵检测模型在此网络下的更新过程, 从而应对随车辆移动而不断变化的未知攻击。

车内网总线中的报文由于总线高速的特性使得难以使用传统的加密或者认证协议进行保护, 因此如何保证总线内报文没有被攻击者篡改从而确保车辆安全运行是一项重要的任务。由于同一个 ID 下的报文具有相关性, 因此基于自然语言处理技术的文本相似度检测能够成为一项解决方案, 此类可以将报文本文通过 word2vec 等技术表示为向量, 然后结合深度学习相关算法进行相似度预测或者序列预测, 一旦异常检测模型检测出当前出现的总线报文不满足要求, 那么则可以判定该条报文遭到攻击者篡改, 进而可以产生对应的报警信息, 向系统报告当前车内网络正遭受入侵威胁。另一方面, 总线的高速特性和消息敏感程度的差异性是车内网平台的显著特点, 因此在车内网平台安全系统中如何利用差异化的消息敏感程度并且保证总线高速传递特性是至关重要的问题。差异化的安全策略可以针对性的对不同敏感程度的消息内容进行加密或者认证, 将能够在保证总线效率的前提下保护总线的通信内容。根据车辆整体系统结构的不同, 功能不同的 ECU 其交互频繁程度也不同, 因此可以尝试对 ECU 按照其功能性区分, 建立不同的域结构, 由此可将 ECU 的通信分为域内通信和域间通信, 这样可以大量的减少所需存储的密钥数量。同时 ECU 消息的敏感程度和其功能也具有一定关系, 针对性的将敏感程度较高的总线报文进行加密和认证处理, 将敏感程度低的报文不做处理, 可以有效的降低各个 ECU 的计算开销并且提高总线的效率。

组件级安全防护中因为组件种类多且数量大而导致漏洞种类众多, 然而现有的漏洞扫描检测技术往往只是针对某一种操作系统, 不具有通用性, 无法对漏洞特征进行统一建模, 不能对车联网中的漏洞进行全方位地进行检测, 而且漏洞修补方法不能根据不同的组件选择合适的修补方法, 即不具有环境自适应性。因此, 为了能系统地保护车联网组件安全, 需要提出一种跨组件操作系统的漏洞检测及环境自适应的漏洞修补方法, 实现统一的漏洞特征建模及环境感知的漏洞修补, 如建立漏洞库, 收集不同组件的漏洞, 通过半监督学习、启发式学习等方法实现对漏洞特征提取并建模, 同时可以考虑借助机器学习、深度学习等技术提高漏洞检测的效率和准确率。

6 总结

本文主要讨论了目前车联网体系中存在的安全问题以及对应的研究现状。首先根据车联网的体系结构, 由外而内的介绍了车联网的主要构成, 并且

指出了当前车联网安全威胁主要来自于三个层级: 网络级、平台级和组件级, 并全面而具体的分析了三个层级的主要安全威胁。并且对当前主要安全问题的研究现状进行了分析和总结, 指出了当前研究的局限性和未来研究的重点内容。最后本文给出了车联网安全的未来发展趋势和研究展望, 为进一步的研究工作奠定了基础。

参考文献

[1] China's Internet of Vehicles set for fast growth. http://www. chinadaily.com.cn/business/tech/201709/14/content_31992978.htm 09.2017.

[2] The Internet of Cars. https://www.transportation.gov/content/internet-cars. 2015.11

[3] The Tesla IoT Car: Case Study. https://blogmitcnc.org/2014/08/21/the-tesla-iot-car-case-study/2014.08

[4] 2018 年我国车联网产业规模或将达两千亿. http://tech.hqew.com/fangan_1881417. 2017.05

[5] 360 网络攻防实验室公布无需钥匙即可开走特斯拉的漏洞. https://bbs.kafan.cn/thread-1804633-1-1.html 2015.01

[6] Shock at the wheel: your Jeep can be hacked while driving down the road. https://www.kaspersky.com/blog/remote-car-hack/9395/ 2015.07

[7] 百度成功破解 T-BOX 系统 车联网安全迈上新高度. http://www.elecfans.com/qichedianzi/20161130453520.html 2016.11

