专题：车联网与安全

智能网联汽车网络安全浅析

李玉峰[1]，陆肖元[1,2]，曹晨红[1]，李江涛[1]，朱泓艺[2]，孟楠[3]
（1. 上海大学，上海 200444；2. 国家宽带网络技术及应用工程研究中心，上海 200436；
3. 中国信息通信研究院，北京 100191）

摘　要：汽车工业正经历着向智能化、网联化范式的转变，（半）自动驾驶汽车通过新一代信息通信技术实现车与云平台、车与车、车与路、车与人的全方位网络连接。当汽车开始变成车轮上的联网计算机时，网络安全成为一个重大挑战，其威胁的作用范围从虚拟空间延伸到了物理空间，危害的对象已经上升为人类生命。介绍了智能汽车的电子/电气结构和网络结构，阐述了智能汽车的网络安全需求，指出了智能网联车辆系统的若干网络攻击，并针对这些攻击对可用的防御措施进行了调查。最后，探讨了未来可能的技术方向。

关键词：自动驾驶；车联网；智能网联汽车；网络安全
中图分类号：TP302
文献标识码：A
doi: 10.11959/j.issn.1000–0801.2020127

A survey of cybersecurity for intelligent connected-automated vehicle

LI Yufeng[1], LU Xiaoyuan[1,2], CAO Chenhong[1], LI Jiangtao[1], ZHU Hongyi[2], MENG Nan[3]
1. Shanghai University, Shanghai 200444, China
2. National Engineering Research Center for Broadband Networks & Applications, Shanghai 200436, China
3. China Academy of Information and Communications Technology, Beijing 100191, China

Abstract: The automotive industry is experiencing a shift to an intelligent and connected paradigm. (Semi-) Autonomous vehicles use a new generation of information and communication technologies to realize a full range of interactions between vehicles and cloud, vehicles and vehicles, vehicles and roads, and vehicles and pedestrian, etc. When cars started to become connected computers on wheels, network security became a major challenge, and because the scope of cyber threats extended from virtual space to physical space, the harm of cybersecurity had risen to human life. The electronic/electrical structure, in-vehicle network structure, and out-of-vehicle network structure of intelligent vehicles were introduced, the security requirements of vehicle networks were elaborated, several cyber-attacks against connected-automated vehicle (CAV) were pointed out, the available defense measures against these attacks were addressed. The advantages and disadvantages of these measures were summarized. Finally, possible defense measures and directions in the future were discussed to further ensure the security of CAV.

Key words: automated driving, internet of vehicles, intelligent connected-automated vehicle, cybersecurity

收稿日期：2020–02–20；修回日期：2020–04–03
基金项目：广东省科技计划基金资助项目（No.20180113）；国家重点研发计划基金资助项目（No.2017YFB0803200）
Foundation Items: Guangdong Science and Technology Program (No.20180113), The National Key Research and Developement Program of China(No.2017YFB0803200)

1　引言

目前，全世界每年约有 135 万人死于交通事故[1]。这些事故的常见原因中 94%涉及人为错误[2]，其中，在驾驶时分心是其中的一个重要原因。自动驾驶技术对路况的高度了解和独立于人的判断力，可以为减少交通事故、挽救人类生命做出贡献。

自动驾驶汽车是智慧交通的重要组成部分，它通过新一代信息通信技术，实现车内及车与云平台、车与车、车与路、车与人的全方位网络连接。随着 5G 技术的诞生，智能网联汽车（connected-automated vehicle，CAV）的发展正面临着前所未有的机遇。2018 年，工业和信息化部在《车联网（智能网联汽车）产业发展三年行动计划》中提出，到 2020 年，车联网用户渗透率达到 30%以上，新车驾驶辅助系统（L2）的搭载率达到 30%以上，联网车载信息服务终端的新车装配率达到 60%以上[3]。

在引入自动驾驶和联网功能之前，汽车就存在很多可以利用的攻击面，只不过旧汽车架构依靠封闭网络，几乎没有外部通信来很好地保障其网络安全。自动驾驶和联网功能引入汽车，一方面将有效降低交通事故，提升交通效率，促进低碳环保，便捷人们的生活；另一方面，将使汽车越来越像一个“轮子上的联网计算机”，使网络安全成为汽车行业的一个重大挑战。例如，在 2015 年，Miller 和 Valasek 远程入侵了一辆吉普切诺基汽车，以控制音频、雨刷、转向和制动，这表明没有网络安全保障的汽车会威胁驾驶员的安全，从而导致超过 140 万辆汽车被召回[4]。此外，在 2016 年和 2017 年，腾讯科恩实验室的安全专家成功入侵了一辆特斯拉汽车[5]，以演示与联网车辆有关的安全威胁和潜在攻击。在 2017—2018 年年初进行的一项研究中，科恩实验室在多种宝马（BMW）车型上共发现了 14 个漏洞，其中 9 个漏洞需要对目标车辆进行实际的物理访问（接触或进入车辆），另外 5 个漏洞只需将手机联网[6]。安全专家通过车辆智能警报系统 App 成功劫持了汽车，从而非法执行了诸如启用/禁用防盗器、开关车门或切断发动机的操作[7]。

