中国汽车工程学会
汽车工程图书出版专家委员会推荐出版

WILEY

车用安全通信——协议、安全及隐私

[意]卢卡·戴尔格罗斯（Luca Delgrossi）
[美]张涛（Tao Zhang） 著
鲁光泉 田大新 王云鹏 译

VEHICLE SAFETY COMMUNICATIONS: PROTOCOLS, SECURITY AND PRIVACY

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

车用安全通信

——协议、安全及隐私

[意] 卢卡·戴尔格罗斯（Luca Delgrossi）
[美] 张涛（Tao Zhang） 著

鲁光泉　田大新　王云鹏 译

北京理工大学出版社
BEIJING INSTITUTE OF TECHNOLOGY PRESS

图书在版编目（CIP）数据

车用安全通信：协议、安全及隐私 /（意）戴尔格罗斯（Delgrossi，L.），（美）张涛著；鲁光泉，田大新，王云鹏译. —北京：北京理工大学出版社，2015.4

书名原文：Vehicle safety communications：protocols，security and privacy

ISBN 978-7-5682-0092-9

Ⅰ.①车… Ⅱ.①戴… ②张… ③鲁… ④田… ⑤王… Ⅲ.①汽车-通信设备 Ⅳ.①U463.67

中国版本图书馆 CIP 数据核字（2015）第 014757 号

北京市版权局著作权合同登记号　图字：01-2014-1559 号

出版发行 / 北京理工大学出版社有限责任公司
社　　址 / 北京市海淀区中关村南大街 5 号
邮　　编 / 100081
电　　话 /（010）68914775（总编室）
　　82562903（教材售后服务热线）
　　68948351（其他图书服务热线）
网　　址 / http：//www.bitpress.com.cn
经　　销 / 全国各地新华书店
印　　刷 / 保定市中画美凯印刷有限公司
开　　本 / 710 毫米×1000 毫米　1/16
印　　张 / 24.75　　责任编辑 / 封　雪
字　　数 / 396 千字　　文案编辑 / 封　雪
版　　次 / 2015 年 4 月第 1 版　2015 年 4 月第 1 次印刷　　责任校对 / 孟祥敬
定　　价 / 98.00 元　　责任印制 / 王美丽

译者序言

交通拥堵、交通污染和交通安全是交通领域亟待解决的三大难题。不断提升交通系统的智能化水平，是提高交通安全水平、缓解交通拥堵和交通污染的有效途径。随着通信技术的快速发展，作为新一代智能交通系统技术的车路协同受到越来越多的关注。协同式的智能交通系统成为智能交通系统的新阶段，美国、日本和欧盟先后部署了相关的国家计划开始关键技术研发。2012 年，美国运输部、美国国家公路交通安全管理局会同密歇根大学在密歇根州进行了车车/车路通信及其预警技术的应用试验，有3000 辆车参与。随后，美国运输部在 2014 年 2 月 3 日发表对外声明，决定推动车车通信技术在轻型车上的应用。这标志着车路协同技术即将从实验室走向应用市场，将成为继安全带、ABS 之后汽车的第三个基础安全装备，将为交通安全带来新的技术变革。

毋庸置疑，车用通信是未来车路协同技术的基础。在为车与车、车与路提供有效、可靠的无线通信的同时，车用通信的安全与隐私问题也越来越受到人们的关注。作为一项可能会影响大部分人出行安全的新技术，安全与隐私是车用通信技术在大规模推广应用之前必须解决的问题。我国也越来越关注车路协同技术的发展，并对其进行了系统研究，但总的来说，通信的安全与隐私问题还没有引起足够的重视，相关的研究工作开展得还不够深入。Luca Delgrossi 和 Tao Zhang 的这本著作，对车用通信的安全与隐私问题，提出了一系列解决方案。本书的翻译出版，对我国车路协同技

术的发展具有非常积极的意义，能够为我国进行车用通信方案的设计和部署提供非常有价值的参考。

本书的翻译工作由鲁光泉、田大新和王云鹏负责，前言、第1～5章由王云鹏负责翻译，第6～9章和第14～17章由田大新负责翻译，第10～13章和第18～22章由鲁光泉负责翻译。参与翻译的人员还包括杨家骐、鲍泽文、张然、陈海冲、李鲁苗、罗毅、李良、宋阳、张鑫、杨越、单雄宇、鲁彬彬。另外，衷心感谢北京理工大学出版社的大力协助。作为一本学术专著，本书涵盖了通信技术、车辆工程、交通运输等学科的知识，专业程度较高，在翻译过程中，我们尽可能保留原著的写作风格，但由于自身水平有限，本书在翻译过程中难免存在不足之处，也希望能够得到各位读者的悉心指正。

