中国通信学会
CHINA INSTITUTE
OF COMMUNICATIONS

车联网安全技术与标准发展态势前沿报告

（2019年）

中国通信学会

2019年12月

版权声明

专家组和撰写组名单

顾问(以姓氏笔划为序)：

方滨兴　中国工程院院士

邬贺铨　中国工程院院士

邬江兴　中国工程院院士

李　骏　中国工程院院士

李德毅　中国工程院院士

沈昌祥　中国工程院院士

专家组：

组长：

陈山枝　中国信息通信科技集团有限公司副总经理、专家委主任
　　无线移动通信国家重点实验室主任

成员(以姓氏笔划为序)：

姓 名	单　位	职 务
王云鹏	北京航空航天大学	副校长
王志勤	中国信息通信研究院	副院长
公维洁	中国汽车工程学会	副秘书长
朱西产	同济大学	教授
李克强	清华大学	教授
李震宇	百度公司	副总裁
陈卫强	厦门金龙联合汽车工业有限公司	技术总监
张同须	中国移动研究院	院长

张屹	三六零科技集团有限公司	标准部总监
周舟	中国汽车工程研究院股份有限公司	副总经理
夏俊杰	中国联通智能城市研究院	副院长
章文嵩	滴滴出行科技有限公司	高级副总裁
谢　飞	中国通用技术集团检验检测认证工作组	副组长
蔡速平	北京汽车集团公司	副总经理

撰写组(按单位排名)

单位	姓名
中国信息通信科技集团有限公司	陈山枝 徐晖 胡金玲 王勇 胡延明 梁承志
中国信息通信研究院	葛雨明 于润东
北京邮电大学	时岩
中国移动通信有限公司研究院	田野
中国智能网联汽车产业创新联盟	罗璎珞、刘建行
清华大学	温福喜
北京汽车集团公司	李峰
华为技术有限公司	陈璟 潘凯
中国联通智能城市研究院	高枫
东软集团股份有限公司	祁帅
中兴通讯股份有限公司	许玲
腾讯计算机系统有限公司	雷艺学
深圳奥联通信有限公司	程朝辉

前　言

车联网产业是汽车、电子、信息通信、道路交通运输等行业深度融合的新型产业形态，已成为我国战略性新兴产业的重要发展方向，是目前跨领域、综合性的研究热点。

目前我国已将车联网产业上升到国家战略高度，产业政策持续利好。我国车联网产业化进程逐步加快，形成了包括通信芯片、通信模组、终端设备、整车制造、运营服务、测试认证、高精度定位及地图服务等较为完整的产业链生态。车联网的功能安全、网络安全、隐私和数据安全是构建车联网应用的关键环节。

根据中国通信学会组织各专业委员会开展前沿报告的工作安排，通信设备制造技术委员会在 2018 年组织我国车联网产学研用各领域专家撰写了《车联网技术、标准与产业发展态势前沿报告》[1]，在业界反响热烈。2019 年在此基础上根据车联网技术和产业的发展情况，通信设备制造技术委员会继续组织专家撰写了《车联网安全技术与标准发展态势前沿报告》。

本报告分析了车联网安全的全球发展态势和我国发展现状，对车联网安全技术与产业发展态势和技术预见进行了预测，探讨了车联网安全面临的重大难题，提出了技术和产业政策建议。报告内容涉及面广，可作为高校、研究机构以及汽车、交通、通信、互联网、集成电路等行业的技术产业发展参考，也可作为政府部门制定政策的参考。

中国通信学会通信设备制造技术委员会

主任委员： 

2019 年 12 月

目 录

缩略语

3GPP	The 3rd Generation Partnership Project	第三代合作伙伴项目
5GAA	5G Automotive Association	5G 汽车协会
ADAS	Advanced Driver Assistant System	先进驾驶辅助系统
C-ITS	China ITS industry Alliance	中国智能交通产业联盟
C-V2X	Cellular V2X	基于蜂窝的车联网
CA	Certificate Authority	认证中心
CCMS	C-ITS Security Credential Management System	C-ITS 安全证书管理系统
CCSA	China Communications Standards Association	中国通信标准化协会
CPA	Certificate Policy Authority	证书策略管理机构
CPOC	Central Point of Contact	联络中心点
DSRC	Direct Short-Range Communication	直接短距离通信
ECA	Enrolment Certificate Authority	注册证书认证机构
ECC	Elliptic Curve Cryptography	椭圆曲线密码算法
ECTL	European Certificate Trust List	欧洲证书信任列表
ETSI	European Telecommunications Standards Institute	欧洲电信标准化协会
GBA	Generic Bootstrapping Architecture	通用引导架构
GCCF	Global Certificate Chain File	全球证书链文件
IEEE	Institute of Electrical and Electronics Engineers	电气和电子工程师协会
IP	Internet Protocol	互联网协议
IPSec	Internet Protocol Security	互联网协议安全
ISO	International Standards Organization	国际标准化组织
ITS	Intelligent Transportation System	智能交通系统
ITU-T	International Telecommunication Union-Telecommunication	国际电信联盟-电信标准化局
LA	Linkage Authority	链接认证机构
LOP	Location Obscurer Proxy	位置模糊处理代理

LTE	Long Term Evolution	长期演进
LTE-V2X	Long Term Evolution V2X	基于 LTE 的车联网
NHTSA	National Highway Traffic Safety Administration	美国高速交通安全管理局
OBU	On Board Unit	车载单元
PCA	Pseudonym Certificate Authority	假名证书认证机构
PKI	Public Key Infrastructure	公钥基础设施
RCA	Root Certificate Authority	根证书认证机构
RSU	Roadside Unit	路侧单元
SAE	Society of Automotive Engineers	汽车工程学会
SCMS	Subscriber Credential Management System	签约用户信用状管理系统
TLM	Trust List Manager	信任列表管理者
TLS	Transport Layer Security	传输层安全
V2X	Vehicle to Everything	车联网
V2I	Vehicle to Infrastructure	车到基础设施
V2N	Vehicle to Network	车到网络
V2P	Vehicle to Pedestrian	车到人
V2V	Vehicle to Vehicle	车到车
WAVE	Wireless Access Vehicular Environment	无线接入车载环境

一、 车联网安全研究概述

车联网是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车与车（V2V）、车与路边设施（V2I）、车与行人（V2P）以及车与网络（V2N）之间进行无线通信和数据交换与共享的网络系统。它通过人—车—路—网之间的实时感知与协同来实现智能交通管理、智能动态信息服务和智能车辆控制的一体化，向用户提供道路安全、交通效率提升和信息娱乐等各类服务，满足人们交通信息消费的需要。

目前，全球范围内普遍接受的 V2X（X：车、路、行人以及网络）车联网通信技术主要包括专用短程通信 IEEE 802.11p/DSRC（Dedicated Short Range Communication）技术和基于移动蜂窝通信系统的 C-V2X（Cellular-V2X）技术。其中 C-V2X[2]包括 LTE-V2X 和 NR-V2X，LTE-V2X[3]是大唐最早在 2013 年提出的概念，并于 2017 年在 3GPP 形成国际标准。由于通信标准的持续演进，在产业发展过程中，将基于蜂窝通信的车联网技术统称为 C-V2X，涵盖了当前正在研究的新空增强车联网技术，即 NR-V2X。与传统网络系统相比，车联网系统有着新的系统组成、新的通信场景，这些在系统安全性及用户隐私保护方面带来了新的需求与挑战。

车联网设备主要包括车联网终端和路侧设备。从车联网终端角度，由于车联网终端集成了导航、移动办公、车辆控制、辅助驾驶等功能，导致车载终端更容易成为黑客攻击的目标，造成信息泄露，车辆失控等重大安全问题。因此车载终端面临着比传统终端更大的安全风险。车载终端存在的多个物理访问接口和无线连接访问接口使车载终端

容易受到欺骗、入侵和控制的安全威胁，同时车载终端本身还存在访问控制风险、固件逆向风险、不安全升级风险、权限滥用风险、系统漏洞暴露风险、应用软件风险和数据篡改和泄露风险。从路侧设备的角度，由于路侧设备是车联网系统的核心单元，它的安全关系到车辆、行人和道路交通的整体安全，主要面临非法接入、运行环境风险、设备漏洞、远程升级风险和部署维护风险。