[8] 腾讯科恩实验室成功远程入侵特斯拉 为全球首次. http://tech.qq.com/a/20160920/048201.htm 2016.09

[9] Watch thieves stealing a Tesla through keyfob hack and struggling miserably to unplug it. https://electrek.co/2018/10/21/tesla- stealing-video-keyfob-hack/ 2018.10

[10] ECU (电子控制单元)https://baike.baidu.com/item/ECU/19446326

[11] 智能网联汽车信息安全白皮书. https://www.bangcle.com/upload/file/20170613/14973588911862.pdf 2016

[12] J. P. Walters, Z. Liang, W. Shi, and V. Chaudhary. “Wireless sensor network security: A survey”. *Security in distributed, grid, mobile, and pervasive computing*, 2007.

[13] Q. P. Pei, Y. L. Shen, and J. F. Ma. “Survey of Wireless Sensor Network Security Techniques.” Journal on Communications vol.28, no. 8, pp. 113-122, 2007.
(裴庆祺, 沈玉龙, 马建峰. 无线传感器网络安全技术综述[J]. 通信学报, 2007, 28(8):113-122.

[14] A Perrig, J Stankovic, and D Wagner. “Security in wireless sensor networks,” *Communications of the ACM*, pp. 53-57, 2004.

[15] S. K. Garg. “Wireless Network Security Threats.” *International Journal of Information Dissemination and Technology*, 2011, vol. 1, no. 2, pp. 110-113, 2011.

[16] J. M. De Fuentes, A Isabel González-Tablas, and A Ribagorda. “Overview of security issues in vehicular ad-hoc networks.” *Handbook of research on mobility and computing: Evolving technologies and ubiquitous impacts*. IGI Global, pp. 894-911, 2011.

[17] A. Kavianpour, and C. Michael. Anderson. “An Overview of Wireless Network Security.” *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*. IEEE, pp. 306-309, 2017.

[18] M. L. Das, A Saxena, and V. P. Gulati. “A dynamic ID-based remote user authentication scheme.” *IEEE Transactions on Consumer Electronics* vol. 50, no. 2, pp. 629-631, 2004.

[19] W. Shi, and P. Gong. “A new user authentication protocol for wireless sensor networks using elliptic curves cryptography.” *International Journal of Distributed Sensor Networks*, vol. 9, no. 4, pp. 730-831, 2013.

[20] A. L. Buczak, and E Guven. “A survey of data mining and machine learning methods for cyber security intrusion detection.” *IEEE Communications Surveys & Tutorials,* vol. 18, no. 2, pp. 1153-1176, 2016.

[21] P. Mishra, et al. “Intrusion detection techniques in cloud environment: A survey.” *Journal of Network and Computer Applications,* pp. 18-47, 2017.

[22] L. D. Wang, and R. Jones. “Big data analytics for network intrusion detection: A survey.” *International Journal of Networks and Communications*, vol. 7, no. 1, pp. 24-31, 2017.

[23] D. Y. Chen, and H. Zhao. “Data security and privacy protection issues in cloud computing.” *2012 International Conference on Computer Science and Electronics Engineering*, Vol. 1, pp. 647-651, 2012.

[24] S. Subashini, and V. Kavitha. “A survey on security issues in service delivery models of cloud computing.” *Journal of network and computer applications*, vol. 34, no.1 pp. 1-11, 2014

[25] A. Singh, and K. Chatterjee. “Cloud security issues and challenges: A survey.” *Journal of Network and Computer Applications*, pp. 88-115, 2017.

[26] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, “A survey of mobile malware in the wild.” *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*. ACM, pp. 3-14, 2011.

[27] P. Faruki, et al. “Android security: a survey of issues, malware penetration, and defenses.” *IEEE communications surveys & tutorials*, vol. 17, no. 2, pp. 998-1022, 2015.

[28] E. Gandotra, D. Bansal, and S. Sofat. “Malware analysis and classification: A survey.” *Journal of Information Security*, vol. 5, no. 2, pp. 56-64, 2014.

