计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400112

大数据时代下车联网安全加密认证技术研究综述

宋 涛[1,2,3] 李秀华[1,2] 李 辉[1,2] 文俊浩[1,2] 熊庆宇[1,2] 陈 杰[4]
1 信息物理社会可信服务计算教育部重点实验室(重庆大学) 重庆 401331
2 重庆大学大数据与软件学院 重庆 401331
3 中国信息通信研究院 北京 100191
4 重庆市特种设备检测研究院 重庆 401121
(m18716350296@163.com)

摘 要 针对车联网攻击风险的持续加剧,车载系统、车载终端、车载信息与服务应用及智能网联汽车运营服务平台等面临的网络安全威胁凸显,广义网络攻击中的信息篡改、病毒入侵等手段已经被证明可用于对智能网联汽车的攻击。传统车联网的弱口令认证和弱加密的特点,难以满足当前车联网领域多网络、多节点安全防护的要求,国内车联网安全加密认证机制的缺乏和加密认证体系不完善,导致车联网通信安全更难得到满足。为解决车联网安全加密认证问题,文中对大数据时代下的车联网安全加密认证技术架构进行了研究。首先介绍了大数据时代下车联网安全现状和车联网安全的相关概念;接着对比分析了当前车联网的安全架构,并提出了大数据时代下的车联网安全加密认证体系,系统地论述了车联网安全技术架构以及车联网通信模块的加密认证方式;然后将所提架构与车联网信息安全标准进行对比分析,详细阐述了车联网安全加密认证关键技术和技术创新性;最后总结并提出了当前车联网安全加密认证技术面临的问题和挑战。

关键词:车联网安全;安全威胁;网络攻击;安全防护;加密认证
中图法分类号 TP393

Overview of Research on Security Encryption Authentication Technology of IoV in Big Data Era

SONG Tao[1,2,3],LI Xiu-hua[1,2],LI Hui[1,2],WEN Jun-hao[1,2],XIONG Qing-yu[1,2] and CHEN Jie[4]
1 Key Laboratory of Dependable Service Computing in Cyber Physical Society (Chongqing University) Ministry of Education,Chongqing 401331,China
2 School of Big Data & Software Engineering,Chongqing University,Chongqing 401331,China
3 China Academy of Information and Communications Technology,Beijing 100191,China
4 Special Equipment Inspection and Research Institute of Chongqing,Chongqing 401121,China

Abstract With the increasing risks of Internet of vehicles (IoV) attack,the network security threats of vehicle-mounted systems,vehicle-mounted terminals,vehicle-mounted information and service applications,the operation and service platform of intelligent connected vehicles (ICVs) are prominent. Information tampering and virus intrusion in the generalized network attack have been proved to be suitable for the attack of ICVs. The characteristics of weak password authentication and weak encryption in traditional IoV are hard to satisfy the current requirements of multi-network and multi-node security protection in the field of IoV. In addition,the lack of domestic security encryption authentication mechanism and the imperfect encryption authentication system make it more difficult to satisfy the requirements of IoV security. To solve the problem of IoV security encryption authentication,the paper studies IoV security encryption authentication technology in the age of big data. Firstly,this paper introduces the current situation and relevant concepts of IoV security in the era of big data. Then it contrasts and analyzes the current IoV security architecture,and puts forward IoV security encryption authentication system in the era of big data,and elaborates systematically the IoV security technology architecture and the encryption authentication way of IoV communication module. Then the architecture proposed in this paper is compared with the information security standards of the IoV and elaborates key technology and innovations of the IoV security encryption authentication. Finally,the paper summarizes and proposes the problems and challenges faced by the current security encryption authentication technology of IoV.