车联网的通信包括车内系统的通信和车与车、车与路、车与网络等的车联网通信，对于车内系统而言，LTE V2X 车载终端是车辆系统中的一个功能节点。而对于 LTE V2X 车载终端而言，车内系统是 LTE V2X 车载终端的执行器，包含了车内所有与其交互的电子电气系统。从车联网通信角度，LTE-V2X 技术包括蜂窝网通信场景和短距离直连通信场景的通信技术。在蜂窝网通信场景下，LTE V2X 车联网继承了传统 LTE 网络系统面临的安全风险，存在假冒终端、假冒网络、信令/数据窃听和信令/数据篡改/重放等安全风险。在短距离直连通信场景下，LTE V2X 系统除了面临假冒网络、信令窃听、信令篡改/重放等安全信令面安全风险外，还面临着虚假信息、假冒终端、信息篡改/重放和隐私泄露等用户面安全风险。从车内通信角度，由于车内系统通过车内网络（如 CAN 总线网络、车载以太网等）与车载终端相联，使整个车内系统暴露在外部不安全的环境中，车内系统面临假冒节点、接口恶意调用和指令窃听/篡改/重放等风险。

车联网应用主要包括基于云平台的业务应用以及基于 PC5/V5 接口的直连通信业务应用。基于云平台的应用以蜂窝网通信为基础，继承了“云、管、端”模式现有的安全风险，包括假冒用户、假冒业务服务器、非授权访问、数据安全等。直连通信应用以网络层 PC5 广

播通道为基础，主要面临伪造/篡改/窃听信息和用户隐私泄露等安全风险。

车联网数据来源广泛、种类众多，各种类型的数据在生成、传输、存储、使用、丢弃或销毁等各个阶段，在终端、网络、业务平台等各个层面均面临非法访问、非法篡改、用户隐私泄露等安全风险。

为了应对上述的安全风险和挑战，车联网系统需要对消息来源进行认证，保证消息的合法性；支持对消息的完整性及抗重放保护，确保消息在传输时不被伪造、篡改、重放；根据业务需求支持对消息的机密性保护，确保消息在传输时不被窃听，防止用户敏感信息泄露；支持对终端真实身份标识及位置信息的隐藏，防止用户隐私泄露。

本报告分析了车联网安全技术和标准在全球的发展态势和我国发展现状，对车联网安全技术与标准发展态势和技术预见进行了预测，探讨了车联网安全在工程建设中的重大难题，提出了技术和产业政策建议。报告内容涉及面广，可作为高校、研究机构以及汽车、交通、通信、互联网、集成电路等行业的技术产业发展参考，也可作为政府部门制定政策的参考。

二、 全球发展态势

（一）综述

LTE-V2X 是为了支持基本道路安全等车联网业务需求,在蜂窝架构基础上，扩展了终端直连通信特性。3GPP 标准组织在现有 LTE 网络的基础之上引入了 V2X 控制功能网元，对车联网终端及业务进行管控，并对上层业务提供方提供服务支撑，满足业务需要。在此网络架构下，LTE V2X 系统安全分为蜂窝通信场景和直连通信场景的安

全。

蜂窝通信场景下的安全架构（如图 1 所示）与 LTE 的安全架构类似，包括网络接入安全、网络域安全、认证与密钥管理、车联网接入安全、车联网业务能力开放安全、网络安全能力开放、应用层安全和车内系统及接口安全。其中网络接入安全、网络域安全、认证与密钥管理和网络安全能力开放继承了 LTE 网络现有安全机制。车联业务接入安全是车联网系统新增的安全域，对于 LTE 网络而言属于应用层安全。它在终端与其归属网络的 V2X 控制功能之间提供双向认证，对终端身份提供机密性保护；在终端与 V2X 控制功能之间对配置数据提供传输时的完整性保护、机密性保护和抗重放保护。车联业务能力开放安全也是车联网系统新增的安全域，保证对上层应用提供 LTE V2X 业务能力开放过程中的接入及数据传输安全。它可采取类似于网络域安全的方法来保护，在不同安全域之间采用 IPSec、TLS 等安全机制为业务提供双向认证、加密、完整性保护和抗重放的安全保障。

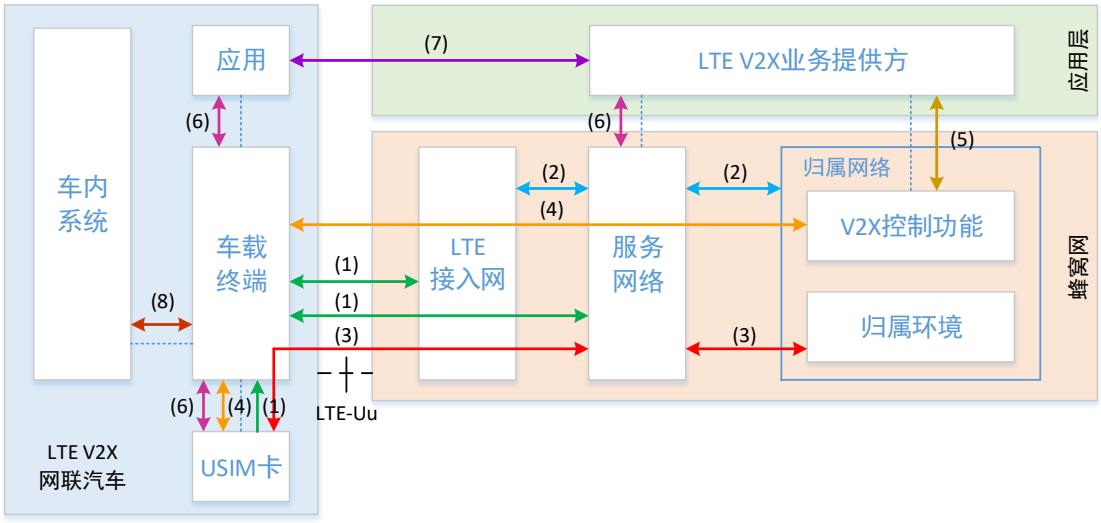

图 1 蜂窝移动通信场景下 LTE-V2X 安全架构[5]

直连通信场景下的 LTE-V2X 系统安全架构（如图 2 所示）包括网络层安全、安全能力支撑、应用层安全、车内系统及接口安全和外部网络域安全。根据 3GPP 组织的 REL14 的规范，终端在网络层不采取任何机制对 PC5 接口上广播发送的直连通信数据进行安全保护，数据的传输安全完全在应用层 V5 接口保障。网络层仅提供标识更新机制对用户隐私进行保护。终端通过随机动态改变源端用户层二标识和源 IP 地址，防止用户身份标识信息在 PC5 广播通信的过程中遭到泄露、被攻击者跟踪。网络层向应用层提供安全能力支撑，采取用户标识跨层同步机制确保源端用户层二标识、源 IP 地址与应用层标识同步更新，防止由于网络层与应用层用户身份标识更新的不同步，导致用户标识关联信息被攻击者获取，用户隐私信息遭到泄露。

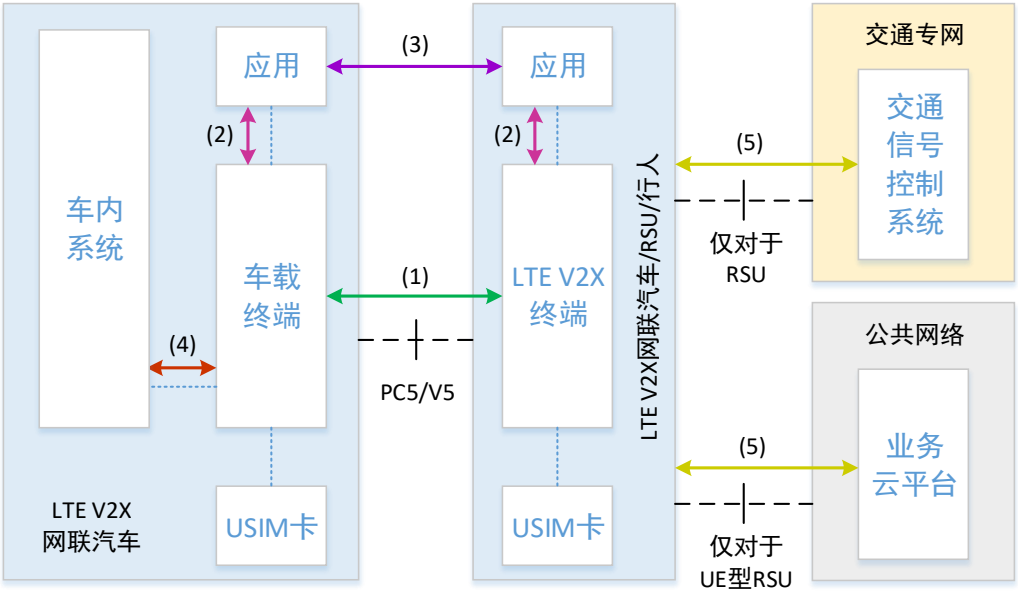

图 2 直连通信场景下的 LTE-V2X 安全架构[5]