[29] ISO: 11898-1: 2003 - Road Vehicles - Controller Area Network.

International Organization for Standardization, Geneva, Switzerland, 2013.

[30] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, and S. Savage, “Experimental security analysis of a modern automobile.” *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010.

[31] C. Miller, and Chris Valasek. “Remote exploitation of an unaltered passenger vehicle.” *Black Hat USA*, 2015.

[32] 360 又“黑”了一辆特斯拉，干扰传感器的“N”种方. http://www.sohu.com/a/110068097_118790, 2016.08

[33] Researchers Discover Vulnerability in Tesla Model S Key. https://latesthackingnews.com/2018/09/13/researchers-discover-vulnerability-in-tesla-model-s-key/, 2018.09

[34] 孙荣创, 张蕾, 王萍. “浅谈单片机常见攻击技术及应对策略”[J]. *中国科技信息*, pp.124-124, 2006(16).

[35] 2016 智能网联汽车信息安全年度报告. https://skygo.360.cn/2017/04/12/2016-skygo-annual-report/2017.04

[36] 车联网丨十三五规划100个重大项目(第五十四项) 加快构建车联网. http://3g.163.com/dy/article/DE92JICU0511PFUO.html 2018.04

[37] J. B. Kenney, “Dedicated short-range communications (DSRC) standards in the United States.” *Proceedings of the IEEE*, vol. 99, no.7, pp. 1162-1182, 2011.

[38] H. A. Omar, W. H. Zhuang, and L. Li. “VeMAC: A TDMA-based MAC protocol for reliable broadcast in VANETs.” *IEEE transactions on mobile computing*, vol. 12, no. 9, pp. 1724-1736, 2013.

[39] F. Yang, et al. “A multi‐channel cooperative clustering‐based MAC protocol for V2V communications.” *Wireless Communications and Mobile Computing*, vol. 16, no. 18, pp. 3295-3306, 2016.

[40] S. R. Jiang, X. Y. Zhu, and L. M. Wang. “An efficient anonymous batch authentication scheme based on HMAC for VANETs.” *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no.8 pp. 2193-2204, 2016.

[41] Y. Wang, H. Zhong, Y. Xu, and J. Cui, “ECPB: Efficient Conditional Privacy-Preserving Authentication Scheme Supporting Batch Verification for VANETs.” *IJ Network Security*, vol. 18, no. 2, pp. 374-382, 2016.

[42] M. Safkhani, N. Bagheri, P. Peris-Lopez, A. Mitrokotsa, and J. C. Hernandez-Castro, “Weaknesses in another gen2-based rfid authentication protocol.” *2012 IEEE International Conference on RFID-Technologies and Applications (RFID-TA)*. IEEE, 2012.

[43] X. Yi, L. Wang, D. Mao, and Y. Zhan, “An gen2 based security authentication protocol for RFID system.” *Physics Procedia*, pp. 1385-1391, 2012.

[44] X. H. Li, H. Liu, F. Wei, J. Ma, and W. Yang, “A lightweight anonymous authentication protocol using k-pseudonym set in wireless networks.” *2015 IEEE Global Communications Conference (GLOBECOM)*. IEEE, pp. 1-6, 2015.

[45] C. Zhong, X. H. Li, Y. Y. Song, A Lightweight Anonymous Authentication Protocol Based on Shared Key in Wireless Network, Chinese Journal of Computers, vol. 41, no. 5, pp. 1157-1171, 2018. (钟成, 李兴华, 宋园园,等. 无线网络中基于共享密钥的轻量级匿名认证协议[J]. 计算机学报, 2018(5).)

[46] R. Mitchell, and R Chen. “A survey of intrusion detection in wireless network applications.” *Computer Communications* , pp. 1-23, 2014.

[47] I, Butun, S. D. Morgera, and R. Sankar. “A survey of intrusion detection systems in wireless sensor networks.” *IEEE communications surveys & tutorials*, vol. 16, no. 1, pp. 266-282, 2014.