总的来说，CAV 的软硬件系统、AI 算法、车内外通信网络、云端平台中的任何一个环节出现安全问题，车辆都面临着被攻击危险，轻则影响单台车辆，重则同时影响成千上万辆汽车。因此，车联网安全不仅仅关系到个人的安全，还关系到整个社会的安全。

很多研究[7-8]认为，复杂的 CAV 系统很难准确预测网络安全问题。尽管人们都同意将网络安全放在 CAV 发展中的重要地位上，但面临的现实问题是：网络安全是一场无止境的博弈，具有足够技术技能和耐心的攻击者们总是会找到突破防护的方法，CAV 的网络空间中也不会有绝对的安全。实际上，全球第二大再保险公司——Munich Re 在一项研究中发现，接受调查的企业风险管理人员中有 55%的人将网络安全视为自动驾驶汽车的首要关注事项。更令人震惊的是，接受调查的公司中有 64%表示，他们完全没有做好应对网络安全的准备[9]。因此，重要的是研究攻击 CAV 的不同方法、降低攻击可能性的方法以及如何最大限度地减少损害。

2　自动驾驶汽车分级与结构

2.1　自动驾驶汽车的分级

2014 年，美国汽车工程师学会（SAE）制订了一套自动驾驶汽车分级标准，见表 1。在表 1 中，汽车自动化水平被分为 6 个等级，范围从 L0（没有自动驾驶功能）到 L5（完全自动驾驶）[10]。

动态驾驶任务（dynamic driving task，DDT）指在道路上驾驶车辆需要做出的实时操作和决策类行为，包括通过方向盘进行车辆横向运动，通过加减速操作车辆纵向运动，通过对物体和事件的检测、认知和响应，达到对车辆周围环境的监

表 1　美国汽车工程师学会自动驾驶分级标准

等级	名称（SAE）	SAE 定义	驾驶操作	驾驶环境监控	后备支援	作用域（条件及环境）
L0	无自动化	人全权操作，完成所有 DDT	人类	人类	人类	无
L1	驾驶支援	通过驾驶环境对方向盘或加减速中的一项提供驾驶支援，其他 DDT 都由人进行操作	人类和系统	人类	人类	部分
L2	部分自动化	通过驾驶环境对方向盘或加减速中的多项操作提供支援，其他 DDT 都由人进行操作	系统	人类	人类	部分
L3	条件自动化	在限定的 ODD 内自动完成所有的 DDT，根据系统请求人回应和干预	系统	系统	人类	部分
L4	高度自动化	在限定的 ODD 内自动完成所有 DDT，可以无须人类驾驶员介入	系统	系统	系统	部分
L5	完全自动化	在所有道路和环境下自动完成所有驾驶操作	系统	系统	系统	全域

测和执行对应操作等。运行设计域（operational design domain，ODD）指设计适用域或者运行范围，描述自动驾驶系统的使用条件及适用范围，例如天气环境、道路情况（直路、弯路的半径）、车速、车流量等。

2.2　智能汽车的功能结构

作为一种具有自主行为能力的智能系统，CAV 从功能上可以分为 3 部分：感知（感知车辆在其中运行的外部环境/环境）、决策与控制（针对感知到的外部环境/环境对车辆运动的决策和控制）以及车辆操纵平台（以实现车辆运动为目的的基础操作平台）[11]。本文按照这 3 部分功能，总结并给出了自动驾驶汽车的功能结构，如图 1 所示，具体介绍如下。

（1）感知部分

包括诸如激光雷达（light detection and ranging，LiDAR）、无线电探测和测距雷达、摄像机、全球定位系统（global positioning system，GPS）、