因此对于 PC5/V5 直连通信接口，LTE V2X 系统主要依靠应用层安全来解决安全风险。

目前，车联网系统在应用层主要考虑采用数字证书的方法实现业务消息的安全保护，相应地系统需要部署 CA 基础设施实现数字证书

全生命周期的管理。通信交互时，车联网终端使用数字证书对将要发送的业务消息进行签名，对所接收到的业务消息进行验签，从而保证消息的完整性以及业务消息来源的合法性。

（二）车联网安全管理系统发展态势

IEEE 1609 系列协议是 WAVE 的高层协议，其中 IEEE1609.2 定义了 WAVE 的安全消息格式及处理过程，是一种较为成熟的车联网安全标准，它借鉴了传统 PKI 系统的体系结构，通过证书链实现终端互信。

车联网证书管理系统中每个模块通过网络交换有效信息，协同工作，共同对外提供安全服务，主要模块有：

- Root CA（根 CA，RCA）

RCA 是所有 CA 的管理者，也是可信系统的中心，以分层的方式为下级 CA 颁发证书。根 CA 的操作与运行需要在隔离的安全环境中，并且需要确保根 CA 服务器为离线状态，以防遭遇来自互联网的攻击。

- Enrollment CA（注册 CA，ECA）

ECA 为终端颁发准入证书，只有获得准入证书的终端设备才可接入系统，并且通过网络申请车联网证书管理系统的其他服务。

- Pseudonym CA（假名 CA，PCA）

PCA 负责颁发设备的短时匿名证书。设备之间通过匿名证书实现可信的信息交互。

目前美国和欧洲均在 IEEE1609.2 的基础上根据各自的实际情况和管理需求设计了相应的车联网安全管理系统。

SCMS 系统是美国针对 V2X 应用层安全设计的一套证书管理系

统，包含了证书颁发、证书撤销、终端安全信息收集、数据管理、异常分析等一系列与安全相关的功能，以此确保 V2X 的安全通讯，其主要结构如图 3 所示。

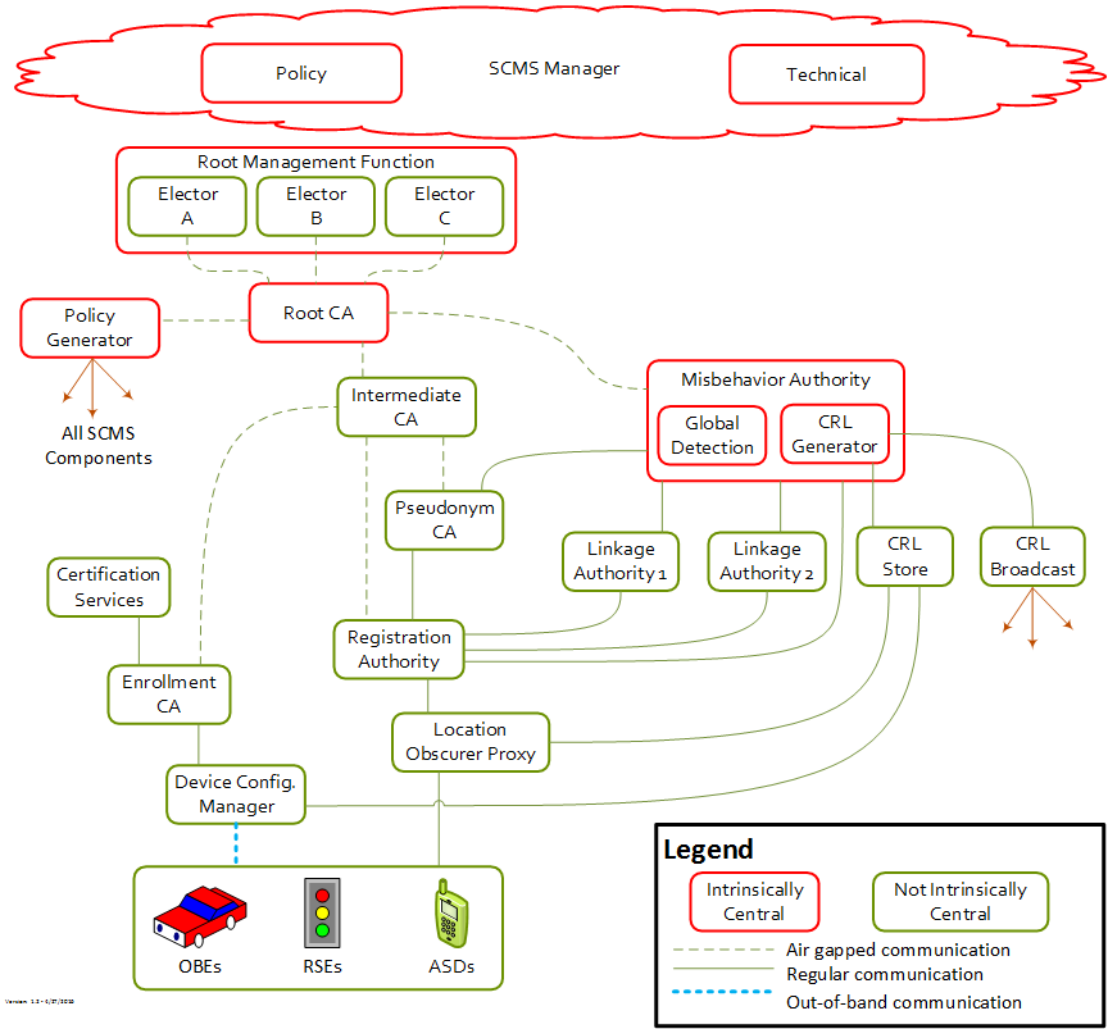

图 3　SCMS 系统架构[20]

CCMS 是欧洲针对合作式智能交通设计的一套证书管理系统，主要结构如图 4 所示。CCMS 考虑不同的信任模型，允许一个或多个根 CA 存在，可以实现单根 CA、交叉认证、桥接 CA 和证书信任列表等多种证书管理模式。

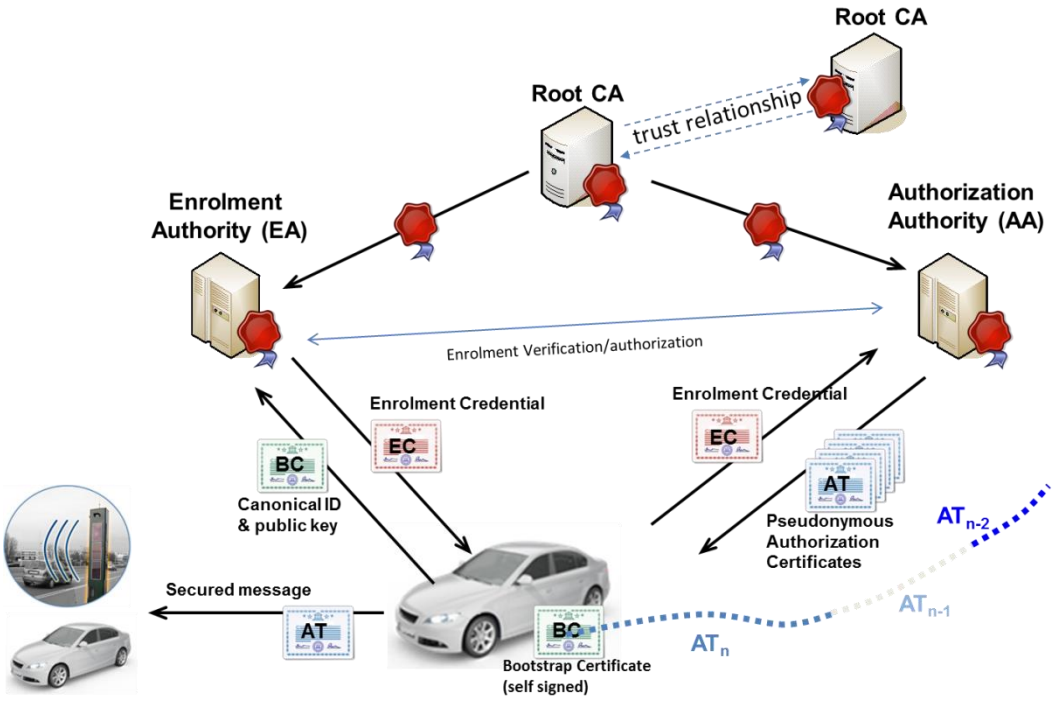

图 4 CCMS 系统架构[15]