[48] S. Shamshirband, N. B. Anuar, and M. L. M Kiah, “An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique.” *Engineering Applications of Artificial Intelligence*, vol. 26, no. 9, pp. 2105-2127, 2013.

[49] S. Shamshirband, N. B. Anuar , M. L. Kiah, and A. Patel. “An appraisal and design of a multi-agent system based cooperative wireless intrusion detection computational intelligence technique.” *Engineering Applications of Artificial Intelligence* vol. 26, no. 9, pp. 2105-2127, 2013.

[50] D. Krishnan, “A Distributed Self-Adaptive intrusion detection system for Mobile Ad-hoc Networks using tamper evident mobile agents.” *Procedia Computer Science* , pp. 1203-1208, 2015.

[51] A. A. Aburomman, and M. B. I. Reaz, “A novel SVM-kNN-PSO ensemble method for intrusion detection system.” *Applied Soft Computing*, pp. 360-372, 2016.

[52] A. A. Aburomman, and M. B. I. Reaz. “A survey of intrusion detection systems based on ensemble and hybrid classifiers.” *Computers & Security* vol. 65, pp. 135-152, 2017.

[53] R. A. R. Ashfaq, X. Z. Wang, J. Z. Huang, Abbas, H., and Y. L. He. “Fuzziness based semi-supervised learning approach for intrusion detection system.” *Information Sciences*, vol. 378, pp. 484-497, 2017.

[54] M. F. Xu, X. H. Li, H. Liu, and C. Zhong, “An Intrusion Detection Scheme Based on Semi-Supervised Learning and Information Gain Ratio.” *Journal of Computer Research and Development* vol. 54, no. 10, pp. 2255-2267, 2017.
(许勐璠, 李兴华, 刘海,等. 基于半监督学习和信息增益率的入侵检测方案[J]. 计算机研究与发展, 2017, 54(10):2255-2267.)

[55] P. Dinadayalan, S. Jegadeeswari, and D. Gnanambigai. “Data security issues in cloud environment and solutions.” *2014 World Congress on Computing and Communication Technologies*. IEEE, 2014.

[56] C. Lin, W. B. Su, K. Meng, et al, “Cloud Computing Security: Ar-

chitecture, Mechanism and Modeling"[J]. Chinese Journal of Computers, vol. 36, no. 9, pp. 1765-1784, 2013.
(林闯, 苏文博, 孟坤,等. 云计算安全:架构、机制与模型评价[J]. 计算机学报, 2013, 36(9):1765-1784.)

[57] M. Elingiusti, L. Aniello, L. Querzoni, and R. Baldoni. "Malware Detection: A Survey and Taxonomy of Current Techniques." *Cyber Threat Intelligence*, pp. 169-191, 2018.

[58] A. Shabtai, U. Kanonov, Y. Elovici, C. Glezer, and Y. Weiss. "Andromaly": a behavioral malware detection framework for android devices." *Journal of Intelligent Information Systems*, vol. 38, no. 1, pp. 161-190, 2012.

[59] Y. Ye, T. Li, D. Adjeroh, and S. S. Iyengar. "A survey on malware detection using data mining techniques." *ACM Computing Surveys (CSUR),* vol. 50, no. 3, pp. 41-55, 2017.

[60] B. Groza, S. Murvay, "Efficient protocols for secure broadcast in controller area networks." *IEEE Transactions on Industrial Informatics* , vol. 9, no. 4, pp. 2034-2042, 2013.

[61] A. Van Herrewege, D. Singelee and I. Verbauwhede, "CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus," in *ECRYPT Workshop on Lightweight Cryptography*, 2011.

[62] B. Groza, S. Murvay and A. Van Herrewege. "LiBrA-CAN: a lightweight broadcast authentication protocol for controller area networks." in *International Conference on Cryptology and Network Security(CANS)*. Springer, pp. 185-200, 2012.

[63] S. Murvay, and B. Groza, "Source identification using signal characteristics in controller area networks" *IEEE Signal Processing Letters*, vol. 21, no. 4, pp. 395-399, 2014.