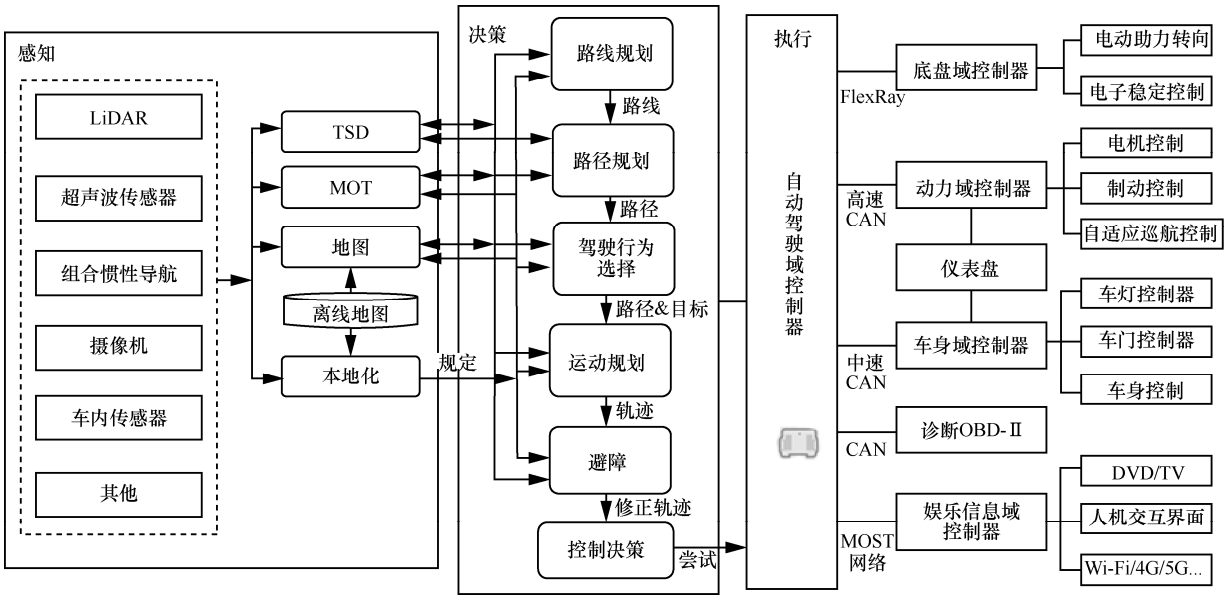


图 1　CAV 功能结构

惯性测量单元（inertial measurement unit，IMU）/里程表等传感器以及 TSD（traffic signalization detection，交通信号检测）子系统、MOT（moving object tracking，移动物体跟踪）子系统、地图子系统、本地化子系统。它接收各种传感器数据并进行信息融合，得到汽车驾驶任务所需要的信息和保证安全所需要的信息。

（2）决策部分

接收感知部分的信息以及有关传感器模型、道路网络、交通规则、汽车动力学等的先验信息，并综合处理 TSD、MOT 等信息，形成决策。决策部分包括路线规划、路径规划、驾驶行为选择、运动规划、避障和控制决策等。

（3）执行部分

执行部分是操纵车辆的平台。为了提升安全性能，当前自动驾驶车辆大都分域进行设计，包括底盘域控制器（电子助力、电子稳定等）、动力域控制器（电机、制动、自适应巡航等）、车身域控制器（车灯、车门、车身等）、诊断 OBD-Ⅱ、娱乐信息域控制器（DVD/TV、人机交互界面、Wi-Fi/4G/5G 等）等。

3　网络安全威胁与防御技术

3.1　智能网联汽车攻击面分析

自动驾驶和联网使汽车变成非常复杂的网络物理系统[12]，也使攻击者看到了新网络空间的更多攻击面，本文总结了 CAV 的攻击向量，如图 2 所示。

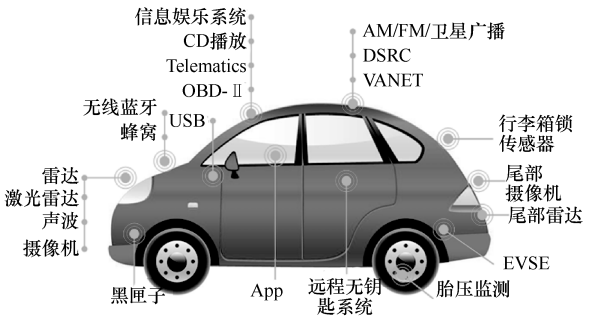


图 2　CAV 攻击向量

一方面，自动驾驶水平的不断提升，使汽车系统设计工程越来越庞大和复杂，质量控制变得越来越难，可被利用的设计缺陷可能越来越多。自动驾驶的发展伴随着软件代码的剧增，其软件代码可超过 1 亿行，代码数量远超过现代的操作系统或波音 757 等的代码数量[13]。每千行代码的缺陷数是评估软件质量指标的重要参数，参考文献[14]认为，每 1 000 行软件代码存在 5~20 个错误。软件缺陷中很大一部分是可以被攻击者利用的漏洞，这些程序漏洞可能导致该软件系统的完整性、可用性或机密性受损。