Keywords Internet of vehicles security,Security threat,Network attack,Security protection,Encryption authentication

到稿日期:2021-04-11 返修日期:2021-07-25
基金项目:国家自然科学基金(61902044,61672117,62072060);国家重点研发计划(2018YFB2100100,2018YFF0214700);重庆市科技计划项目基础科学与前沿技术研究专项(cstc2019jcyj-msxmX0589);重庆重点基金项目(CSTC2017jcyjBX0025,CSTC2019jscx-zdztzxX0031);中央高校基本科研业务费(2020CDJQY-A022)
This work was supported by the National Nature Science Foundation of China(61902044,61672117,62072060),National Key R & D Program of China (2018YFB2100100, 2018YFF0214700), Chongqing Research Program of Basic Research and Frontier Technology (cstc2019jcyj-msxmX0589),Key Research Program of Chongqing Science & Technology Commission(CSTC2017jcyjBX0025,CSTC2019jscx-zdztzxX0031) and Fundamental Research Funds for the Central Universities(2020CDJQY-A022).
通信作者:李秀华(lixiuhua@cqu.edu.cn)

1　引言

近年来，随着汽车制造技术、计算机科学技术、网络通信技术等新一代科学技术的深度融合，汽车逐步向智能化、网联化的方向发展。通过“人-车-路-云”实时互联感知实现车辆智能控制、智能管理、信息服务和智能决策，为人类提供了更安全、高效、节能的出行方式[1]。但随着汽车智能化、网联化程度的不断提高，车联网安全风险和威胁日益凸显，车载系统、车载终端、车载信息与服务应用及智能网联汽车运营服务平台等均面临不同程度的安全威胁，传统的网络信息篡改、病毒入侵等手段已被证明可用于攻击智能网联汽车。例如：2013年 Charlie Miller&Chris Valasek 通过车载 OBD 接口破解了丰田普锐斯汽车[2]；2015 年 1 月，宝马 Connected Drive 智能驾驶系统被发现存在安全漏洞，导致数百万辆车面临被攻击的风险[3]；2015 年 2 月，通用公司搭载的 Onstar 车载系统被黑客入侵并控制；2015 年 7 月，白帽黑客演示了入侵 Uconnect 车载系统的全过程；2016 年 9 月，腾讯科恩实验室对特斯拉 ModelS 进行了远程攻击实验，成功入侵并控制车辆。车联网安全不仅影响着个人和企业安危，还可能造成重大的生命和财产损失，甚至上升为国家公共安全问题。“4.19 讲话”中表示，“安全是发展的前提，发展是安全的保障，安全和发展要同步推进”。智能网联汽车安全已成为车联网产业和智能网联汽车生态圈能否快速健康稳定发展的重要因素。

目前，世界各国高度重视车联网安全发展。2017 年 8 月，美国交通部道路交通安全管理局（NHTSA）发布新版《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[4]，对车辆辅助系统进行网络安全评估；2017 年 8 月，英国政府发布《智能网联汽车网络安全关键原则》；我国于 2017 年 6 月 1 日正式实施《中华人民共和国网络安全法》，明确要求包括车厂、车联网运营商在内的网络运营者须“履行网络安全保护义务，接受政府和社会的监督，承担社会责任”[5]；《中国制造 2025》已经将汽车网络安全列为关键基础问题进行研究，希望通过产学研用管共同努力，推动车联网整体架构、关键共性技术、标准规范、核心产品形成全链条的安全防护体系，助力智能网联汽车与智能交通的深度融合与发展。

长期以来，车厂一直只注重车辆功能安全，依赖 ISO26262 标准为车厂和零部件供应商提供功能安全开发指导，但是仅通过类似车机编码或固定凭证的方式进行认证，无法满足较高的访问控制需求，攻击者仍能通过伪造凭证的方式访问车联网管理平台进行网络攻击[6]。同时，负责车辆控制和数据传输的车载系统、车载终端、车载信息与服务应用及智能网联汽车运营服务平台之间缺乏通信互信，无法保障车-车、车-云等通信场景下的通信安全。虽然车联网被广泛推广与应用，但车企未及时响应车联网安全发展号召，在车联网身份认证和通信加密方面的认识相对薄弱，导致车联网各节点之间存在多种安全问题，具体如下：

