车联网安全
关键技术解析

刘宴兵　常光辉　李　瞰　著

科学出版社

车联网安全关键技术解析

刘宴兵　常光辉　李　暾　著

科学出版社
北京

内 容 简 介

本书从汽车前沿趋势技术车联网本身的应用特点出发，结合传统的网络与信息安全内容，全面展示了车联网安全技术的内容。全书共 9 章，详细介绍了车联网安全研究的背景、安全基础、车联网的各种典型应用场景及其安全架构，车联网环境下的认证、访问控制、隐私保护以及其他安全技术，车联网安全案例分析、车联网安全产品及相关标准。另外，本书还给出了车联网中存在的其他安全问题和关键技术，力求全方位展现目前车联网安全领域的发展情况。

本书可作为车联网技术及网络空间安全领域专业技术人员、研究人员、管理人员、优化与维护人员及高等院校相关专业师生的参考书。

图书在版编目(CIP)数据

车联网安全关键技术解析/刘宴兵，常光辉，李暾著. —北京：科学出版社，2019.6

ISBN 978-7-03-058787-9

Ⅰ. ①车… Ⅱ. ①刘… ②常… ③李… Ⅲ. ①互联网络-应用-汽车-安全技术 ②智能技术-应用-汽车-安全技术 Ⅳ. ①U461.91-39

中国版本图书馆 CIP 数据核字(2018)第 208131 号

责任编辑：陈 静/ 责任校对：樊雅琼

责任印制：师艳茹 / 封面设计：迷底书装

科 学 出 版 社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京建宏印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2019 年 6 月第 一 版 开本：720×1000 1/16

2019 年 6 月第一次印刷 印张：13 1/4

字数：251 000

定价：88.00 元

(如有印装质量问题，我社负责调换)

前　言

著名咨询公司麦肯锡在《展望 2025：决定未来经济的 12 大颠覆技术》中预测了 12 项将对未来世界产生深远影响的颠覆技术，其中物联网排名第三，自动汽车位列第六，此两项技术的经济影响力总和将达到 8 万亿美元。以人工智能、大数据、云计算、移动互联网、物联网、自动汽车为基础的智能网联交通技术在近些年来越来越受到人们的关注，从而催生车联网的诞生和快速发展。从物联网定义的角度来看，车联网也是物联网技术的重要分支，但又有其特殊性。就目前车联网发展的最新状况而言，国际上对车联网这一概念的内涵和外延还没有公认统一的定义。一般地，车联网可以理解为包括车辆内部网络、车-车网络、车-路网络以及这些网络与车云平台等网联元素在内的复杂网络体系。车联网技术力图实现车-X（X：车、行人、路、互联网）之间的信息数据传播与通信交流，通过人-车-路-网之间互联互通，加之车云大数据平台的智能处理能力，形成实时可感知、及时能决策、调度最优化的智能交通，以期大幅提升道路畅通能力、降低交通安全事故数量，创造智慧交通城市。

车联网发展的前景广阔，汽车将成为互联网上一个个的移动通信节点，但由于在车联网中的车辆与网络系统深度融合，从而传统网络中所潜伏的信息安全问题必然会移植到车联网中。不仅如此，其危害程度也必然更大。设想一辆行驶中的汽车突然遭遇黑客攻击，则可能瞬间造成车毁人亡的严重后果。因此车联网的安全可靠性是制约其健康发展的关键所在。车联网安全涉及众多具体细节问题，如车联网的通信保密、车联网体系中各种元素的安全认证、安全接入、涉众的隐私保护、车辆自身的安全控制等。这些问题在移动性强、拓扑变化快的车联网环境中面临着诸多挑战。

本书在结合实际项目，参阅大量文献资料的基础上，形成了目前的内容体系，意在介绍车联网发展的新趋势及车联网安全的主要关键技术。全书共 9 章，第 1 章以简明、易于理解的方式向读者介绍车联网体系结构和关键技术，同时，也分析了车联网发展及其制约问题。第 2 章从安全基础理论出发，概述车联网技术所涉及的密码学知识及关键技术理论知识，为本书后面的部分具体技术与应用做铺垫。第 3 章介绍车联网的几种典型应用场景以及安全需求，阐述了一种车联网安全体系。第 4～6 章结合实际工程项目，分章节具体介绍车联网安全中的认证、访问控制、隐