另一方面，各种方式的联网为乘客体验带来了明显的优势，但它同时也打开了智能网联汽车的各种攻击入口[15]。从车内网络来看，摄像头、雷达、激光雷达等感知器件，远程信息处理盒 T-BOX、车内网关等通信设备，CAN、LIN、MOST、FlexRay 和以太网等通信协议，OBD-Ⅱ端口、EV 充电接口和 USB 等外部接口以及各种车载网络应用等，在攻击者的视角里都是可以展开攻击的入口。从车辆与其他实体间的联网来看，它涵盖了 V2V（vehicle to vehicle，车辆到车辆）、V2I（vehicle to infrastructure，车辆到基础设施）、V2P（vehicle to pedestrian，车辆到行人）和 V2N（vehicle to network，车辆到网络）通信。为了实现 V2X 通信，车辆配备了不同的无线通信系统，例如专用短程 IEEE 802.11p /DSRC 技术和基于移动蜂窝通信系统的 C-V2X 技术。其中，C-V2X 包括 LTE-V2X 和 NR-V2X。这些通信技术以及车载自组织网络（vehicular Ad hoc network，VANET）的各种组网协议和技术，都是攻击者关注的重要攻击入口。此外，鉴于 CAV 的云平台应用以蜂窝网通信为基础，它面临“云、管、端”模式的安全风险及第三方入侵并破坏 CAV 系统关键功能的风险。

3.2　智能网联汽车网络安全需求

在概念设计和开发的早期阶段确定 CAV 的网

络安全需求，对于确保车辆和乘员安全非常重要，身份验证、完整性、私密性和可用性是安全系统最重要的先决条件[16]。

（1）身份验证

通过验证通信参与者身份并防止所有未经授权的访问来保护敏感信息和关键数据。CAV 中的身份认证包括涉及根访问应用程序的可靠身份验证、CAV 内部和外部连接的充分身份验证、敏感信息访问的身份验证和CAV内部设备的身份认证等。身份认证在系统设计的早期阶段需要仔细考虑，本质上，只有认证的各方才能够访问消息并检索其原始内容。为了满足认证要求，密钥管理和分发必须高效且准确。

（2）完整性

数据完整性主要指数据在其整个生命周期中必须完整。在 CAV 网络中，至关重要的是能够验证消息在传输过程中是否受到了诸如噪声和衰落之类的干扰影响以及攻击者故意的数据破坏。此外，软件的完整性、协议的完整性也是重要的安全要求。需要在设计时纳入完整性检查技术，如 Hash、安全协议和数据分组过滤等。

（3）隐私

CAV 网络包含个人身份、付款账户信息、通讯录信息、位置信息、车辆电子标识等隐私信息。在 V2V 和 V2I 的通信模式中，车辆采用不同的技术来共享信息（例如地理位置信息），而这些共享信息可能被恶意用来跟踪用户，因此需要进行隐私保护。此外，还需要考虑被动第三方（例如行人）数据的隐私保护，因为汽车可能会从未经授权的访问中收集、使用或共享隐私数据。

（4）可用性

可用性旨在将CAV安全状态维持在预定义和可接受的阈值以下。车联网是高度动态、实时响应的网络，在正常操作条件下实现持续可用已经具有相当大的挑战性，如果某些部件和软件在使用中面临必须更新或打补丁的情况时，更难保障可用性。因此，在设计初期就应该考虑冗余备份等可用性保障技术，当 CAV 网络某一部分出现故障或暂时中断时仍能保持网络可用。

3.3 网络攻击分类及技术对策

本节从认证/鉴权、可用性、完整性、隐私保护 4 个方面归纳了与智能网联汽车相关的网络攻击及相应的技术对策。

3.3.1 认证/鉴权攻击及相关技术对策

身份真实性是CAV网络的首要要求，以保护其免受多种攻击，包括 Sybil 攻击[17]、假冒攻击、密钥/证书复制攻击、GNSS 欺骗攻击等。身份认证过程中的任何缺陷都可能对整个网络造成严重后果。

- Sybil攻击意味着一个恶意的车辆创建或者盗用大量的假身份，向网络中的其他节点（例如其他车辆或路侧单元）发送虚假消息，而其他节点若无法检测到攻击者的真实身份，可能认为恶意消息是合法的。例如，当攻击者在某些位置创建大量假名时，某个位置的 CAV 数量增加，交通系统可能认为该位置存在严重的拥堵状况，从而迫使其他车辆更改自己的路线。为了克服这种攻击，任何通信实体都应使用加密方案和身份确认方案[18]。
- 假冒攻击意味着攻击者通过有效的网络标识符将信息传递给合法节点[19]。一个人假装自己是另一个人以获取利益或隐瞒其真实身份，在这种情况下，攻击者通常可以假冒授权用户访问授权方的登录详细信息和密码，攻击者可以通过钓鱼攻击和中间人攻击等方式，拦截、分析和寻找网络中带有身份验证信息的分组来实现假冒攻击。在 CAV 网络中，恶意节点可能冒充路边单元，诱骗用户泄露其身份验证详细信息。获取身份验证信息后，它可以用其访问分类信息，甚至可以用其作为与其他方的身份验证。攻击者还可能冒充其他车辆