（1）缺乏安全认证机制导致的安全问题。随着汽车网联化程度的提高，车辆被攻击的渠道越来越多样化。由于缺乏车联网安全认证机制，车联网容易遭受信息篡改、信号窃取、重放等多种攻击，国内针对车联网安全的研究处于起步阶段，相关法律法规不健全，导致车联网安全事件频频出现。

（2）缺乏统一的车联网管理平台引发的安全问题。在车联网通信过程中，车联网安全通信需依赖可靠的互信环境，但国内尚未建立车联网互信体系，缺乏针对车联网的统一身份认证管理平台，缺乏车联网各节点之间的双向认证。因此，攻击者可通过外部平台非法接入来获取平台内的流动数据，影响车联网各节点之间的通信安全，更严重的是可能会导致车联网多节点瘫痪。

（3）无法保证数据隐私性而导致的安全问题。车联网数据量庞大，数据交互频繁，用户隐私数据多。目前缺乏车联网安全加密认证体系，通信数据很容易被非互信体系下的伪服务、伪信号基站窃取，数据的隐私性难以得到保障，数据容易被窃取和利用。

为解决车联网通信安全问题，建立互信环境下的车联网安全加密认证体系，构建基于主流商密算法的智能网联汽车身份标识和密钥管理平台，实现网络通信的双向认证，保证数据的私密性和完整性[7]。本文提出了一种车联网安全加密认证架构，文中第 2 节详细论述了车联网的网络安全发展历程，以及将传统车联网安全加密认证体系应用于当前车联网安全加密认证时存在的问题；第 3 节对比分析了当前车联网的安全架构，提出了基于大数据时代下的车联网安全加密认证体系架构，分别阐述了架构中各模块的功能，并将该架构中下的技术要求与当前汽车信息安全标准进行了对比分析；第 4 节详细介绍了推动车联网安全加密认证体系建设的关键技术；第 5 节分析了当下车联网网络安全建设所面临的技术挑战；最后总结全文并强调车联网网络安全的发展对国家信息安全建设的重要性。

2　车联网安全概述

车联网源于物联网，是基于车载移动互联网、车际网与车内网，依据约定的数据交互标准与通信协议[8]，在 V2X 之间开展信息交换以及无线通信的系统网络。车联网的发展推动了车辆智能化控制、智能动态信息服务与智能化交通管理的深层融合，也推动了建立一体化网络的进程[9]。

车联网系统架构主要由 3 层构成，分别为感知层、网络层和应用层。感知层主要是利用传感技术感知车辆的状态信息，网络层主要借助无线通信网络与现代智能信息处理技术来实现交通的智能化管理，应用层主要针对交通信息服务的智能决策和车辆的智能化控制[10]。在车联网为车辆、驾乘人员提供智能化服务时，车联网安全问题一直备受关注。本节首先介绍车联网安全的发展历程，然后介绍车联网安全分类与常见的车联网攻击方式。

2.1　车联网的安全发展历程

车联网安全指借助新一代信息和通信技术，实现车内、车与车、车与路、车与人、车与服务平台的全方位网络安全连接[11]。1981 年，本田汽车公司与日本消费电子厂商阿尔派合作，共同研发了第一款陀螺仪车载导航。但是随着网络技术的发展和黑客的盛行，日本汽车频繁发生攻击轮胎压力监测系统、使用广域网攻击车载 LAN 和解析防盗器密钥等恶意事件。对此，日本开始高度重视车联网安全，并开始制订相应的方针和对策，车联网安全也被正式提出。

1999 年，美国联邦通信委员会将 5.9GHz 宽带用于车间通信，标志着美国车联网正式建立。2002－2004 年，美国

开始执行车辆安全计划，该计划同时测试和评估多种无线通信技术是否能够满足行车安全应用的通信需求（主要包括DSRC、2.5G/3G蜂窝网络、蓝牙、IEEE802.11等）[12]。2016年12月，美国交通部发布《联邦机动车安全标准——第150号》，以保障车联网数据安全，防止黑客攻击。