私保护三大关键技术。第 7 章介绍车联网安全系统中所用到的其他安全技术。第 8 章介绍车载终端嵌入式系统安全案例分析。第 9 章向读者简单介绍目前车联网安全产品及相关标准协议。

本书的部分内容来源于国家科技重大专项(No.2011ZX03002-004-02)、国家自然科学基金项目(No. 61772098&61772099)和重庆市重点产业共性关键技术创新专项(No. CSTC2015ZDCY-ZTZX40001)。李银国教授、蒋建春教授及其团队为本书编写提供了指导和帮助；王宇航、李培真、李露、叶青、赵璐、赵雷镇、罗杰等硕士研究生参加了本书的编排工作，并以不同方式给予了帮助，谨在此向他们表示衷心的感谢。我们还要感谢所有直接或间接为本书做出贡献的同事、同仁和参考文献的作者。

在编写本书的过程中，我们考虑了不同层次读者的需要，每一部分力求从基本原理入手，由浅入深、循序渐进，直至分析关键问题、剖析具体算法，读者可以根据具体需要进行有选择性的阅读。

由于车联网及其安全相关技术和标准化工作还在研究和发展过程中，多种解决方案还处于研究和讨论阶段，有些相关的研究成果来源于外文期刊，加之作者水平有限，书中难免有疏漏和不妥之处，敬请读者批评指正。

作　者

2018 年 7 月

目　录

第1章 绪 论

1.1 车联网的简介

1.1.1 车联网的概念

物联网技术的发展给人们生活提供很大的便利，同时为人们的生活和工作带来高质量、高水平的服务。现今，物联网技术越来越受到人们的关注，学术界、工业界、政府等都投身其中，大大加快了其发展的速度。车联网(internet of vehicles，IoV)是物联网技术的重要分支，从当前车联网发展的最新状况来看，其内涵和外延还没有公认统一的定义。车联网可以理解为包括自身网络、车-车联网和移动互联网(Internet)在内的复杂网络体系，它以每辆车作为基本元素，通过传感器技术采集原始数据，包括车内产生数据、车际产生数据以及车载终端产生数据，再利用无线通信技术、信息数据挖掘技术、网络技术、智能控制技术、云计算与流计算技术等对原始数据进行状态评估以及做出相应决策。车联网实现车-X(X：车、行人、路、互联网)之间的信息数据传播与通信交流，通过人-车-路-网之间实时互联感知实现车辆智能化控制、智慧城市与交通、信息服务智能决策的一体化，提高出行效率，为人们提供优质服务。可以说，在车联网中，汽车就是一个移动通信节点或终端。

常规地讲，车联网的组成实体包括车辆节点、路侧单元(road-side unit，RSU)、可信中心(trust center，TC)。网络体系结构如图1.1所示。

1)车辆节点

车辆节点作为车联网通信环境中唯一具有移动属性的通信实体，通过部署各类智能传感器装置、车载计算装置及无线通信装置，实现信息感知采集、信息计算处理和通信功能。在交通路网中，车辆节点既是消息的产生者又是转发通信报文的路由器，车辆间通过多跳的通信方式把数据转发给远距离的车辆节点。

2)路侧设备

路侧设备作为车联网中的固定通信节点，相比于车辆节点具有更强的计算处理能力和无线通信范围，通常为车与车(vehicle to vehicle，V-V)、车与基础设施

(vehicle to infrastructure，V-I)以及车与可信中心(vehicle to trust center，V-TC)提供通信连接方式，并为车辆节点接入网络提供相关的接入服务，部分时候也作为互联网网关接入网络。

3)可信中心

可信中心是车联网通信体系中的一类基础服务设施，它主要为接入网络中的通信节点颁发证书、存储密钥、完成身份认证等。此外，可信中心是整个网络结构中唯一让所有节点无条件信任的设施，进而实现对网络中所有节点的管理与监督。