[64] W. Choi, H. J. Jo and S. Woo. "Identifying ecus using inimitable characteristics of signals in controller area networks". *IEEE Transactions on Vehicular Technology*, vol. 67, no 6, pp. 4757-4770, 2018.

[65] D. K. Nilsson, U. E. Larson and E. Jonsson. "Efficient in-vehicle delayed data authentication based on compound message authentication codes," in *2008 IEEE 68th Vehicular Technology Conference (VTC)*. pp. 1-5, 2008.

[66] W. Choi, H. J. Jo and D. H. Lee. "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN," *IEEE Transactions on Intelligent Transportation Systems*, vol. 16,no. 2, pp. 1-14, 2014.

[67] A. I. Radu and F. D. Garcia. "LeiA: a lightweight authentication protocol for CAN", in *European Symposium on Research in Computer Security. Springer (ESORICS)*, pp. 283-300, 2016.

[68] R. Kurachi, Y. Matsubara and H. Takada. "CaCAN-centralized authentication system in CAN (controller area network)," in *14th Int. Conf. on Embedded Security in Cars (ESCAR 2014)*. 2014.

[69] N. Bravo, S. Koppula and Matthew Chang. "A Public-Key Authentication Scheme for Controller Area Networks", 2015.

[70] A. Hazem and H. A. Fahmy. "LCAP-a lightweight can authentication protocol for securing in-vehicle networks." in *10th escar Embedded Security in Cars Conference (ESCAR 2012)*, Berlin, Germany. Jun. 2012.

[71] J. A. Bruton. "Securing can bus communication: An analysis of cryptographic approaches," *National University of Ireland, Galway*, 2014.

[72] TRILLIUM SECURE (IOT AUTOMOTIVE CYBER SECURITY SAAS), https://pitchbook.com/profiles/company/162130-06 ,Oct. 2016

[73] M. Muter and N. Asaj. "Entropy-based anomaly detection for in-vehicle networks," *Intelligent Vehicles Symposium IEEE*, pp. 1110-1115, 2011.

[74] M. R .Moore, R. A. Bridges and F. L. Combs. "Modeling inter-signal arrival times for accurate detection of CAN bus signal injection attacks: a data-driven approach to in-vehicle intrusion detection," in *Conference on Cyber and Information Security Research (CCISR)*. Nov. 2017.

[75] B. Groza and S. Murvay. "Efficient Intrusion Detection With Bloom Filtering in Controller Area Networks," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 4, pp. 1037-1051, 2019.

[76] A. Taylor, N. Japkowicz, and S. Leblanc. "Frequency-based anomaly detection for the automotive CAN bus," in *Industrial Control Systems Security (WCICSS)*, pp. 45-49, 2015.

[77] S. N. Narayanan, S. Mittal and A. Joshi. "Using Data Analytics to Detect Anomalous States in Vehicles," *Computer Science*, 2015.

[78] K. T. Cho and K. G. Shin. "Fingerprinting electronic control units for vehicle intrusion detection," in *25th USENIX Security Symposium* (USENIX Security 16), pp. 911-927. 2016.

[79] A. Taylor, S. Leblanc and N. Japkowicz. "Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks," in *Data Science and Advanced Analytics (DSAA), 2016 IEEE International Conference on. IEEE*. pp. 130-139, 2016.

[80] M. J. Kang and J. W. Kang. "Intrusion detection system using deep neural network for in-vehicle network security". *PloS one*, vol.11, no. 6, 2016.

[81] C. Wang, Z. Zhao and L. Gong. "A Distributed Anomaly Detection System for In-Vehicle Network Using HTM," *IEEE ACCESS*, vol. 6, pp. 9091-9098, 2018.

[82] C. Jichici, B. Groza and S. Murvay. "Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks," in *International Conference on Security for Information Technology and Communications. Springer (ICSITCS)*, pp. 109-125, 2018.

[83] M. Wolf, A. Weimerskirch and C. Paar, "Security in automotive bus systems," in *Workshop on Embedded Security in Cars.*

(ESCAR), 2004.