国际上，2020年12月前，来自世界各地的汽车领域专家（汽车制造商、各层供应链、网络安全顾问、研究机构和政府）组建的ISO/SAE 21434标准的联合工作组编写了汽车信息安全标准规范ISO31434协议，为全世界车联网安全的发展奠定了基础[13]。

2017年至今，在国家安全管理局的指导下，由中国汽车技术研究中心牵头编制的《车联网网络安全白皮书》不断更新，为我国车联网安全的发展指明了方向；2020年，由中国汽车工程研究院股份有限公司、国汽（北京）智能网联汽车研究院有限公司和浙江清华长三角研究院联合牵头，发布了《智能网联汽车信息安全评测白皮书》。调查数据显示，2016－2018年我国信息安全市场规模的增速一直维持在20%以上，高速增长[14]。2018年我国信息安全市场规模达到495亿，同比增长20.90%。对比全球网络安全市场7%的复合增速，我国网络安全市场仍然保持着较快的增长[15]，如图1所示。

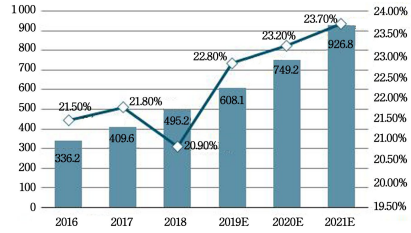

图1 中国网络安全市场及预测数据[15]

Fig. 1 China cyber security market and forecast data[15]

2.2 车联网安全概念

2.2.1 车联网安全分类

车联网信息安全可以分为以下几大类：移动终端APP安全、车载终端安全、云端安全、通信安全和车辆内部安全[16]，如表1所列。

表1 车联网信息安全分类

Table 1 Classification of Internet of vehicles information security

Type	Child class	Instructions
Cloud security	Cloud services and cloud data security	Backend data security based on cloud service and cloud data
Communications security	Wireless Communication Security	Communication security in the process of "mobile phone-backend-vehicle" communication
	Near-field and physical communication security	NFC, Bluetooth, USB, OBD and other communication security
On-board terminal safety	On-board terminal system and APP security	Hu system, Hu APP security
Mobile Terminal Security	Mobile application APP security	Mobile phone terminal and APP application security
Internal safety of vehicle	ECU module, gateway and CANBUS security	Vehicle electronic ECU module, gateway, CANBUS communication security

（1）后台云端安全

车联网服务平台是提供车辆管理与信息服务的云端平台，负责车辆及相关设备信息的汇聚、计算、监控和管理；提供智能交通管控、远程诊断、电子呼叫、道路救援等车辆管理服务，以及天气预报、信息咨询等内容服务[17]，如图2中的红框区域所示。