（三）车联网安全信任锚点模型发展态势

在车联网证书管理系统中信任锚点在车联网安全中扮演着非常重要的角色，所有车载终端授权和通信的安全性取决于信任锚的安全性。在车联网证书管理系统中，共同的信任锚点是根证书颁发机构，根节点是车联网中受信任的实体，允许其自己颁发自签名证书。使用车联网证书管理系统的所有设备，以及系统中所有关联的网络功能，都必须通过某种安全手段来建立对根 CA 的合法性和完整性的信任（即未发生损害）。常用的信任锚点管理机制是保护信任 CA 列表的可信列表。例如可以作为预配置的一部分，通过安全的初始过程（例如带外证书下载）为车辆 OBU 提供根 CA 列表。

美国的 SCMS 系统有一个管理组件负责对策略和根进行管理，如图 5 所示。SCMS 的根 CA 管理包括一系列选举人，这些选举人是认可或撤销根CA证书并认可或撤销选举人证书的受信任的设备和组

织。选举人和根 CA 是信任锚点系统的一部分。此选举人机制可提供针对单点故障风险的保护，由于大多数选举人可以撤销或认可另一个选举人证书或根 CA 证书，因此 SCMS 允许采用标准化方式交换系统中的任何 CA 证书。

SCMS 系统使用 SCMS 管理器来确认根 CA 的可信度。同时 SCMS 管理器还包括策略生成器，负责维护策略文件以及包含所有信任链的全局证书链文件（GCCF）。

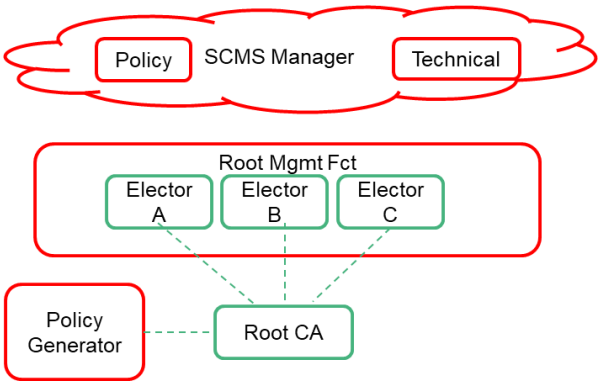

图 5 美国 SCMS 系统的可信锚点模型[9]

在欧洲，车联网证书管理系统 CCMS 使用信任列表管理器（TLM）作为可信锚点，可以认可或撤销根 CA，这些根 CA 放置在欧洲证书信任列表（ECTL）上，并由与 TLM 相关的 CPOC 分发，如图 6 所示。CCMS 使用 C-ITS 证书策略颁发机构（CPA），其作用是任命 TLM 并确认 TLM 可以信任 CPA 批准运行的根 CA。根 CA 的可信度记录在由 TLM 签署的欧洲中央信任列表（ECTL）中。

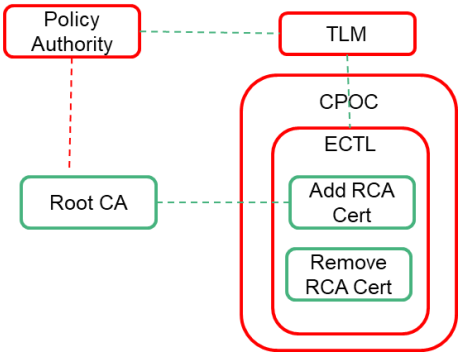

图 6 欧洲可信锚点管理实体[9]

（四）车联网隐私保护技术发展态势

车联网应用的隐私包括位置隐私、用户数据隐私和用户身份隐私。车联网应用不仅能够为驾驶者提供道路周边基础设施和导航信息，还能对车辆位置及其他相关信息进行详细记录。在车联网中，用户的身份隐私和位置隐私相互关联，密不可分，攻击者通过身份信息可以追踪到车辆的位置信息，通过车辆的位置信息可以追踪到车辆的行驶轨迹，进而可以揭示用户的身份信息。所以在车联网通信中既要保护车辆的身份隐私，也要保护车辆的位置隐私。

2017 年，美国众议院通过了《确保车辆演化的未来部署和研究安全法案》。不同于以往的“非强制性”规定,该法案属于首次从联邦层面规制自动驾驶的法案。法案要求自动驾驶汽车的开发者需制定数据的隐私保护计划,且禁止生产商在没有隐私保护计划的情况下销售自动驾驶汽车。法案规定隐私政策需明确以下内容:(1)信息被收集、使用、分享和存储的方法;（2）提供给车主或使用者关于该类信息收集、使用、分享和存储的选择;（3）生产商关于车主或使用者数据最小化、去标识化,及保留方面的做法;（4）隐私保护的要求如何延伸适用于分享使用数据的主体的做法。

欧盟 GDPR 关于个人数据保护的规定将统一适用于自动驾驶数据中的个人数据。在行业自律层面，2014 年，汽车制造商联盟(Alliance of Automobile Manufacturers)和全球汽车制造商协会(Association of Global Automakers)为汽车技术和服务制定了 7 条隐私保护原则,涉及透明性、选择性、尊重情景、数据最小化、数据安全、完整性和可取

性、可责性等;另外规定，只有在基于与消费者的合同、经消费者同意或为了履行法律要求的情况下才可与第三方共享个人数据。

目前车联网中主要是通过对车载终端的通信证书采用匿名的方式来保护用户标识，并根据设定的逻辑更换所使用的通信证书来达到保护用户隐私的目的。

为了平衡匿名证书数量与隐私保护间的矛盾，美国的 SCMS 系统选择每周颁发 20 张匿名证书，并且规定当移动距离大于 2 千米且移动时间超过 5 分钟时需更换一次匿名证书。在更换证书的同时，终端同步更换设备的 MAC 地址，从而防止攻击者利用设备的 MAC 地址对用户进行实时跟踪。为了防止攻击者描绘用户的历史轨迹，SCMS 系统规定匿名证书的有效时间为一周，超过一周需使用下一批匿名证书。同时，匿名证书在使用前以加密方式存储，防止设备被入侵后匿名证书被非法获取。

在服务端，SCMS 系统设计采用位置模糊化代理（LOP）将所有终端设备的地址进行替代处理，从而使 SCMS 系统中的其他单元无法获取终端设备的准确位置信息。为了防止 LOP 对服务请求信息进行监听，终端设备的服务请求数据采用加密方式发送，由 LOP 转发给 RA，RA 可对接收到的密文请求数据解密并进行相应的处理。

为了保护用户隐私，SCMS 对系统侧服务单元提出了严格的匿名管控标准，要求系统中的任何单一服务设备均无法根据自身获取的信息独立判断出两张匿名证书是否将颁发给同一个终端使用，切断匿名证书间的关联性。为此，SCMS 系统采用两个 LA 服务器，防止单一 LA 服务器通过链接值扩展来确定证书关系。此外，在匿名证书申请过程中，在 RA 处设计了洗牌模式，防止 PCA 获取确切的终端信息。

RA 在收到终端设备的匿名证书请求后将其扩展，并将多个终端扩展后的请求进行统一的洗牌处理，最后再发送给 PCA 申请证书。

欧洲匿名证书预装载的时间最多为三个月，有效期不超过一周，并行有效的最大数量为每个节点最多 100 个证书，同时匿名证书中不包含任何可能将主题与其真实身份相关联的名称或信息。