来获利。已经提出了许多应对假冒攻击的方法，例如可以通过使用更完善的身份验证方案来应对假冒攻击[20]。

- 密钥/证书复制攻击是指一个或多个节点使用重复密钥/证书声明合法身份[21]。已有几种密钥管理方案可以应对这种攻击[22]。
- GNSS 欺骗攻击是利用欺骗、替换 GNSS 信号方式来伪造位置信息。GNSS 欺骗攻击可以引发其他类型的后续攻击。通过使用基于加密和经过身份验证的位置信息，可以防止此类攻击[23]。

3.3.2　可用性攻击及相关技术对策

可用性是 CAV 强制性要求，与传统的 IT 系统不同，网络安全 CIA（confidentiality，integrity and availability，机密性、完整性和可用性）三要素中，可用性是 CAV 系统中最重要的目标[24]。针对智能网联汽车的可用性攻击包括干扰攻击、恶意软件攻击、DoS（denial of service，拒绝服务）或 DDoS（distributed denial of service，分布式拒绝服务）攻击、黑洞攻击、消息延迟攻击等。

- 干扰攻击是发出干扰信号以破坏通信信道。GPS、雷达、激光雷达、摄像头等部件正确地感知信息是自动驾驶汽车正确决策的先决条件，这些部件容易受到光、电磁信号和其他物理形式的干扰攻击[26]。对干扰的检测具有一定的挑战性，设置冗余部件和多传感器数据融合方法是对抗干扰攻击的有效方法。
- 恶意软件攻击通常包括病毒、蠕虫、间谍软件、广告软件和特洛伊木马等。恶意软件对车联网具有极大的危害，由于车联网是高度动态的，并且经常需要更新，因此车辆必须确保其接收的更新信息的来源可信，如果车辆接收了伪造的更新要求并安装了恶意软件，则会带来很大风险，某些情况下还会导致严重故障。一般来说，可以通过使用恶意检测和防火墙来缓解这种攻击[27]。
- DoS 或 DDoS 攻击通过向 CAV 信息系统发送大量垃圾数据，阻断车辆内部网络（例如 CAN 总线）和/或外部网络（例如 C-V2X），以使车辆无法正常提供服务，该攻击通常被认为是对车辆相关信息系统可用性的最严重威胁之一。一般可以采用身份验证、防火墙、入侵检测等方案应对此类攻击[25]。
- 黑洞攻击。在黑洞攻击中，攻击者没有将数据分组转发到目的地，而是将其丢弃，从而造成了一个黑洞[28]。这种类型的攻击能够阻断车辆之间的信息，如果攻击者位于两辆 CAV 之间的关键路径中，则黑洞攻击可能意味着这两辆 CAV 无法彼此通信并变得孤立。黑洞攻击可以通过多种方式缓解：引入信誉机制；机器学习也可以在网络中实施，以检测恶意行为的车辆，预测哪些路径将是安全的。
- 消息延迟攻击。延迟的消息影响系统的正常工作，特别是对于时间紧迫的任务[29]。可以通过使用经过身份验证的计时方法来防止这种攻击。

3.3.3　数据完整性/数据信任攻击及相关技术对策

攻击者，尤其是那些经过身份验证的攻击者，可以轻松更改数据或创建虚假数据。因此，为了防止/减轻对数据完整性的攻击，必须进行安全的通信和信息加密。

- 伪造信息攻击：Sybil 攻击可以看作伪造信息攻击的一个例子。攻击者可以通过散布关于道路拥堵的伪造信息获利，他们还可以通过发布伪造信息造成拥堵，这种攻击实施简单、代价很低，所以可能会被广泛使用。而且由于车联网的分布式特性，这种攻击还可以产生很大的影响，如果攻击者能够让下一辆合法车辆转发了它的伪造

信息，那么这辆车就会在不知不觉中成为攻击者。通常使用消息签名和基于信誉的方案对这种形式的攻击进行防御[18]。

- 重放攻击：表示数据被欺诈性地重复或延迟，当攻击者使用先前生成的帧与其他节点通信时，将发生重播攻击。可以通过使用序列号、时间戳和安全通信来防止重放攻击[30]。
- 伪装攻击：是指使用伪造身份获得对系统的访问。例如一个恶意节点伪装成紧急车辆，使周围的车辆被诱使减速、改变车道等。有效检测恶意组件和身份验证可能是应对此类攻击的方法[31]。
- 数据篡改攻击：合法节点可以通过捏造和广播虚假消息来进行此攻击。主要的对策是签名并验证传输的消息[29]。