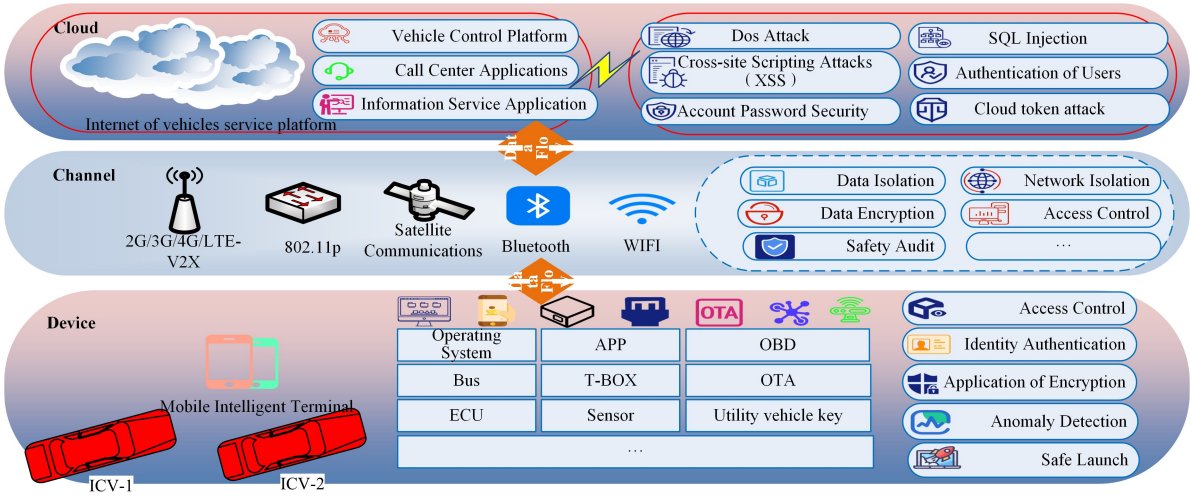

图2 车联网云-管-端安全架构（电子版为彩色）

Fig. 2 Cloud-tube-end security architecture of Internet of vehicles

从图2中可以看出车联网服务平台在车联网架构中的位置，车联网服务平台的作用是通过无线网络为终端设备提供服务。由于车联网平台都是基于云计算技术的，云计算本身的安全问题会被引入到平台中。云计算是一个由多个单一安全域通过轻耦合方式联合而成的逻辑安全域[18]，它所具有的可扩展性、开放性和管理的复杂性使访问控制变得非常繁杂，传统单一安全域中的访问控制模型和机制无法解决多域环境中可能出现的安全威胁，因此云计算的应用面临跨域认证问题、授权问题和应用操作安全问题等。在车联网服务平台层面，平台面临拒绝服务攻击、SQL注入、跨站点脚本攻击、

用户认证鉴权、账户口令安全等风险。

为保障车联网后台服务的稳定性，车联网后台服务大多基于 Linux 操作系统。攻击者通过 Linux 固有漏洞入侵服务器，篡改或非法获取用户信息。

(2)通信安全

车联网通信安全主要有：无线通信安全、近场和物理通信安全。

在无线通信中，移动终端通过车联网平台与车载终端进行信息交互；在信息通信过程中，黑客可以通过伪造基站来截取中间信号，并进行翻译转发，最终达到窃取信息、控制车辆的目的[19]。

在车辆近场通信中，主要使用 WIFI、RFID、蓝牙、红外线、NFC 等进行近程无线通信；在近场通信过程中，黑客可以使用嗅探、中间人攻击、重放攻击等多种方式威胁通信安全，通过非法截取车辆传输数据、逆向解析、寻找数据弱点、执行恶意代码或假冒传入数据来威胁车辆安全，如图 3 所示。

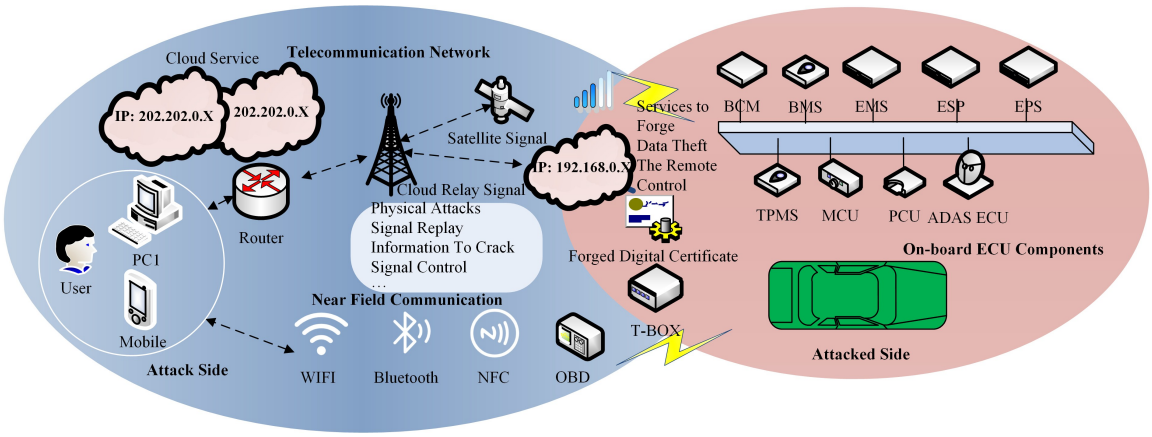

图 3　远、近程攻击示意图

Fig. 3　Schematic diagram of distance and short range attacks

在物理通信过程中，攻击者可通过外接 OBD 接口(车载诊断系统)窃取 T-BOX 中的数据信息、CAN 总线及其他总线报文信息，并发送非法报文信息更改和控制车内的 ECU，威胁驾乘人员的生命安全。