（五）车联网安全监管发展态势

目前，美国、英国、德国等国家陆续发布与智能网联汽车与自动驾驶相关的法律法案，力图从国家层面细化涉及汽车全生命周期各参与体的网络安全责任，加强对车联网安全的重视程度。

美国 2016 年公布《自动驾驶汽车政策》，将高度自动驾驶汽车的安全部署任务分为四大部分，包括自动驾驶汽车性能指南、州政策模式、现行监管方式和监管新工具与权力。

美国交通部道路交通安全管理局（NHTSA）在 2017 年 8 月发布了新版《联邦自动驾驶系统指南：安全愿景 2.0》，要求汽车厂商采取措施应对网络威胁和网络漏洞，对车辆辅助系统进行网络安全评估。

英国要求汽车制造商承担起包括抵御网络攻击、对抗黑客在内的一系列网络安全责任。2017 年 8 月，英国政府发布《智能网联汽车网络安全关键原则》，提出包括顶层设计、风险管理与评估、产品售后服务与应急响应机制、整体安全性要求、系统设计、软件安全管理、数据安全、弹性设计在内的 8 大方面关键原则。将网络安全责任拓展到供应链上的每个主体，并强调在汽车全生命周期内考虑网络安全问题。

德国在 2017 年 6 月颁布了《道路交通法第八修正案》与《自动

驾驶道德准则》。《道路交通法第八修正案》原则性规定了自动驾驶的定义、驾驶人的责任与义务、驾驶数据的记录等内容，为自动驾驶各方利益主体规定了权利义务边界，提出政府监管方向。《自动驾驶道德准则》作为全球第一个自动驾驶行业的道德准则，通过在道路安全与出行便利、个人保护与功利主义、人身权益或财产权益等方面确立优先原则，为自动驾驶所产生的道德和价值问题立下规矩。

（六）车联网安全标准

目前国际上各大标准组织积极进行车联网安全的研究和标准化工作，均设立了专门的安全工作组开展车联网安全标准的研制工作，为车联网安全的发展提供必要的理论依据。

国际标准化组织 ISO 是负责除电工电子领域外的国际标准化工作的非政府性国际组织，其下属道路车辆技术委员会（TC22）成立 SC32/WG11 Cybersecurity 信息安全工作组，联合美国汽车工程师协会（SAE）共同开展信息安全国际标准 ISO 21434 Road Vehicles — Cybersecurity engineering 的制定工作。该标准旨在定义整个车联网产业链中使用的通用术语，明确车联网中关键网络安全问题，设定车辆网络安全工程的最低标准，并为相关监管机构提供参考。ISO/IEC JTC1 SC27（信息安全、网络空间安全和隐私保护技术委员会）的 WG3（安全评估、测试和规范工作组）中，《基于 ISO/IEC 15408 的网联汽车信息安全测评准则》标准研究项目，旨在基于 ISO/IEC 15408 标准，分析网联汽车面临的安全威胁和安全目标，提出安全要求和安全功能组件。

美国汽车工程师协会（SAE）中的汽车电子系统安全委员会负责

汽车电子系统网络安全方面的标准化工作，制定了全球第一个关于汽车电子系统网络安全的指南性文件 J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems，该文件定义了完整的生命周期过程框架，将网络安全贯穿了从概念阶段到生产、运营、服务和退役的所有生命周期，为开发具有网络安全要求的汽车电子系统提供了重要的依据。该文件为车辆系统提供了网络安全的基本指导原则，为后续的车联网安全的标准化工作奠定了基础。

国际电信联盟（ITU-T）SG17 工作组已经开展了对智能交通以及联网汽车安全的研究工作。有 12 个标准项目，包括：软件升级、安全威胁、异常检测、数据分类、V2X 通信安全、边缘计算、车内以太网安全等。目前已经正式发布的标准有 X.1373 Secure software update capability for intelligent transportation system communication devices，这个标准通过适当的安全控制措施，为远程更新服务器和车辆之间提供软件安全的更新方案，并且定义了安全更新的流程和内容建议，该标准正在修订中。目前，ITU-T 在研的标准有 Security guidelines for V2X communication systems for determination，Security Requirements of Categorized Data in V2X Communication 和 Security threats in connected vehicles，主要围绕 V2X 面临的安全威胁和安全需求，提出相应的安全指南，该标准已经冻结，即将发布。

联合国世界车辆法规协调论坛（WP.29）成立了汽车信息安全任务组（TFCS/OTA），提出了关于网络安全和信息保护措施的指南草案，并正在以该任务组提交的研究报告为基础，制定汽车信息安全专用国际法规。

为实施更为安全的保护，ETSI 中的 ITS 技术委员会制定了相应

的技术规范，该技术规范主要包括安全架构、安全服务、安全管理、隐私保护等方面。

3GPP SA3 在 REL 14 开始进行 LTE-V2X 安全的研究和标准化工作，形成了 3GPP TS 33.185 Security aspect for LTE support of Vehicle-to-Everything (V2X) services 标准规范，规定了 LTE-V2X 的安全架构以及安全机制。目前 3GPP SA3 在 REL 17 开始研究 eV2X 的安全，主要围绕 5G-V2X 的安全需求和安全关键问题进行研究。

三、 我国发展态势

（一）车联网安全管理系统发展态势

为了实现车联网终端之间的安全认证和安全通信，我国的车联网系统使用基于公钥证书的 PKI 机制确保终端间的安全认证和安全通信,通过采用数字签名和加密等技术手段实现车联网终端之间消息的安全通信。因此需要车联网安全管理系统来实现证书颁发、证书撤销、终端安全信息收集、数据管理、异常分析等一系列与安全相关的功能，确保车联网应用安全。

车联网安全管理系统是车联网安全通信的重要组成部分，包括注册 CA、V2V 假名 CA、V2I 授权 CA 和证书撤销 CA 等，车联网安全管理系统的架构及可信模型与我国车联网业务及其管理模式紧密相关。

根据我国车联网发展情况及业务需求，可以看出我国的车联网安全管理系统会存在两种可能的架构，即集中式管理架构和分布式管理架构。

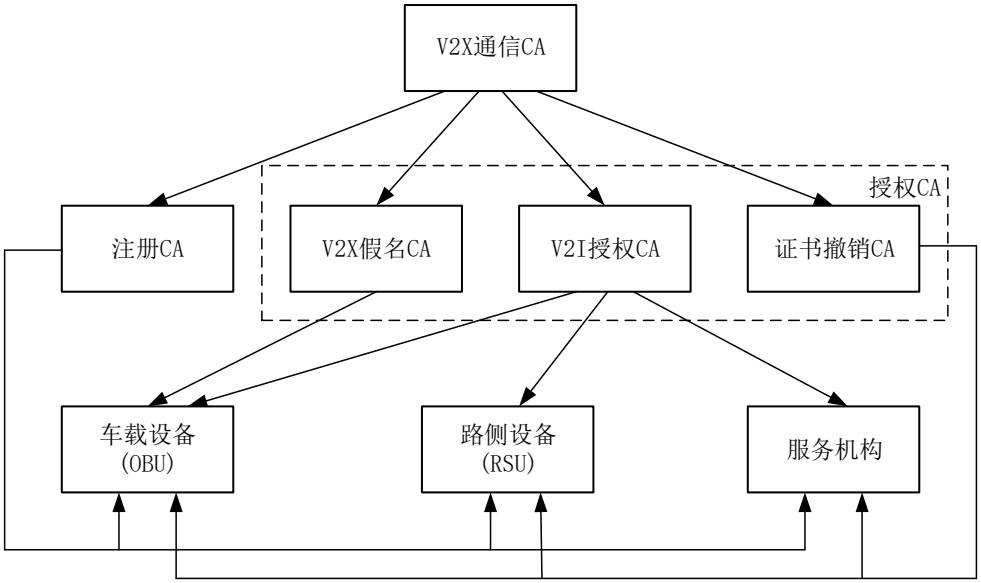

图 7　集中式车联网安全管理系统架构[5]

图 7 给出了集中式车联网安全管理系统架构。该架构采用单一根 CA 的方式，部署统一的 CA 体系结构，所有的子 CA 都在同一个根 CA 下管理。根 CA 可由车联网管理责任部门负责运营维护。这种部署方式适用于对车联网有明确主管责任部门进行统一管理的场景。集中式部署的优点是所有的证书由统一的根 CA 管理，管理比较简单，缺点是不能重用现有的 CA 系统，需要重新建立新的 CA 体系。