译　者

2014年8月于北京航空航天大学

前言（一）

经过数十年的发展，车辆已具备多种辅助驾驶功能。现代汽车已经具有主动制动避撞、安全车距保持、车道保持、避让行人等功能，这些功能是通过安装在车辆上的传感器实现的。车辆可以通过传感器监测其行驶安全性并感知周围的行车环境。当车辆实现了用自己的“眼睛”检测周围的行车环境，并将这些信息传递给周围车辆的功能的时候，上述功能会变得更加完善。这就进入了车车通信技术的发展时代。

在当今世界几乎所有事物都趋于联网的大环境下，人们自然会想到开发具有信息交流功能的汽车。然而，目前高档汽车上最先出现的车车通信应用都需要人的参与：车辆能够为乘员提供浏览网页和查看邮件服务，或者允许远程访问车辆状态，例如重新调整车辆充电过程。在车辆之间、机器之间实现直接通信是一个全新的领域，本书将对该领域中的一些规则进行阐述。

Luca Delgrossi 和 Tao Zhang 不仅是定义车车通信的先驱，同时也是车车通信方面研究的开拓者。从最早参与美国运输部（U. S. Department of Transpor-tation，US DOT）按照美国电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）的标准进行的早期研究项目到现在发展情况测试，他们参与了许多著名的项目，并创立了汽车领域里的通用语言。在此，谨对他们能够通过本书分享其学术成就表示祝贺。作为工程师，由于在开发车车通信功能时需要借助此语言进行研究，本书将成

为我们的重要参考书籍。

开展车车通信研究前景何在？可以肯定的是，我们能够提高车辆和道路交通的安全水平。汽车可以将检测到的危险情况发送给后面的车辆，通过提前预警的方式减缓驾驶员面对紧急情况时的惊慌情绪。这些预警包括前方道路转角处发生交通事故、前方出口匝道有“黑冰”路况、在右侧车道上有故障车辆等。最后，驾驶辅助系统可以通过将采集到的信息进行整合分析以及与其他传感器的联合使用，实现更高级的自动控制，比如采取紧急制动和车道保持等功能。此外，从车辆上收集的大部分信息都可以用来提高车辆的机动性，甚至能够通过更加统一的车车通信平台来提高通行效率。最终，车辆可以通过接收到的信息进行协调控制，使车车通信成为自动驾驶新兴领域中的一个元素。

我们尚未完全进入车车通信的时代，在未来的几年内也不能实现。任何网络技术的价值都是随着通信实体数目的增多而提高的。要想在道路上使通信车辆达到合适的数量并不是一项简单的工作，在研究开展的过程中还存在其他的问题，比如使用者会担心系统的安全问题而阻碍研究的推广。本书在介绍车车通信内容的同时也会对相关问题加以适当的阐述。

Ralf G. Herrtwich
驾驶辅助系统和底盘系统
群组研究和先进工程
戴姆勒公司

前言（二）

我为能够在这本适时且重要的书上发表一些自己的想法感到非常荣幸。

本书是由该领域内的两位先驱编写的。他们是车车通信和车路协同技术方面技术、规范、开创性研究和相关应用方面研究的积极参与者。本书将很快成为该领域内的一本参考书，它在技术层面上提供了清晰的、有组织的、全面性的指导，站在该领域研究的最前沿，而且具有历史性、推动性和应用性。

本书对我们的产业发展非常重要，它让我们看到了交通运输领域发生巨大转变的希望。

本书是车车通信研究成就的一个重要见证，作者是学术界和工业界充满激情、富有远见的领导者——Luca Delgrossi 和 Tao Zhang。他们在该领域研究多年，使得这些技术逐渐发展成熟，并最终达到了可以普遍应用的程度。

事实上我们相信，他们的努力最终不仅仅在传统的道路交通领域内有重大意义，更会在相近领域有恰当的体现。

本书所介绍的技术和应用必将在智能交通、智能城市、自动化产业和因移动信息广泛连接而著称的“物联网”方面起到非常重要的作用。

感谢 Luca Delgrossi 和 Tao Zhang 这么多年来的梦想坚持、研究努力和科研成果。感谢这本书，给许多人介绍了该领域技术的价值体系，这些人也会帮你们实现梦想！