(3)车载终端安全

智能网联汽车车载终端具备数据输入输出、数据计算处理、数据存储、数据通信、ECU 数据采集、控制指令发送等功能，同时也集成了定位、导航、娱乐等多种功能。车载网关、T-BOX、传感器、OTA、车载 OS、车载信息娱乐系统、ECU、OBD-II 接口安全通信的安全威胁主要存在于车内域、V2X 通信域以及基础设施设备域[20]。

车载终端硬件安全主要体现在：车载终端硬件系统使用电路和芯片实现数据运算和数据存储时，可能会遇到密码分析攻击、侧信道攻击、故障注入攻击等破坏数据保密性和完整性的安全威胁[21]，导致数据泄露或被篡改，进而导致芯片运行不稳定。

车载终端操作系统安全主要体现在：通过符合车载端应用场景的身份权限管理和访问控制机制，可对车载操作系统实现溢出攻击、暴力破解、中间人攻击、重放、篡改、伪造等多种安全威胁，无法保证操作系统文件和数据的可用性、保密性和完整性[22]。

车载应用安全主要体现在：车载终端所安装的应用软件可能存在被逆向分析、反编译、篡改、非授权访问等不同的安全风险，导致应用软件在运行时产生的数据或通过相关服务接口提供的数据不能在安全条件下处理。车载终端安全示意图如图 4 所示。