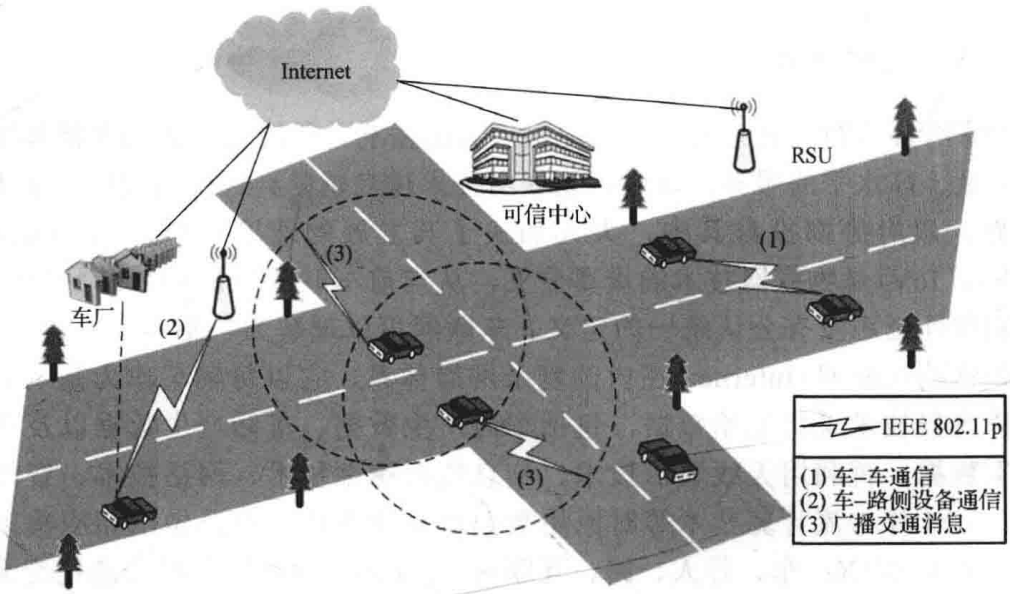

图 1.1　车联网体系结构图

1.1.2　车联网的特点

车联网由于其构建对象的特殊性，除了具备移动自组织网络(mobile Ad-Hoc network，MANET)的自组织、多跳传输和拓扑结构经常变化等特点，以及继承了物联网的基本特征外，还存在以下 3 个独有的特点。

(1)路网中车辆节点的驾驶速度一般为 18～152km/h，导致网络拓扑结构变化快、通信链路“寿命短”。根据相关学者的研究表明：在 100km/h 的时速下，平均每条消息的传输时间为 1～10s。若节点无线覆盖范围为 250m，则通信链路能稳定保持 15s 以上的概率只有 57%。

(2)车辆节点间的无线信道通信质量受道路交通规划、道路状况、路边建筑布局、车速等多种因素影响，使得交互消息只能沿道路方向传播给其他节点，难以预知车辆的运动规律，从而导致车载自组织网络(vehicular Ad-Hoc network，

VANET)主要沿着道路方向呈现管状形态，降低 VANET 容量和空间利用率。当洪泛广播应用于网络时，将容易导致网络拥塞。高大的建筑物将阻挡无线信号传输，当数据包竞争无线信道时，将造成信号衰落。

(3)由于移动节点兼有主机和路由的功能，且行为具有独立自主的特性，所以 VANET 更容易遭受入侵和拒绝服务等网络攻击，增加了安全保障的难度。

通过总结分析可以发现：①相对于物联网，在车联网环境中，每个感知元素即车辆，对计算能力和存储空间提出了更大要求，这也是车联网中的难题之一。因此，对车联网而言，采取的方式是在终端对感知层采集到的信息作相关处理。②相对于移动自组织网络，车联网的每个感知对象都在高速移动，从而导致车辆节点接入方式频繁切换，网络拓扑快速变化，车联网要求更强的可靠性以及通信实时性。③相对于其他智能联网终端，车联网的每个感知对象引入了更多的接入方式、通信接口，以及更多样的应用场景，如协同驾驶、主动安全、网络应用、交通管理监控等。

1.1.3 车联网的前景

截止到 2015 年年末，全球可数的互联网实体超过 66 亿。随着车联网的快速发展，联网的车辆已经达到 6200 万辆，成了仅次于计算机和手机的第三大网络实体。如今，车联网作为政府、企业以及学术界的关注焦点，其产业链庞大，涉及领域多，商业前景巨大。车联网的发展为人们的出行、生活带来极大的方便。例如，对于现在研究较热的无人驾驶进行 V-X 信息交互，未来道路上可能就没有红绿灯，而只有错综复杂的道路和井然有序的车辆。