Flavio Bonomi
思科公司，副总裁
高级架构和研究部主管
思科系统公司

前言（三）

汽车在当今全球社会中所扮演角色的重要性一如既往。Luca Delgrossi和Tao Zhang编写了一本意义重大的书，该书提出了在车辆设计、公共监管机构和消费者方面一个最重要的问题，即安全和现代通信能够给什么带来显著改善并使其得以实现的问题。这是一个复杂的课题，我不得不称赞作者在研究中所采用的清晰和结构化的方法。首先，他们从许多观点中总结了有关机动车辆“安全”的事实现状。其次，他们抓住了先进技术的要旨，明白对于减少事故数量和降低事故损失的研究是永无止境的课题，该课题需要借助一些在特定时刻可以使用的应用技术。这也为我们带来了一些新的技术方法，其核心是对无线通信技术和数码电子产品的开发。再次，他们提出了多学科方法的重要性，这也是该书如此重要的原因之一，它融合了来自不同技术领域的基础和细微的知识，将汽车工程、安全、无线通信工程和网络安全都组织到一个架构内，这就给尽快减少机动车辆事故数量、降低事故带来的人员伤害和财产损失带来了希望。

我们正处于数字化革命迫使车辆设计者和制造商重新考虑和修改汽车的功能和控制系统的时代，同时也是高速公路基础设施发生巨大变化的时代。这些变化的产生在很大程度上是因为功能强大的移动设备得到广泛使用，这些设备具备不断增长的计算能力、访问储存和实时信息的能力、移动通信能力等以及功能更加强大的接口。研究人员希望一些已经进入人们日常生活中的功能能够在车辆上得到实现，包括娱乐、便利性、车辆管理

和行车安全。我们在数字传感器和执行器、人工智能和各种子系统方面进行了大量投资，并把它们应用到汽车和高速公路上，这些投资要依靠大规模普及才能获利。以汽车安全问题为例，需要考虑以下两个方面：首先，从被动系统到主动系统，最后到自动化系统，该自动化系统可以在很少或者没有驾驶干预的情况下实现自动化安全指引。其次，从独立的车辆到与其他车辆或周围基础设施之间互相通信的系统，最终实现信息交互的深度优化系统，该优化系统协调共享信息、协同决策以提高行车安全性和机动性，并减少对环境的影响。这就是网络和云计算的时代。

要想实现以上描述还有着很复杂的技术性问题，本书可以为解决这一问题奠定基础。本书内容包括了车内信息传送和处理的体系结构，以及车辆对外部信息的接收和处理。值得注意的是，本书的主题通过几个层面进行讨论，清晰地阐述了影响车辆安全的因素。这些主题包括：车辆交互的总体方案，以及利用信息连通性实现各种功能的方式。其中，一个重要的内容就是信息交互技术的解释性说明和如何满足设计要求，包括延迟、延迟抖动、可扩展性要求。本书对于计算和仿真的过程都进行了详细描述，使得读者能够理解其中各细节。本书极其重要的研究内容之一是对安全和隐私的深入探索，以及建立加密和密钥/证书管理的基本机制。我们很难想象，如果没有本书的正确思想引导，该如何建立智能汽车的基本控制系统。同时，要明白我们所面临的问题是什么，以及找到难以满足通信要求的核心原因。最后，虽然我们可以理想化一些概念，并构建一个理想化的安全系统，再对其进行仿真研究，但是这仍然不如根据实验和典型实际场景进行研究。作者阐述了该领域已经取得的一些研究成果。本书对于从事车车交互系统的研究人员以及想要了解这方面潜在技术的人员来说，都是一本非常不错的参考书。

在本前言的最后，谨表达对于 Luca Delgrossi 和 Tao Zhang 编写本书的感谢。我知道他们每天处于充满压力的生活环境里，很难抽出大量时间来编写本书。无论如何，他们成功地向我们提供了一本非常优秀的书，并且为他人奠定了相关研究的知识基础。我们可以看到他们在日常工作之外的付出，同时我们对他们的努力和成就表示称赞。

Adam Drobot
董事长
Open Tech Works 公司
达拉斯，得克萨斯

前言（四）

每天由道路交通事故所造成的人员伤亡和财产损失都是巨大的。虽然近几年来出现了许多改善行车安全性的措施，但是随着车辆数目和车辆平均行驶里程的增加，解决行车安全问题变得越发困难。因此，开发可以显著减少碰撞事故次数、降低事故损失的安全系统就变得尤为重要。无线通信技术或许能够成为新的自动安全系统的基础。