图 8 给出了分布式车联网安全管理系统架构，该架构通过 CA 之间的交叉认证实现可信的 PKI 体系。

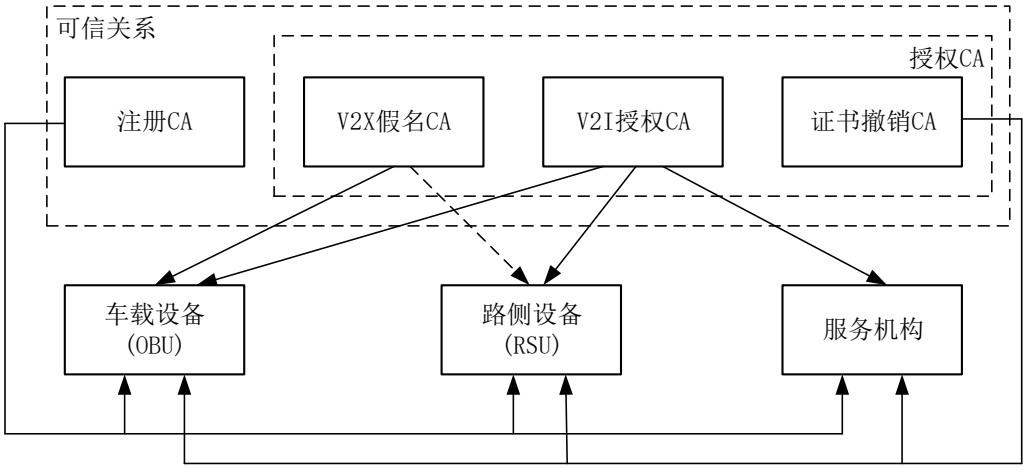

图 8　分布式安全基础设施部署方式[5]

分布式部署方案不需要有共同的根 CA，不同的业务可以设置不同的根 CA，但需要在不同的根 CA 之间建立互信关系。这种部署方式适用于多部门共同对车联网进行管理和维护的场景。这种方式的优点是容易对接现有的管理机制，可在现有 CA 系统中增加相应的功能即可。缺点是需要执行交叉认证，增加了消息长度和消息处理时延。

需要注意的是，不管使用哪种部署方案，颁发证书的 CA 都需要具备很高的安全性。攻击者可能可以从不安全的 CA 系统获得 CA 颁发的有效证书，进而发送恶意构造的 V2X 消息，造成严重的后果，如车辆碰撞等交通事故。颁发证书的 CA 应根据当前业界的最佳实践，通过第三方评估认证等方式，证明自身的安全性和公信力。

（二）车联网安全管理系统产业实践

车联网安全管理系统是车联网商业化部署应用的重要保障。车联网“人-车-路-云”通信过程中需要对车载设备、路侧基础设施等参与主体的身份合法性进行安全认证，避免车联网设备因黑客攻击，误导车辆做出错误判断，甚至导致车辆碰撞等危害事件发生。目前国内相关单位持续开展 V2X 通信安全研究和标准制定，国家标准化管理委员会在 2019 年 5 月发布了国标 GB/T 37376-2019《交通运输 数字证书格式》、GB/T 37374-2019《智能交通 数字证书应用接口规范》和 GB/T 37373-2019《智能交通 数据安全服务》。中国通信标准化协会（CCSA）完成了行标《基于 LTE 的车联网通信安全技术要求》、《车联网信息服务 数据安全技术要求》、《车联网无线通信安全技术指南》、《车联网信息服务 用户个人信息保护要求》和《车联网信息服务平

台安全防护要求》的制定。同时，CCSA、C-ITS 和全国汽车标准化技术委员会正在制定多部 V2X 通信安全标准，众多企业已经依据标准开展了车联网通信安全的测试验证活动。

2018 年 4 月，中国信息通信科技集团有限公司（中国信科）发布了业内首个车联网安全管理系统，该系统实现了注册 CA、V2V 假名 CA、V2I 授权 CA 和证书撤销 CA 等功能，实现了车联网注册证书、匿名证书、应用证书和证书撤销列表的管理，实现了车联网安全的验证。

2019 年 8 月，国汽（北京）智能网联汽车研究院有限公司搭建的 VSS 系统众测平台正式对外开放。VSS 是针对 V2X 通信设计构建的安全认证防护系统，是推广 V2X 应用不可或缺的组成部分。VSS 包括根 CA、中间证书 CA、注册证书 CA、消息证书 CA 和受理服务器 AS。

2019 年 10 月 22 日到 24 日，由 IMT-2020（5G）推进组 C-V2X 工作组、中国智能网联汽车产业创新联盟、中国汽车工程学会、上海国际汽车城（集团）有限公司共同主办的 C-V2X“四跨”互联互通应用展示，重点演示了车联网通信安全身份认证机制，实现“跨芯片模组、跨终端、跨整车、跨安全平台”的全方位演示。演示活动应用场景和安全机制全面依照国内 LTE-V2X 标准体系进行技术开发，由中国信科和国汽智联搭建的车联网安全管理平台为车载通信终端 OBU 和路侧终端 RSU 提供通信证书，实现 V2V、V2I 直连安全通信，综合演示车联网通信安全机制。

（三）车联网安全监管

近两年，我国陆续颁布车联网相关的法规政策，安全作为车联网的重要组成部分，在相应的法规政策中都被着重提出，从安全管理和安全技术层面都有相应的规定和要求。

2017 年 6 月 1 日开始实施的《中华人民共和国网络安全法》，明确要求网络运营者履行网络安全保护义务，依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行。有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

2018 年 6 月，工信部和国家标准化管理委员共同颁布了《国家车联网产业标准体系建设指南》，在智能网联汽车标准体系的通用规范中，规划了信息安全类（编号 204）的标准体系。在遵从信息安全通用要求的基础上，以保障车辆安全、稳定、可靠运行为核心，主要针对车辆及车载系统通信、数据、软硬件安全，从整车、系统、关键节点以及车辆与外界接口等方面提出风险评估、安全防护与测试评价要求，防范对车辆的攻击、侵入、干扰、破坏和非法使用以及意外事故。在信息通信标准体系的网络与数据安全部分，涉及安全体系架构、通信安全、数据安全、网络安全防护、安全监控、应急管理等方面的标准。

2018 年 1 月，发改委组织起草了《智能汽车创新发展战略（征求意见稿）》，明确提出构建全面高效的智能汽车信息安全体系，保障

车联网网络安全产业的健康有序发展。明确提出完善信息安全管理联动机制，明确相关主体的安全管理责任，定期开展安全监督检查；从云、管、端全方位加强信息安全系统防护能力；加强数据安全防护管理。建立智能汽车数据全生命周期的安全管理机制，加强数据安全监督检查，开展数据风险、数据出境安全等评估工作，加强管理制度建设。

在 PKI 管理方面，2009 年颁布的《电子认证服务管理办法》明确了对电子认证服务提供者实施监督管理的方法，包括提供电子认证服务机构的资质要求、电子认证服务许可申请流程等。

（四）车联网安全标准

为了适应车联网的发展，TC114、TC260、CCSA、C-ITS 等都设立了车联网安全相关工作组，加速研制车联网安全标准，重点关注车联网无线通信安全和数据安全。

全国汽车标准化技术委员会（简称汽标委）下属的智能网联汽车分技术委员会（TC114）负责归口管理我国智能网联汽车领域的国家标准和行业标准，成立了先进驾驶辅助系统（ADAS）标准工作组、信息安全、自动驾驶等工作组。2017 年，汽标委正式成立汽车信息安全标准工作组，已完成《汽车信息安全通用技术要求》、《车载网关信息安全技术要求》、《汽车信息交互系统信息安全技术要求》等 3 项汽车信息安全基础标准和《电动汽车远程管理与服务系统信息安全技术要求》、《电动汽车充电信息安全技术要求》等 2 项行业急需标准的预研工作，并向国家标准化管理委员会提交了推荐性国家标准立项申请。

全国信息技术安全标准化技术委员会（信安标委）TC260 是国家标准化管理委员会的直属标准化技术委员会。2017 年 7 月，TC260 立项了与车联网安全相关的强制性国家标准项目《信息安全技术网络产品和服务安全通用要求》。