继车辆实现联网之后，车联网具有丰富的应用场景和产业：一是数据流量的应用效率将会得到极大的提升，从个人领域到汽车应用；二是融合了包括导航、影音、就餐、购物、娱乐、保险、安全等多样化的应用场景；三是推动相关应用软件、硬件的服务与销售。

在便捷类应用场景中，网联车为人们的生活带来更多的便捷：随着车载平台的智能化发展，车主通过语音、手势操作控制，内置的移动热点转换技术，实现信息交互类服务，实现切换路线、选择路线、自动导航，实现和商家互联，购物、预订餐厅，实现家居互联以及公司互联等，为生活带来更多便捷。

在效率类应用场景中，全面实现智能化交通：随着车载平台的智能化发展，首先是车辆系统的自动更新，人们无须前往 4S 店，也可以实现车辆硬件和软件的自动更新；然后，车主可以通过无线设备远程获取车辆信息或控制车辆，如获取车辆停放的位置信息或将车主信息定位发送给车辆，控制车辆识别并完成接送车主等。

在实用类应用场景，加强用车、行车安全：未来车联网环境下的汽车，车

辆每时每刻产生的数据都将会被记录并保存，为分析行车安全提供良好的原始数据。在大数据的环境下，可以建立较为精确的模型，对安全等其他问题进行预测，进一步提高汽车的安全防护功能，如汽车周边物体安全距离通知、被盗车辆跟踪、道路救援等。

车联网通过车-X之间的通信和信息交换，可以实现智能动态信息服务、车辆智能化控制，甚至是整个城市智能化交通管理的应用。可见，车联网在未来的发展有很大的前景。

1.2　车联网的发展

1.2.1　车联网的发展时间轴

从一面世，IoV研究便备受国内外重视。1999年，美国交通运输部特别针对欧美地区的车辆通信网络和智能交通系统(intelligent transport system，ITS)电子元器件间的数据传输设计并制定了专用短程通信(dedicated short range communications，DSRC)技术协议体系标准。其中，将IEEE 802.11p协议部署在车载电子无线通信设备的底层并作为基础的通信标准，IEEE 1609系列协议簇为高层ITS提供交互标准，独立划分5.9GHz频段，作为底层高速率数据传输的固定频段。随后，谷歌(Google)公司开始尝试开发车载人工智能软件，用来辅助驾驶员控制车辆。2010年，包括代号“GoogleFleeetl”在内的7辆试验车，在人工监督下行驶了1.4×10^4km，并完全自主行驶了1000km。2015年，美国西部的内华达州首次批准了德国戴姆勒(Daimler)股份公司的一款自动驾驶卡车用于商业用途；此外，沃尔沃等欧洲的7家公司共同联合启动实施了“SARTRE”项目，并在西班牙高速路上成功让3辆无人驾驶轿车和1辆无人驾驶卡车行驶了124英里(1英里=1.609344km)。

国内，2009年，在深圳举行的全国第四届GPS运营商大会上，IoV的概念被首度提出。2010年，在无锡举行的第一届中国国际物联网博览会开幕式上，诞生了中国的“车联网”概念，旨在实现真正的“物以网聚、感知中国”。2011年，国防科技大学自主研发的HQ3无人车，成功地在长沙到武汉的高速公路上完成了共计286km的无人驾驶实验；此外，为了推动车联网产业的发展，我国科学技术部(简称科技部)国家高技术发展计划(863计划)分别在2011年和2012年先后启动“智能车路协同关键技术研究”和“车联网技术研究”。2014年至今，腾讯、阿里巴巴、百度陆续加入车联网研究的大潮，并研发出相关解决方案；目前，中国联合网络通信集团有限公司(简称联通)已同中国第一汽车集团有限公司(简称一汽)、东风汽车集团有限公司(简称东风)、上海汽车集团股份有限公司(简称上

汽)、宝马公司等汽车公司并肩推广智能车联网系统并开展合作。2016 年，百度与奥迪中国、通用汽车公司、一汽大众三大汽车品牌达成合作，加速车联网产品在车型上的落地，为更多车主用户提供智能化的人车互联服务。2018 年 1 月，重庆首款无人驾驶共享汽车——力帆 330EV 在美国硅谷推出，驾驶者只需在 iPad 上输入目的地，汽车便能完全自主驾驶到达目的地，预计短期内实现条件干预全自动驾驶。图 1.2 简化展示了车联网的国内外研究现状。