[84] G. Han, H. Zeng and Y. Li. "SAFE: Security-aware flexray scheduling engine," in *Proceedings of the conference on Design, Automation & Test in Europe. European Design and Automation Association*, Aug. 2014.

[85] J. H. Kim, S. H. Seo and N. T. Hai. "Gateway framework for in-vehicle networks based on CAN, FlexRay, and Ethernet," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 10, pp. 4472-4486, 2015.

[86] S. Seifert and R. Obermaisser. "Secure automotive gateway—secure communication for future cars," in *2014 12th IEEE International Conference on Industrial Informatics (INDIN)*. pp. 213-220, 2014.

[87] R. Gopalakrishna, E. H. Spafford, and J. Vitek., "Faultminer: discovering unknown software defects using static analysis and data mining", 2006.

[88] J. Viega, J. T. Bloch, Y. Kohno, and G. McGraw, "ITS4: A static vulnerability scanner for C and C++ code," *Proceedings 16th Annual Computer Security Applications Conference (ACSAC'00). IEEE,* pp. 257-267, 2000.

[89] A. Costin, J. Zaddach, A. Francillon, and D. Balzarotti, "A large-scale analysis of the security of embedded firmwares," *23rd {USENIX} Security Symposium ({USENIX} Security 14)*. pp. 95-110, 2014.

[90] D. Davidson, B. Moench, S. Jha, and T. Ristenpart, "FIE on firmware: finding vulnerabilities in embedded systems using symbolic execution"*//Presented as part of the 22nd {USENIX} Security Symposium ({USENIX} Security 13)*. pp. 463-478, 2013.

[91] S. Michel, P. Triantafillou, and G. Weikum. "KLEE: a framework for distributed top-k query algorithms"*//Proceedings of the 31st international conference on Very large data bases. VLDB Endowment,* pp. 637-648, 2015.

[92] Y. Shoshitaishvili, R. Wang, C. Hauser, and C. Kruegel. "Firmalice - Automatic Detection of Authentication Bypass Vulnerabilities in Binary Firmware," *Network and Distributed System Security Symposium (NDSS),* 2015.

[93] Y. Shoshitaishvili, R. Wang, C. Salls, N. Stephens, M. Polino, A .Dutcher, J. Grosen, S. Feng, C. Hauser, C. Kruegel, and G. Vigna, "SOK: (State of) The Art of War: Offensive Techniques in Binary Analysis." *2016 IEEE Symposium on Security and Privacy (SP). IEEE,* pp. 138-157, 2016.

[94] 黄涛."基于模糊测试的车控网络漏洞挖掘技术研究与实现"[硕士学位论文]. 电子科技大学, 2018.

[95] Z. H. Dai, B. Zhao, and T. Wang, "A Fuzzing Test Method for Embedded Device Firmware Based on Taint Analysis", *Journal of Sichuan University (Engineering Science Edition,* vol.48,no.2, pp. 125-131, 2016.
(戴忠华, 赵波, 王婷, "基于污点分析的嵌入式设备固件模糊测试方法". *四川大学学报(工程科学版),* 48(2):pp. 125-131, 2016.)

[96] J. Zaddach, L. Bruno, A. Francillon, and D. Balzarotti, "AVATAR: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares".*//Network and Distributed System Security Symposium (NDSS)*, pp. 1-16, 2014.

[97] C. Shan, G. P. Jing, and C. Z. Hu, "8031 Microcontroller Software Vulnerability Detection Algorithm Based on Vulnerability Knowledge Database", *Transactions of Beijing Institute of Technology*, vol. 37, no. 4, pp. 371-375, 2017.
(单纯, 荆高鹏, 胡昌振,等. "基于漏洞知识库的 8031 单片机系统软件漏洞检测算法". *北京理工大学学报,* 2017, (4):371-375.)

[98] Y. Shi, Y. E. Sagduyu, K. Davaslioglu, and R. Levy, "Vulnerability Detection and Analysis in Adversarial Deep Learning," *Guide to Vulnerability Analysis for Computer Networks and Systems*. Springer, Cham, pp. 211-234, 2018.