3.3.4 保密/隐私攻击及相关技术对策

CAV 的位置、智能交通系统安全消息和驾驶员个人信息等，未经授权不能泄露给非法实体。可以使用信息加密和安全通信来避免信息泄露。

- 窃听攻击是试图通过监听网络通信来窃取信息。对汽车内部网络来说，窃听轮胎气压、蓝牙或 CAN 消息是一种攻击[31]。此外，由于无线电频道的广播性质，为了更新驾驶状态而进行的 V2V 通信容易受到窃听攻击[32]。窃听可能不会影响可用性，但是敏感信息会泄露。可以使用安全通信来防止窃听。
- 拦截攻击拦截通信信号，然后尝试分析并提取有用的信息。Garcia 等[33]利用一个 40 美元的无线电设备拦截获取目标车钥匙的解锁信号，之后经过较低代价的计算，即可获取目标车钥匙的全部信息，进而任意解锁目标车辆。这个结果适用于全球将近 1 亿辆汽车，可以采用高等级的加密方案来减轻数据拦截攻击。

对智能网联汽车的威胁及对策做一个小结，见表 2。

表 2　智能网联汽车威胁及对策

攻击	属性	防御措施	参考文献
Sybil	身份认证、完整性	加密方案、身份确认方案和信誉机制	[17-18]
假冒攻击	身份认证、完整性	消息签名、身份验证等	[19-20]
密钥/证书复制攻击	身份认证、完整性	完善的密钥管理方案	[21-22]
欺骗攻击	身份认证、保密性	加密方案和身份验证	[23]
DoS/DDoS 攻击	可用性、身份认证	身份验证方案和防火墙、入侵检测等方法	[25]
干扰攻击	可用性、完整性	设置冗余部件，多传感器数据融合	[26]
恶意软件	可用性、保密性	恶意软件检测和防火墙等	[27]
黑洞攻击	可用性、完整性	信誉机制、基于机器学习的恶意行为检测	[28]
延迟攻击	可用性、身份认证	经过身份验证的计时方法	[29]
伪造信息	完整性、可用性、身份认证	消息签名和基于信誉的方案	[18]
重放攻击	完整性、身份认证	使用序列号，时间戳和安全通信	[30]
伪装攻击	完整性、身份认证	恶意行为检测和身份验证	[31]
篡改攻击	完整性、可用性	签名并验证传输的消息	[29]
窃听攻击	机密性、身份认证	加密方案，网络隔离机制	[31-32]
拦截攻击	机密性、身份认证	加密方案、身份验证	[33]

4　安全策略

应对CAV网络安全风险的常用方法除了加强防御技术研究之外，还包括相关的立法、标准[40]、管理、培训等策略。

网络安全专家提供了大量解决方案，以确保更好的 CAV 网络安全。中国通信学会发布的《车联网安全技术与标准发展态势前沿报告（2019）》对世界各国的车联网安全立法、标准推进、技术态势等进行了较全面的总结[34]。参考文献[35]建议各国应加强对生产自动驾驶汽车公司的监管。参考文献[36]建议采用网络安全排名措施促进安全技术进步。

自 2016 年以来，美国汽车信息共享和分析中心（Auto-ISAC）一直在维护一系列汽车网络安全最佳实践[37]，为实施汽车网络安全原则提供指导。欧盟网络安全局（ENISA）发布了智能汽车安全的优秀实践。这些实践给出了在设计安全、风险管理和技术实践方面的建议：在设计安全上，强调需要从产品开发的开始就考虑安全要素，贯穿整个供应链以及整个 CAV 生命周期；在风险管理上，针对智能汽车的新兴威胁和攻击场景，采用专门的管理方法，包括从设计过程的最初阶段就开始进行网络安全风险分析且定期修订，监控安全漏洞，在开发阶段进行例如渗透测试的安全评估，建立威胁情报流程以及及时了解新兴的攻击类型、来源以及新的相关漏洞等。

最后，如 Yan 等[41]所发现，加强人们的网络安全意识是增强 CAV 网络安全的关键问题。人们在正确评估网络安全风险的能力方面存在差异，有 23%的人正确处理了不到一半的网络安全方案；只有 4%的人可以正确处理超过 90%的网络安全方案。此外，冒险的网络安全行为通常与对自动化技术的过度信任有关[39]。当驾驶员对汽车的信任度过高时，它更容易受到攻击[8]。一个开放的研究问题是如何向公众解释这些网络安全问题以及如何对人们进行相关的网络安全的培训和科普。

5　未来技术方向

汽车产业正从过往仰赖机械元件运作，如火如荼地向智能联网目标前进。随着继续将全球供应链生产的芯片、协议、应用、代码、算法等添加和集成到智能网联汽车中，网络安全风险不断攀升。

只有在安全的前提下，智能网联汽车行业才

表 3　智能网联汽车网络安全的技术前瞻

未来方向	研究关注
功能安全和网络安全一体化	CAV 全生命周期内的功能安全、网络安全一体化设计方法、分析方法
内生安全技术	通过内生安全构造技术，使汽车获得非特异性免疫能力，应对 0-Day 等未知网络威胁
CAV 网络证书管理	证书管理系统的系统架构、模型和信任锚点等
测试技术	CAV 网络安全如何构建体系化的网络安全测试床，并能实施有效的测试
区块链技术	区块链的 CAV 网络应用及网络安全增强
轻量级认证技术	满足 CAV 高速实时应用的轻量级快速认证技术
深度学习防御	保护智能车载系统各个方面（入侵检测、软件漏洞检测、恶意软件检测）的深度学习方法
云网融合的安全	云网融合背景下的 CAV 流式数据安全处理等
软件定义的安全	使用软件定义平台实现网络威胁检测和威胁缓解的自动化
5G 智能网联汽车安全	引入 5G 技术后的 CAV 网络安全研究