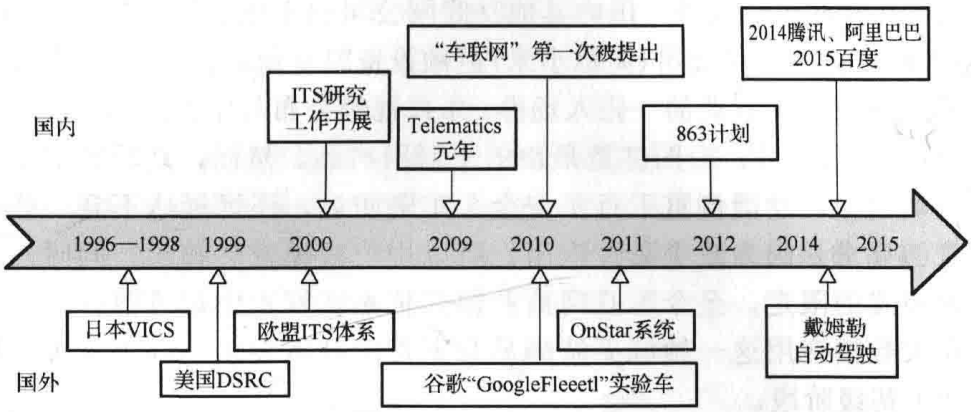

图 1.2 车联网国内外研究现状示意图

1.2.2 车联网行业现状

就目前来看，还没有完成整体车联网行业体系构建。从目前的市场格局来看，其中蕴含的大蛋糕吸引了大量企业争先加入，主要的竞争者包括各大互联网巨头、各大车企、一些初创公司以及部分成熟的车联网公司，竞争者之间构成横向、纵向竞争，相互影响，互相促进，一起推动着车联网发展。

互联网巨头和整车企业在车联网产业链中拥有核心地位。由于汽车制造壁垒很高，汽车生产资质由整车企业掌握着，因此，整车企业在控制集成的核心竞争上没有其他企业能够撼动，处于车联网非常核心的地位，这里主要指车联网的运营平台。另外，整车企业还控制着车联网的数据核心基础——控制器局域网络(controller area network，CAN)总线，在前装市场上掌握着很大的主动权(包括培养用户习惯、积累用户数量)。例如，福特汽车公司旗下的 SYNC、别克汽车公司旗下的 Intellilink、宝马汽车公司旗下的 iDrive、凯迪拉克汽车公司旗下的 CUE、丰田汽车公司旗下的 G-Book、雪佛兰汽车公司旗下的 MyLink 等，结合全球定位系统(global positioning system，GPS)进行路径规划，通过协同式的辅助驾驶技术实现智能信息交互，也更加侧重信息与机车本身的交互，力图能有反馈式的控制系统能力。互联网技术革命性的发展对传统的制造产业产生了很大影响，先于传

统汽车制造商，互联网企业反而成为进军车联网行业的先锋队。在工业 4.0 时代，各大互联网公司争先进入这一领域，都希望在新行业发展中分得一杯羹，从国外的苹果(Apple)公司、谷歌公司，到国内的华为、腾讯、阿里巴巴以及百度，依托自身原有优势，都在车联网中大显身手，通过与传统车企合作，以车载智能产品、无人驾驶、互联网汽车生态系统等为主要内容，积极布局汽车智能化、自动驾驶、智能网联汽车生态系统，大力推进汽车智能化的进程。

除上述互联网各巨头外，国内其他互联网公司也希望能够栖身车联网竞争者之列。小米科技有限责任公司(简称小米)巨额投资凯立德股份有限公司(简称凯立德)，赢得车联网相关行业的一张入场券。乐视视频公布与宇龙通信科技有限公司在通信 5G 上进行合作，力图打造最快的车联网产品。然而，现阶段的车联网还在研发周期当中，功能侧重于行车安全、车辆防盗，还远远达不到一些更高级应用场景的要求。因为缺少黏性应用，所以用户规模依然较小。同时，由于互联网盈利模式的限定，至今车联网商业模式依然在探索中艰难前行。这也导致车联网在大数据应用这一领域无法满足数据量的基本要求。综上，车联网整体发展还处于初级阶段。