中国通信标准化协会（CCSA）长期致力于车联网系列标准的制定，研制的车联网安全相关标准涵盖车联网安全的方方面面，目前，CCSA 已经完成了行标《基于 LTE 的车联网通信安全技术要求》、《车联网信息服务 数据安全技术要求》、《车联网无线通信安全技术指南》、《车联网信息服务 用户个人信息保护要求》和《车联网信息服务平台安全防护要求》的制定，正在研制的车联网安全相关标准有《基于 LTE 的车联网无线通信技术 安全证书管理系统技术要求》、《基于 LTE 的车联网无线通信技术 安全认证测试方法》。

四、 技术预见

（一）5G 车联网安全技术

随着蜂窝通信技术的不断发展，LTE V2X 车联网也将朝向 NR V2X 技术方向演进。5G 在车辆联网领域的应用主要体现在道路环境感知、远程驾驶、编队驾驶等方面，车辆联网系统的实现需要依靠强大的通信能力来依赖和支持。5G 的低延迟、高可靠性特性及大容量的通信设备，使车辆联网的发展和应用更加可靠和迅速。

NR V2X 车联网业务具有不同的安全等级和安全需求，例如编队驾驶场景中车联网消息将只在编队中传播，编队之外的车辆不应收到处理编队的消息，因此在这种场景下车联网系统应该考虑支持机密性。因此 NR V2X 车联网安全除了继承了 5G 网络的安全风险和挑战外，

还面临着新的安全需求。

NR V2X 车联网为了支持更多的车联网业务和场景，在 PC5 接口上引入了单播和组播模式，因此需要相应的安全机制来保证车联网消息的完整性、机密性和抗重放攻击，同时也需要研究相应的隐私保护机制来保证 5G 车联网的安全。

（二）车联网与边缘计算融合的安全

边缘计算是 5G 网络中实现低时延业务的使能技术之一，可以提供对车联网基础通信能力的支持。同时边缘计算还可以对车联网的其它前瞻性应用场景，如交叉口信号灯控制参数优化、区域内高精度地图的实时加载、区域内自动驾驶车辆的调度等提供支持，因此车联网将与边缘计算技术相结合，形成分层、多级边缘计算体系，满足高速、低时延车联网业务处理及响应的需要。

但是边缘计算的数据处理实时性、数据多源异构性、终端资源受限性和接入设备复杂性，使得传统云计算环境的安全机制不再适用于边缘设备产生的海量数据的安全防护，边缘计算的数据存储安全、共享安全、计算安全、传输和隐私保护等问题成为边缘计算模型必须面对的安全挑战。

车联网与边缘计算融合的体系架构需要针对数据安全、身份认证、隐私保护和访问控制提出相应的安全机制，保证车联网业务的安全开展。传统的网络与业务的信任模型不能适应新的业务模式，例如边缘计算与车联网应用之间的信任关系缺失会导致攻击者接管用户服务，因此需要研究车联网业务与边缘计算之间新的信任模式，满足边缘计算系统与车联网系统共生融合的部署方式。

（三）车联网通信设备认证及安全交互技术

为了确保车联网业务中消息来源的真实性、内容的完整性、防止消息重放，采用数字证书通过数字签名/验签的方式对车联网业务消息进行保护。为了实现上述机制，车联网终端需要完成设备初始化，以安全的方式完成密码公私钥对、数字证书等敏感参数的初始配置。该过程对设备安全生产环境有着较为严格的要求，给车企及 C-V2X 终端生产企业带来了新的挑战。

目前车联网设备的初始安全配置过程主要是由车辆生产企业在生产线上完成，对终端设备厂商有较高的安全生产要求，需要根据车联网的安全要求对生产线进行改造。特别是终端设备公私钥对的产生以及登记注册证书的申请对于生产线有更加严苛的安全要求。企业不仅面临着生产线、生产流程升级改造的问题，同时还面临着安全生产合规、安全审计、安全信任关系构建、安全成本管控等多方面难题。因此需要更为有效的车联网通信设备认证及安全交互方法，满足车企对车联网设备初始安全配置的需要。

3GPP 定义的 GBA（Generic Bootstrapping Architecture，通用引导架构）框架提供了一种基于移动通信网络和用户卡的通用认证和会话密钥管理机制，可以为应用层业务提供完整的安全认证及应用层会话通道加密服务。因此如何将 GBA 框架应用在车联网安全体系下是目前研究的热点，车联网安全管理系统通过引入 GBA 机制，可以在不需要根证书的情况下安全地进行多证书的安全导入，有助于建立证书间的互信机制，以解决隶属于不同 CA 管理系统的节点间消息验证及互通的问题。

（四）车联网安全管理系统增强技术

车联网安全管理系统支持对车联网设备进行证书的安全发放、使用和撤销，当车联网安全管理系统检测到恶意的车联网设备时需要将其证书撤销，或者当车联网设备发生故障或者报废时，需要将颁发给车联网设备的证书撤销。因此，车联网设备的异常行为检测和报告是车联网安全管理系统的重要组成部分。

目前异常行为检测包括本地的异常行为检测和后台安全运营中心的全局异常行为检测。本地的异常行为检测可以通过车联网设备检查接收到的安全消息的完整性、可靠性和正确性，以及结合车辆的传感器信息进行分析、判断。由于本地异常行为检测仅能在时间和空间上提供有限的信息，因此只依靠本地的检测不足以可靠地识别攻击者，因此需要依赖于后台安全运营中心的全局检测，后台安全运营中心的全局异常行为检测可以通过实时对车载智能终端设备的系统资源、应用行为、网络连接以及 CAN 总线接口的监测，结合云端的安全大数据进行分析，发现并定位车载终端中的异常行为，并根据预置策略执行阻断，实现基于终端检测与响应技术（Endpoint Detection and Response）的车载智能终端动态防护。例如，车联网安全管理系统既可以识别、处置来自车联网设备的异常请求，也可以通过依靠威胁情报和大数据能力，创建并持续学习不同场景、不同工况下的车联网行为模型，根据行为模型对监测到的异常行为进行安全分析，对异常行为可造成的汽车信息安全事件进行告警、预测和处置，从而建立起检测车联网设备异常行为的能力。但是目前这两种异常行为检测方法仍存在对正常车联网设备异常行为误报、漏报的问题，需要不断地改进

检测机制和算法，从而保证现有的车联网设备的正常运行不被干扰。

（五）可信计算在车联网中的应用

车联网安全威胁主要来源于三个方面：车载终端设备安全、车联网通信安全以及车联网运营安全。车联网被攻击的核心是通过各种方式入侵车辆总线系统来实现对汽车的控制，因此车联网安全技术应从车载终端、车联网运营端及车辆通信三个层面进行安全布局。

可信计算体系架构以密码体系为基础、可信主板为平台、可信软件为核心、可信网络连接为纽带，为计算体系提供度量和控制服务，保障信息和网络环境的整体安全。引入可信计算体系架构可以从根本上解决车联网安全问题。

可信计算商用化发展可以追溯到 1999 年 10 月，由 HP、IBM、Intel 和 Microsoft 等公司牵头组织 TCPA。TCPA 专注于从计算平台体系结构上增强其安全性。目前国际上的标准为 2003 年 TCG 组织发布的 TPM2.0 标准，该标准被广泛推广使用。国内则在可信计算 2.0 基础上推出了可信计算 3.0 的概念，能够保证车联网体系结构、资源配置、操作行为、数据存储可信，因此将可信计算的体系结构引入车辆网安全架构可以从计算平台体系结构上解决其安全性问题。

（六）基于区块链理念的车联网及安全技术

区块链作为分布式数据存储、点对点传输、共识机制、加密算法等技术的集成应用,被认为是继大型机、个人电脑、互联网之后计算模式的颠覆式创新,很可能在全球范围引起一场新的技术革新和产业变革。区块链技术的发展需要云计算、大数据、物联网等新一代信息技术作为基础设施支撑,同时他也对推动新一代信息技术产业发展具