能获得公众的真正认可。与其他行业的网络安全技术研究相比，智能网联汽车的网络安全研究刚刚起步，需要开启或进一步研究的方向很多，本文列举了其中一部分，见表 3。

参考文献：

[1] Autoliv innovation and research[Z]. 2019.

[2] Waymo. On the road to fully self-driving[R]. 2017.

[3] 工业和信息化部. 车联网（智能网联汽车）产业发展行动计划[R]. 2018.
Ministry of Industry and Information Technology. Action plan for the development of the connected car (smart connected car) industry[R]. 2018.

[4] MILLER C, VALASEK C. Remote exploitation of an unaltered passenger vehicle[R]. 2015.

[5] NIE S, LIU L, DU Y. Free-fall: hacking tesla from wireless to CAN bus[R]. 2017.

[6] CAI Z, WANG A, ZHANG W, et al. 0-days & mitigations: roadways to exploit and secure connected BMW cars[R]. 2019.

[7] See “Hacking smart car alarm systems”[Z]. 2019.

[8] PARKINSON S, WARD P, WILSON K, et al. Cyber threats facing autonomous and connected vehicles: future challenges[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(11): 2898-2915.

[9] Techcrunch. Why a cybersecurity solution for driverless cars may be found under the hood[Z]. 2017.

[10] Society of Automotive Engineers International. Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems[Z]. 2014.

[11] KATO S, TAKEUCHI E, ISHIGURO Y, et al. An open approach to autonomous vehicles[J]. IEEE Micro, 2015, 35(6): 60-68.

[12] LYU X, DING Y, YANG S H. Safety and security risk assessment in cyber-physical systems[J]. IET Cyber-Physical Systems: Theory & Applications, 2019, 4(3): 221-232.

[13] EL-REWINI Z, SADATSHARAN K, SELVARAJ D F, et al. Cybersecurity challenges in vehicular communications[J]. Vehicular Communications, 2019: 100214.

[14] LIBICKI M C, ABLON L, WEBB T. The defenders dilemma: charting a course toward cybersecurity[Z]. 2015.

[15] Survey: securing the modern vehicle[Z]. 2019.

[16] DE LA TORRE G, RAD P, CHOO K K R. Driverless vehicle security: challenges and future research opportunities[Z]. 2018.

[17] RABIEH K, MAHMOUD M M, GUO T N, et al. Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs[C]//Proceedings of 2015 IEEE International Conference on Communications. Piscataway: IEEE Press, 2015: 7298-7303.

[18] BHAVESH N B, MAITY S, HANSDAH R C. A protocol for authentication with multiple levels of anonymity (AMLA) in VANETs[C]//Proceedings of the 27th International Conference on Advanced Information Networking and Applications Workshops (WAINA). Piscataway: IEEE Press, 2013: 462-469.

[19] MOKHTAR B, AZAB M. Survey on security issues in vehicular ad hoc networks[J]. Alexandria Engineering Journal, 2015, 54(4): 1115-1126.

[20] WASEF A, SHEN X. EMAP: expedite message authentication protocol for vehicular Ad Hoc networks[J]. IEEE Transactions on Mobile Computing, 2013, 12(1): 78-89.

[21] DIMITRIOU T, ALRASHED E A, KARAATA M H, et al. Imposter detection for replication attacks in mobile sensor networks[J]. Computer Networks, 2016(108): 210-222.

[22] SEO S H, WON J, SULTANA S. Effective key management in dynamic wireless sensor networks[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(2): 371-383.

[23] PSIAKI M L, HUMPHREYS T E. GNSS spoofing and detection[J]. Proceedings of the IEEE, 2016, 104(6): 1258-1270.

[24] CHEMINOD M, DURANTE L, VALENZANO A. Review of security issues in industrial networks[J]. IEEE Transactions on Industrial Informatics, 2013, 9(1): 277-293.

[25] THILAK K D, AMUTHAN A. DOS attack on VANET routing and possible defending solutions-a survey[C]//Proceedings of International Conference on Information Communication and Embedded Systems (ICICES). Piscataway: IEEE Press, 2016: 1-7.

[26] YAN C, XU W Y, LIU J H. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle[Z]. 2016.

[27] SHUKLA D, VAIBHAV A, DAS S, et al. Security and attack analysis for vehicular ad hoc network: a survey[C]// Proceedings of International Conference on Computing, Communication and Automation (ICCCA). Piscataway: IEEE Press, 2016: 625-630.