1.2.3　车联网的发展趋势

全球著名管理咨询公司麦肯锡发布的《2015 年汽车互联和自动驾驶技术咨询报告》，针对亚洲、欧洲、北美三个地区的普通用户和车企高管进行调研，调研结果显示，车企和相关行业需要在“端到端的整体数字化和努力提高客户认可度”两个关键领域采取行动，并且报告指出，能够适应新竞争的汽车厂商将迎来巨大商机。

在第二届中国电动汽车百人会论坛上，权威声音表示支持 IoV 是 5G 的重要涉及目标；促进 IoV 的发展，拥有 IoV 技术架构的主机厂必然会把车联网解决方案用到更多的汽车上面，传统汽车业也会被带动起来，以便摊薄研发成本。

IoV 以车辆为移动的信息感知对象，在消除信息孤岛的同时，为交通行业提供更安全、节能、环保、智能、高效的出行方式和多样化的智能服务模式。但是，IoV 的实现必须依赖于各种先进的智能传感技术、无线通信技术、控制技术、互联网技术和系统集成技术等，而 IoV 具有通信网络拓扑结构频繁变化、车辆节点之间高动态自主协同、通信场景多样化以及通信环境开放性等特点，从而使得路网中的车辆节点比传统的网络节点面临更多、更复杂的网络攻击，给车联网系统的安全防护和主动防御带来了新的挑战，而且，当前的 IoV 未能形成完整的安全体系。目前，国家对建设安全体系基础设施的需求已经提出了指导方针，在《国民经济和社会发展第十三个五年规划纲要》中指出：“强化信息安全保障……着力

构建量子通信和泛在安全的物联网……加快构建高速、移动、安全、泛在的新一代信息基础设施，推进信息网络技术的广泛应用”。在《中国制造2025计划》指南中指出“以加快建立具有全球竞争优势、安全可控的信息产业生态体系为主线，强化科技创新能力、产业基础能力和安全保障能力，突破关键瓶颈……”作为信息产业发展的指南。2016年，国家已将“LTE-V无线传输技术标准化及样机研发验证”列入新一代宽带无线移动通信网国家科技重大专项中，在助推LTE-V标准形成的同时，也极大地加速了车联网产业化的发展进程。

1.2.4 车联网标准及组织

日本、美国、欧洲是车联网标准化工作及车联网主要工作的集中地区，他们之间的技术既有一定的互通性，又独立发展。政府部门一般负责制定具有法律效应的具体的规章制度，行业组织则一般负责在没有逾越规章制度的前提下制定行业标准，研究机构则通过项目来测试各种架构和技术。

1. 日本情况

日本是车联网发展的先行者，日本的日产、本田、丰田三大汽车巨头在前期推动车联网发展起到了很重要的作用。今天，随着汽车大数据的自动化采集技术日益成熟和高速移动通信技术飞速发展，日本信息技术(information technology，IT)巨头(如日本电气股份有限公司(简称NEC)、NTT Docomo、日立等)纷纷进军车联网领域。在1996年初，比较成熟的车联网信息系统——交通信息通信系统(vehicle information and communication system，VICS)已经基本覆盖了整个日本，VICS可以及时向车载导航器发送交通限制、道路拥挤等道路交通信息。到2013年年底，该系统在日本的安装车辆已经超过3000万辆，在同期日本车辆的占有率为40%。

随着互联网的飞速发展，车载终端应用得到了进一步的完善。本田不仅率先把车载导航引入汽车，而且还将大数据云服务引入其中。本田在极大地推动车联网技术发展的同时，也在车联网领域占领了市场。在2013年，本田又一次在其高端车系列讴歌(Acura)上推出基于云端的车联网服务“Acura Link”，可以实现实时路况、人工搜索、保养通知、远程诊断、远程控制、车辆防盗和紧急救援等功能。本田讴歌借助车联网，采用一套完整的云端大数据分析系统在后台为每一个客户提供技术支撑，时刻准备为用户提供细致周到的服务以提升驾驶体验。

日本车联网发展迅速，其规划由日本政府直接参与，向车联网路侧设备、车-X以及无人驾驶等技术体系综合推进。