有重要的促进作用。

车联网存在数据来源广，多方参与，利益不一致且无单一可信方和大量流程交互等特点。可以发现,区块链技术所倡导的解决问题的场景和优势与车联网特征不谋而合。利用区块链,可以通过数据防篡改和可追溯的统一账本来记录车联网中各个参与方整个生命周期的信息,该账本在各参与方之间共享（参与方既可以是信息提供者,又可以是信息使用者），实现去中心化的信息互通。同时,结合智能合约、链上链下数据互通等更前沿的技术,可实现整个价值链上各种流程的自动化和智能化。

区块链很可能在车联网领域引起一场技术革新和产业变革，从而推动车联网及安全技术的发展，产生颠覆式的创新。

五、 工程难题

（一）满足车联网安全需求的安全芯片

为了确保车联网通信消息来源的真实性、内容的完整性、防止消息重放，目前采用数字证书通过数字签名/验签的方式对车联网消息进行保护。为了实现上述机制，车联网终端需要以安全的方式存储密码公私钥对、数字证书等敏感参数，目前车联网终端设备的安全参数及安全凭据包括密码公私钥对、CA 系统证书、注册证书、匿名通信证书和应用证书等。

同时车联网终端也需要实现系统隔离机制，以芯片/硬件/固件安全为基础，采用硬件隔离和安全域隔离的方式，将具有高安全要求特征的核心驾驶系统和驾驶辅助应用，与具有低安全要求特征的车载娱乐系统和娱乐应用进行隔离，以保护敏感数据和操作。

随着车联网终端渗透率的不断提升，车联网终端设备的验签处理能力预计在每秒 2000 次左右，目前市场已有的快速验签芯片仅支持 ECC 算法，支持国内 SM2 算法的车规级产品缺失，因此车联网安全芯片存在着相当大的挑战。

验签性能和 SM2 算法不仅是车联网安全芯片普遍面临的问题，在中国需要支持国密等级更是芯片安全首要考虑的问题。在第一阶段建议安全芯片需要达到国密二级等级，即《安全芯片密码检测准则》安全等级的第二级。

（二）车联网相关的安全算法

为了防止数据在车联网内部或外部遭受攻击者非法窃听、篡改、伪造等威胁，车联网系统可采用密码技术对数据在传输、存储、使用的过程中进行加密保护，确保数据的机密性和完整性；建立完善的密钥、证书管理体系，保证密码资源的安全。同时，对车联网数据的访问进行权限控制，防止非授权用户访问。

目前车联网安全主要采用非对称密码算法，国外主要是 ECC NISTP256 和 brainpool,在我国主要使用 SM2、SM3 和 SM4 算法。

随着自动驾驶等车联网业务的不断发展，在空口上传输的消息可能会越来越大，时延越来越低，因此需要减少安全的开销。目前车联网安全使用的是显式证书，安全开销比较大，未来可能会使用隐式证书等新机制来减少空口开销及算力消耗。目前美国使用的生成隐式证书的算法是 ECQV 算法，我国并没有类似的用于车联网隐式证书的算法，这样可能会限制未来车联网应用的发展。

（三）车联网业务管理模式

车联网安全管理系统(即颁发证书的 CA 系统)的架构和部署与车联网的管理模式强相关，不同的管理模式和业务模式会导致完全不同的车联网安全管理系统架构。美国和欧洲的车联网安全管理系统之间的差别就是由美国和欧洲在车联网业务管理模式的不同造成的。

我国车联网安全管理系统的建设部门和管理办法需要尽快明确，以保证车联网安全管理系统的安全性，同时解决不同 CA 系统颁发的证书互认问题。车联网设备的管理机制和管理部门也需要进一步明确，尤其是车载设备如何与现有车辆的全生命周期阶段的监管结合，如何与现有各个行政区划层级下的管理实体结合，目前都没有明确的结论，导致目前车联网安全管理系统的设计和证书管理流程的设计存在较大的不确定性。

在车联网隐私保护方向，如何实现车载设备、手持设备等移动设备的隐私保护，并同时满足政府信息监管的需求，也需要在车联网安全管理系统架构和证书管理机制上进行深入研究和设计。

六、 政策建议

（一）加强车联网安全总体规划部署和顶层设计

车联网安全是车联网产业发展的重要保障，为了加快车联网产业的发展，国家应统筹规划，从国家层面提升对车联网安全的总体规划部署和顶层设计，加强车联网安全监管力度，促进我国车联网安全产业发展。

（二）加快颁布国家车联网安全相关的法律法规和有关政策

建议国家完善车联网安全相关的法律制度。加强车联网安全相关的法律制度研究，在车联网发展的过程中同步考虑已经或可能产生的法律监管问题。出台车联网安全相关的战略政策，从国家层面制定出台车联网安全保障战略、行动计划等，明确车联网安全工作的定位、发展目标和保障措施等。

（三）落实责任，加强协作

明确政府各部门在车联网行业领域的职责划分，按照国家政策规定监督指导相关单位落实车联网安全保护责任。组织、协调行业监管部门、研究机构、车联网企业、安全厂商等共同合作，研究制定车联网安全相关的管理、技术、测评等标准规范。

（四）推进自主关键技术研发

国家、国内相关标准化组织及车联网联盟要加快推进基于我国自主密码体系（国产密码算法）及自主知识产权的车联网安全规范及安全协议标准，加快车联网设备基于国产密码算法安全解决方案设计、车联网设备基于国产密码体系及国际通用标准算法的安全芯片的设计和实现，以及车联网设备基于国产密码算法及国际通用标准算法的通讯安全协议的设计及制定。

参考文献

[1]. 陈山枝、胡金玲等撰写，车联网技术、标准与产业发展态势前沿报告，中国通信学会，2018 年 12 月

[2]. Shanzhi CHEN, Jinling Hu, Yan Shi, and Li Zhao, Vehicle-to-Everything (v2x) Services Supported by LTE-Based Systems and 5G. IEEE Communications Standards Magazine 1(2): 70-76(2017)

[3]. Shanzhi CHEN, Jinling Hu, Yan Shi, and Li Zhao, LTE-V: A TD-LTE based V2X Solution for Future Vehicular Network, IEEE Internet of Things Journal, Vol.3, Issue: 6, p997-1005, December 2016.

[4]. 陈山枝、胡金玲、时岩、赵丽，“LTE-V2X 车联网技术、标准与应用”，电信科学，2018 年 4 月，第 34 卷，第 4 期，pp.1-11。

[5]. LTE-V2X 安全技术白皮书，IMT-2020（5G）推进组，2019.7

[6]. 车联网通信安全与机遇 GBA 的证书配置白皮书，中国移动，2019.9

[7]. 5GAA：Provisioning Simplification Approaches，2018.12

[8]. 5GAA: Overview of (proposed) regional privacy and security regulations and their requirements，2018.12

[9]. 5GAA：Analysis of C-V2X security and privacy requirements and impact on SCMS design，2018.12

[10]. 5GAA：Simplified Architecture Options per Region，2018.12

[11]. 3GPP TS 33.185 Security aspect for LTE support of Vehicle-to-Everything (V2X) services

[12]. 3GPP TR 33.885 Study on security aspects for LTE support of Vehicle-to-Everything (V2X) services

[13]. 3GPP TS 33.401 3GPP System Architecture Evolution (SAE); Security architecture

[14]. European Commission Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) Release 1.1 June 2018

[15]. ETSI TS 102 731 Intelligent Transport Systems (ITS); Security; Security Services and Architecture V1.1.1 2010-09

[16]. ETSI TS 102 940 Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management V1.2.1; 2016.11

[17]. ETSI TS 102 941 Intelligent Transport Systems (ITS); Security; Trust and Privacy Management V1.2.1 2018.5

[18]. IEEE Std 1609.2-2016 IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management

Messages 2016

[19]. SAE J2945/1_201603 On-Board System Requirements for V2V Safety Communications

[20]. U.S Department of Transportation Security Credentials Management System (SCMS) Design and Analysis for the Connected Vehicle System

[21]. 陈正,李博，胡宁，张东伟，高夕冉 “车联网安全问题的研究及应对方法” 北京汽车 2019.1

[22]. 孙航，解瀚光，“王兆智能网联汽车信息安全标准体系建设与产业政策研究” 中国汽车 2018

[23]. 孙智“智能网联汽车网络安全问题综述汽车安全技术” 2019.2

中国通信学会

地址：北京市海淀区万寿路 27 号院 8 号楼

邮政编码：100840

联系电话：010-68209072、68209071

传真：010-68209074

网址：https://www.china-cic.cn/