在过去的十几年里，工程师已经在应用于车辆安全的无线通信技术方面取得了突破性进展。使用专用短程通信（DSRC）可以获取高质量的数据（数据由车载传感器获取），这在很大程度上完善了现有系统。在车辆之间共享这些高质量数据，可以使得车辆“看见”周围的行车环境和潜在的危险。2012 年，在早期样机开发和相关实验进行的基础上，一种基于无线通信的安全系统在世人面前展示了其功能。

本书重点关注车辆安全通信，阐述了建立适用于日常行驶车辆的完整无线通信系统的基本原理、设计准则和通信协议。同时，还描述了一些风险和挑战，诸如如何建立车辆间的信任机制、数据的安全交换机制以及车车通信网络的隐私保护机制等。

车辆安全通信系统的设计过程中存在有许多问题，比如传统车辆需要在短时间内完成加速过程，这就要求通信延迟尽量低并且搭建通信通道的速度要快。与现有网络不同，在车辆间交换关键安全数据是通过对短消息进行周期性广播来实现的。提高数据传输可靠性的传统机制（例如数据包

确认和重新传输）不再有效，因为车辆是时刻运动的，延迟的数据包很可能包含过时信息。数据的传输可以在不同环境中实现，从城市峡谷到山地地区和农村地区，不同环境对于信号传播和网络性能都有不同影响和要求。此外，通信系统还必须能够迅速适应车辆的高速运动状态和交通密度等情况。

类似地，对于车车通信网络还有专门的安全性和隐私方面的要求。车辆要在很短时间内交换数据信息，因此它们必须对这些信息建立充分的信任。保护驾驶员的隐私会与其他一些功能产生冲突，这些功能包括通信安全、车辆安全应用程序、错误或恶意实体检测等。全国范围的车车通信网络需要高度的系统可扩展性，这对安全和隐私管理提出更高层次的复杂要求。在这样的要求背景下，许多针对小型网络的解决办法都无法扩展、失效或者变得效率低下。

同时，车车通信网络的搭建也受到车辆需求带来的额外约束。车载安全设备必须进行机动车等级标准认证，解决车载硬件或者软件的问题或者对其进行改装会在给消费者和制造商带来不便的同时产生巨大的成本。最后，由于现代车辆的使用寿命普遍较长，若要使得不同年代的车载通信和安全系统协调工作，这就给车辆发展带来了兼容性方面的挑战。

在过去的十几年里，工业界、学术界和政府部门之间开展合作，大力推动了车辆安全通信的发展。本书介绍了这些努力所催生的主要成果，并为以后的研究奠定了坚实的基础。为了吸引更多读者，我们将尽量平衡技术细节与文本可读性之间的矛盾。

本书大纲

第1章至第3章主要介绍主动安全的概念，包括撰写本书的动机、内容和车辆安全应用的种类。第1章给出美国、欧洲、日本和其他一些国家的道路交通事故数据，说明交通事故在人员伤亡和财产损失方面造成的巨大代价，也同时说明了车辆安全问题的实际现状。第2章阐述主动安全系统的发展过程，包括对于被动安全技术（如安全带和安全气囊）、主动安全技术和最新的驾驶辅助系统的介绍。第3章介绍支持车载安全系统的车载单元，包括电子控制单元、传感器和车载通信网络等，同时还讨论车辆数据采集、定位与安全方面的问题。

第4章至第9章重点介绍面向车辆安全的无线通信技术，即车车通信。第4章讨论车车通信的模式和应用需求，强调车车通信网络的重要性。此外，还对现有的各项技术进行评估，以得出其是否适用于车辆安全通信的结论。第5章介绍5.9 GHz DSRC的频率分配和车间无线通信（Wireless Access in Vehicular Environment，WAVE）的接入标准协议栈。第6章和第7章分别描述按照美国电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）802.11p标准的物理和介质访问控制层行为。第8章介绍有关确定DSRC最佳数据传输速率的研究。第9章介绍WAVE的上层协议，包括WAVE简讯通信协议（WAVE Short Message Protocol，WSMP）和关于DSRC多通道操作的IEEE 1609.4标准。

第10章至第12章阐述在几个方面具有代表性的安全应用，这些应用

是近期合作研究的部分研究成果。第 10 章主要介绍车路（Vehicle to Infrastructure，V2I）协同技术应用。第 11 章主要介绍车车（Vehicle to Vehicle，V2V）交互通信技术应用。第 12 章介绍 DSRC 的扩展性和消费者车联网拥塞控制算法方面的进展。