[28] PATHAN K. Security of self-organizing networks: MANET, WSN, WMN, VANET[M]. Boca Raton: CRC Press, 2016.

[29] SAMARA G, AL-RABA’NAH Y. Security issues in vehicular ad hoc networks (VANET): a survey[Z]. 2017.

[30] BHARGAVA B, JOHNSON A M, MUNYENGABE G I, et al. A systematic approach for attack analysis and mitigation in V2V networks[Z]. 2016.

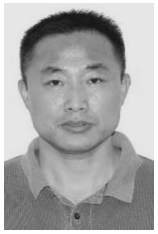
[31] LIU J, SUN W, SHI Y P. In-vehicle network attacks and countermeasures: challenges and future directions[J]. IEEE Network, 2017, 31(5): 50-58.

[32] LI K, VOICU R C, KANHERE S S, et al. Energy efficient legitimate wireless surveillance of UAV communications[J]. IEEE Transactions on Vehicular Technology, 2019, 68(3): 2283-2293.

[33] GARCIA F D, OSWALD D, KASPER T, et al. Lock it and still lose it—on the (in) security of automotive remote keyless entry systems[C]//Proceedings of 25th USENIX Security Symposium.

[S.l.:s.n.], 2016.
[34] 中国通信学会. 车联网安全技术与标准发展态势前沿报告[R]. 2019.
China Institute of Communications. Frontier report on development trends of telematics security technology and standards[R]. 2019.
[35] LIM H S M, TAEIHAGH A. Autonomous vehicles for smart and sustainable cities: an in-depth exploration of privacy and cybersecurity implications[J]. Energies, 2018, 11(5): 1062.
[36] BURZIO G, CORDELLA G F, COLAJANNI M, et al. Cybersecurity of connected autonomous vehicles: a ranking based approach[C]//Proceedings of the 2018 International Conference of Electrical and Electronic Technologies for Automotive. Piscataway: IEEE Press, 2018.
[37] Auto-ISAC. Automotive cybersecurity best practices–executive summary[Z]. 2018.
[38] YAN Z, ROBERTSON T, YAN R, et al. Finding the weakes links in the weakest link: how well do undergraduate students make cybersecurity judgment?[J]. Computers in Human Behavior, 2018(84): 375-382.
[39] NOY I Y, SHINAR D, HORREY W J. Automated driving: safety blind spots[J]. Safety Science, 2018(102): 68-78.
[40] 陈山枝, 胡金玲, 时岩, 等. LTE-V2X 车联网技术、标准与应用[J]. 电信科学, 2018, 34(4): 1-11.
CHEN S Z, HU J L, SHI Y, et al. Technologies, standards and applications of LTE-V2X for vehicular networks[J]. Telecommunications Science, 2018, 34(4): 1-11.
[41] YAN Z, ROBERTSON T, YAN R, et al. Finding the weakes links in the weakest link: how well do undergraduate students make cybersecurity judgment?[J]. Computers in Human Behavior, 2018(84): 375-382

[作者简介]

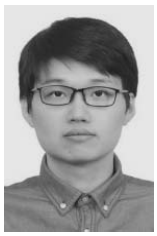


李玉峰（1975– ），男，上海大学教授、博士生导师，主要研究方向为网络信息安全管控、智能系统网络安全、宽带网络等。发表论文 50 余篇，其中 SCI/EI 检索 30 余篇；申请发明专利 39 项（授权 29 项）；公开出版专著 3 种。曾获得省部级科学技术进步奖一等奖、二等奖 4 次。

陆肖元（1975– ），男，上海大学计算机学院教授级高级工程师，上海宽带技术及应用工程技术研究中心（国家宽带网络技术及应用工程研究中心）副主任，临港智慧城市发展中心主任，科学技术部“863”计划、科学技术支撑、国家重点专项专家，上海科学技术发展重点领域“十二五”“十四五”技术预见专家。长期从事通信、宽带网络、智慧城市和大数据研究开发工作，主要研究方向为智慧城市和 5G 接入。

曹晨红（1991– ），女，博士，上海大学计算机学院讲师，主要研究方向为网络测量与安全、物联网系统与网络、智能感知技术。

李江涛（1990– ），男，博士，上海大学计算机学院讲师，主要研究方向为公钥密码学、车载网安全与隐私保护。



朱泓艺（1990– ），男，博士，上海宽带技术及应用工程研究中心（国家宽带网络技术及应用工程研究中心）助理研究员，主要研究方向为信息通信理论、无线通信、多接入边缘计算和信息安全技术。

孟楠（1982– ），女，博士，中国信息通信研究院安全研究所网络安全研究部副主任、高级工程师，主要从事电信网和互联网安全防护以及云计算、区块链等新技术安全的技术和标准研究工作。