[99] M. Chandramohan, "Scalable analysis for malware and vulnerability detection in binaries [Ph.D. dissertation]" *Nanyang Technological University*, 2018.

[100] R. Russell, L. Kim, L. Hamilton, T. Lazovich, J. Harer, O. Ozdemir, P. Ellingwood, and M. McConley, "Automated Vulnerability Detection in Source Code Using Deep Representation Learning". in *2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA),* pp. 757-762, 2018.

[101] S. D. Yang, G. M. Liang, and K. Yu, "Study on discovery technology against ARM-based embedded system vulnerability", *Modern Electronics Technique*, vol. 38, no. 18, pp. 57-59, 2015.
(杨世德, 梁光明, 余凯. "基于 ARM 嵌入式系统底层漏洞挖掘技术研究". *现代电子技术*, 2015, 38(18):57-59.)

[102] P. H. Zhang, X. Tian, and K. W. Lou, "Firmware vulnerability analysis based on formal verification of software and hardware," *Chinese Journal of Network and Information Security*, vol. 2, no. 7, 2016.
(张朋辉, 田曦, 楼康威. "基于软硬件协同形式验证的固件漏洞分析技术". *网络与信息安全学报*, 2016, 2(7))

[103] D. Li, Q. Yin, and J. Lin, "Firmware Vulnerability Detection in Embedded Device Based on Homology Analysis." *Computer Engineering*, vol. 43, no. 1, pp. 72-78, 2017.
(李登, 尹青, 林键, "基于同源性分析的嵌入式设备固件漏洞检测". *计算机工程,* 2017, 43(1):pp. 72-78.)

[104] Y. Komano, Z. Xia, T. Kawabata, H. Shimizu, "Efficient and Secure Firmware Update/Rollback Method for Vehicular Devices," *International Conference on Information Security Practice and Experience*. Springer, Cham, pp. 455-467, 2018.

[105] B. Lee, J. H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment." *The Journal of Supercomputing*, vol.73, no.3, pp.1152-1167, 2017.

[106] S Alam, “Securing Vehicle Electronic Control Unit (ECU) Communications and Stored Data [Ph.D. dissertation]”. Queen's University, 2018.

[107] K. Mayilsamy, N. Ramachandran, and V. S. Raj, “An integrated approach for data security in vehicle diagnostics over internet protocol and software update over the air”. *Computers & Electrical Engineering*, vol. 71, pp. 578-593, 2018.

[108] M. Steger, C. Boano, M. Karner, J. Hillebrand, W. Rom, and K. Römer “SecUp: secure and efficient wireless software updates for vehicles,” 2016 *Euromicro Conference on Digital System Design* (DSD). IEEE, pp. 628-636, 2016.

[109] G. Djabarov, G. Hotz, S. A. Gandhi. “Multiple system images for over-the-air updates”: U.S. Patent 8,631, 239. 2014.

[110] M. Khurram, H. Kumar, A. Chandak, V. Sarwade, N. Arora, and T. Quach, “Enhancing connected car adoption: Security and over the air update framework,” *2016 IEEE 3rd World Forum on Internet of Things (WF-IoT). IEEE*, pp. 194-198, 2016.

[111] A. Chawan, W. Sun, A. Javaid, “Security Enhancement of Over-the-Air Update for Connected Vehicles,” *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, Cham, pp. 853-864, 2018.

李兴华 现西安电子科技大学博士生导师, 博士, 教授, 主要研究领域为网络与信息安全、隐私保护、云计算、安全协议形式化方法。Email: xhli1@mail.xidian.edu.cn

钟成 现西安电子科技大学硕士研究生, 主要研究领域为网络与信息安全, 车联网安全, 入侵检测。Email: czhongcs@126.com

陈颖 现西安电子科技大学硕士研究生, 主要研究领域为网络与信息安全, 车联网安全。Email: chenying3321@qq.com

张会林 现西安电子科技大学硕士研究生, 主要研究领域为网络与信息安全, 车联网安全。Email: huilin_zhang@qq.com

翁健 暨南大学教授、博士生导师, 主要研究方向为密码学与信息安全。Email: cryptjweng@gmail.com