第 13 章至第 21 章介绍有关车车通信网络安全和隐私保护方面的问题。第 13 章阐述在大规模车车通信网络中特有的安全隐患与隐私要求。第 14 章描述基本加密机制，该机制对于支持车联网中的安全和隐私至关重要。第 15 章着重讲解如何将公钥基础设施（Public Key Infrastructure，PKI）扩展到管理安全凭据的应用方面（例如将数字证书用于大规模车车通信网络），并讨论在使用数字证书和 PKI 隐私保护时需要解决的问题。第 16 章至第 18 章介绍并分析三种隐私保护数字证书管理方法：共享证书、短期证书和群体证书。第 19 章提出的方法扩展了第 16 章至第 18 章中所给出的各解决方案，该方法可以排除违反运营商安全证书管理系统的潜在风险，从而能够保护驾驶员的隐私。第 20 章对前面提到的三种隐私保护数字证书管理方法进行简单的对比。第 21 章介绍支持 DSRC 网络安全的 IEEE 1609.2 标准。

本书在最后一章，即第 22 章，讨论第四代蜂窝网络在支持相应车辆安全通信技术方面的应用。

Luca Delgrossi
Tao Zhang

致　谢

感谢所有参与本书所提及研究的学者、研究人员、各界朋友，在此我们无法将各位名讳一一列举。在防碰撞联盟（Crash Avoidance Metrics Partnership，CAMP）项目中，我们组建了一个富有协作成效的理想环境。研究荣誉应当颁给 CAMP 项目的负责人 Mike Shulman。作为一系列国际项目的领导者，Farid Ahned－Zaid、Hariharan Krishnan、Michael Maile 和 Tom Schaffnit 带领我们不断改进原型样机系统。我们通过与 CAMP 项目工程师的交流拓展了思路并获取了丰富的知识。在车路协同联盟（Vehicle Infrastructure Integration Consortium，VIIC）项目中，我们开发了车载设备和终到终隐私保护安全证书管理系统来实现安全通信。非常感谢包括 VIIC 项目主要负责人 Ralph Robinson、Dave Henry 和 Tom Schaffnit 在内的 VIIC 项目中的所有工程师和专家，他们都做出了卓越的贡献。宝马、克莱斯勒、福特、通用、本田、现代－起亚，梅塞德斯－奔驰、日产、丰田、大众－奥迪等公司都参与了 CAMP 和 VIIC 项目，在此，为它们能在当下如此激烈的竞争环境中配合开展本研究表示感谢。

在美国加利福尼亚州帕罗奥多的梅赛德斯－奔驰团队中，有一些 DSRC 方面的先驱致力于该项工作。Qi Chen 和 Daniel Jiang 与卡尔斯鲁厄理工学院的 Felix Schmidt－Eisenlohr 合作，共同开发了网络仿真器 2（Network Simulator 2，NS－2），本书中有许多结果都是由该软件模拟得出的。网络研究人员可以免费使用该软件。Michael Maile 带领团队开展了交

叉口协同避撞系统（Cooperative Intersection Collision Avoidance System for Violations，CICAS－V）的开发，同时他也是车路（V2I）协同系统研究领域的世界级专家之一。Craig Robinson 是 2008 年公开展示的综合安全系统的首席研发人员。Gordon Peredo、Graham Brown 和 Kyla Tirey 对 V2V 和 DSRC 系统研究有着多年的经验，他们在乘用车和商用车上建立了大量功能完整的模型系统。Mike Peredo 开发了应用于路测设备的软件，本书中有多张关于该软件的照片。Tessa Tielert 在 DSRC 项目的拥塞控制和可扩展性研究中取得了重大突破。

本书中有关隐私保护安全技术的车辆通信研究成果是在与 Telcordia 公司多位同事的密切合作下共同完成的，特别感谢 Stanley Pietrowicz、Hyong Shim、Giovanni Di Crescenzo 和 Eric van den Berg 的大力配合。我们已经与诸多工业界伙伴和汽车供应商建立了密切的合作关系，特别感谢 Roger Berg、Sue Graham 和日本电装国际（美国）的大力支持，是他们最早参与并研发了我们今天仍然在使用的平台和系统。

Andrew Moran 和 Yvonne Peredo 对本书第一部分内容中的数据和实例进行了研究和验证工作。John Kenney 对本书初稿提供了宝贵的意见。Emma Asiyo 和 Greg Stevens 对本书给予了支持。最后，特别感谢本书编辑的大力支持：Wiley 公司的 Diana Gialo 和 Kristen Parrish 以及 Toppan Best－Set Premedia 公司的 Stephanie Sakson。

Luca Delgrossi
Tao Zhang