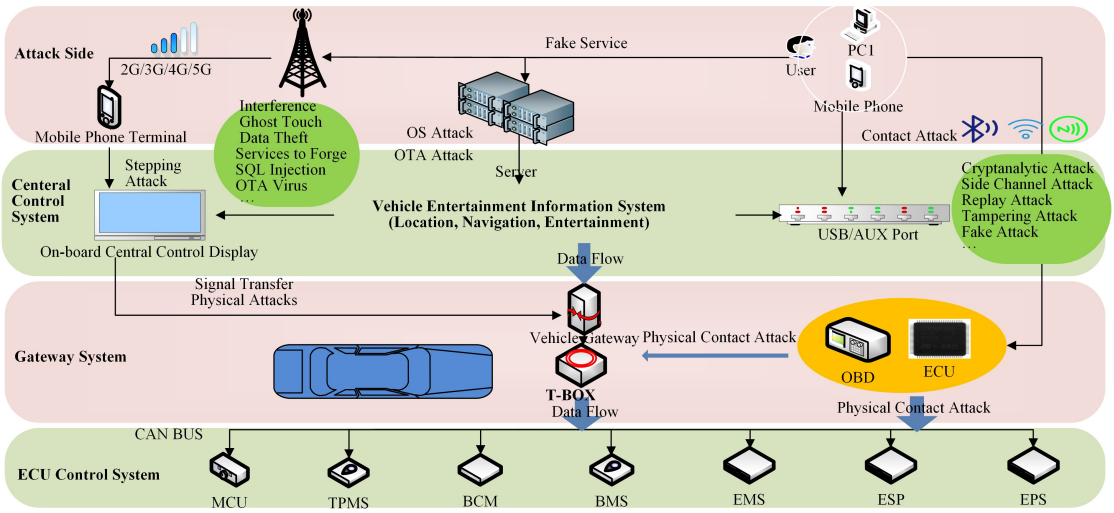

图 4　车载终端安全示意图

Fig. 4　Safety diagram of on-board terminal

(4)移动终端安全

车联网中移动终端以手机设备为主,用于人与车、人与车联网服务平台等的交互,如手机远程解锁、手机远程启动车辆等。手机是人与车之间信息交互的重要媒介,同时也是车联网交互的重要接入口,因此,针对移动终端应用的攻击成为了车辆攻击一个重要源头。移动智能终端接入车内网络时,可作为攻击智能网联汽车的跳板。车载终端上存有的隐私数据,如车联网服务平台账户、密码、认证凭证等信息存在泄漏的风险[23]。攻击者若控制移动智能终端,可进一步获取账户密码,登录服务平台,进而影响汽车安全。攻击示意图如图 5 所示。

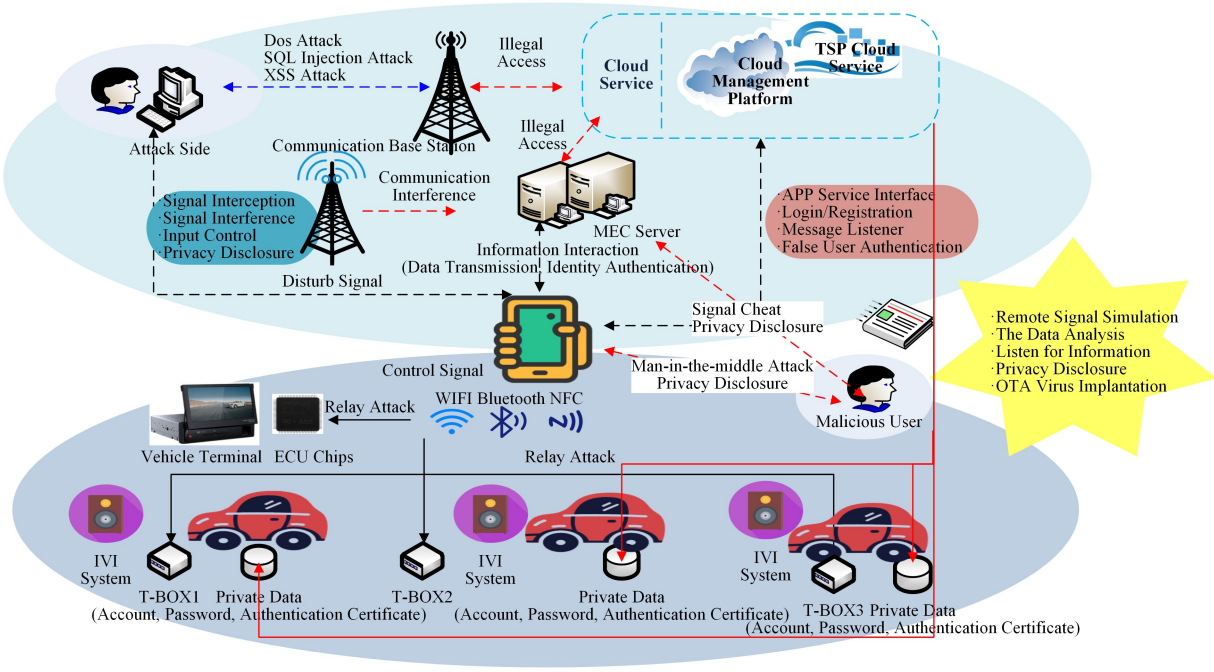

图 5 通过移动终端攻击车载终端示意图

Fig. 5 Schematic diagram of attacking vehicle-mounted terminals through mobile terminals

(5)车辆内部安全

在车辆内部网络通信中,主要通过由 LIN, CAN/CANFD, MOST, FlexRay, Ethernet 等多种总线技术和通信协议组合而搭建的汽车电子网络系统进行信息通信[24]。目前,各大 OEM 厂主要采用 CAN 总线通信方式,它的数据结构、仲裁技术、通信方式能够满足汽车高实时性和轻量化的要求,但 CAN 总线存在一些固有的安全隐患,具体如下:

1)点到线的传播,私密性差

在 CAN 总线通信过程中,报文以广播的形式进行传送,所有 ECU 节点均可接收到总线发送的每一帧消息,如图 6 所示,这种广播方式可能会导致报文被恶意监听,汽车总线数据被恶意捕获分析,最终导致车辆被攻击者控制。

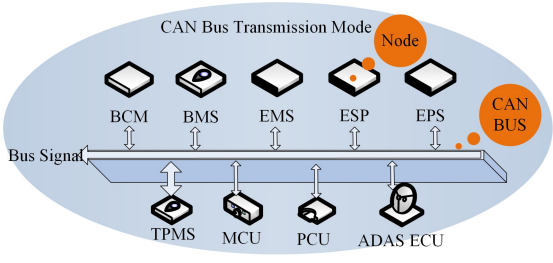

图 6 CAN 总线消息传播方式

Fig. 6 CAN bus message propagation mode

2)传播的消息源不完整

在 CAN 总线通信协议中,总线的每帧数据没有标注原始地址信息,导致接收到的数据的 ECU 无法确认数据的真实性,也无法确认数据是否为原始数据,攻击者一旦注入虚假信息对 CAN 总线报文进行伪造、篡改[25],后果不堪设想。

3)总线的脆弱性

CAN 总线协议是一种基于优先级仲裁机制的协议,这种机制可能会导致总线受到拒绝服务攻击。攻击者可以通过嗅探或监听等手段对汽车总线进行重放或洪泛攻击[26],导致 ECU 无法正常发送和接收报文。

2.2.2 常见的攻击方式

(1)网络嗅探

在车-云通信过程中,车载终端与云端交互会产生大量的用户隐私数据,如车辆行驶轨迹数据、用户身份信息、车辆里程数量等信息,在这些信息的传输过程中可能出现网络嗅探。攻击者可通过分析嗅探的信息获取车载终端的管理员权限,对车内以明文传输的 CAN, LIN 总线进行攻击[27],进而控制车内各 ECU 组件,影响车辆行为。

(2)云服务伪造

由于车-云通信中缺少双方的身份认证,攻击者可伪造云端服务接口向车载终端注入病毒,从而实现对车载操作系统、车机应用、车内 ECU 组件的恶意操作[28]。

(3)信号干扰

云端向车载终端发送信息或指令的过程被攻击者干扰,使得信号不能传送至车载终端。

(4)数据篡改

攻击者篡改车载终端从云端接收的数据,改变消息内容,用假消息代替原始消息,或者将某些额外消息插入其中,从而干扰车辆正常行驶[29]。

(5)拒绝服务

攻击者通过控制车载终端信道，发送大量的非法数据包占领总线资源，导致 ECU 无法提供正常的服务，无法处理正确的数据。

(6)重放

攻击者非法截取信号或消息，然后将其再次发送，从而进行非授权的恶意操作，如重放车钥匙开门信号。

3　车联网安全技术架构

本文第 2 节介绍了车联网攻击的多种类别和方式，在网络攻击手段日益变化的同时，提升车联网的安全防护水平显得尤为重要。车联网安全生态产业须构建贯穿“端-管-云-用”全链条的综合防御体系[30]，才能实现车联网安全的可持续发展。本节将从车联网安全管理体系设计、平台总体架构设计、平台技术架构设计、车载终端和移动智能终端安全通信设计等方面对车联网安全技术架构进行研究，构建了一套可信的车联网身份标识和密钥管理体系，以保证车联网安全。

3.1　车联网安全管理体系架构

车联网发展至今，安全问题层出不穷，但是国内乃至全世界都没有一套完整的可信体系来保障车联网安全。传统车联网安全管理体系架构主要基于 OEM 厂商的安全管理与认证平台，车载终端、移动终端通过 OEM 厂商提供的数字证书进行身份标识和身份认证，从而实现车辆与云端的数据交互。

Yang 等[31]基于数字签名提出车联网安全体系，目的是解决通信各端身份识别问题和复杂通信场景下消息安全传输机制问题，阐述了汽车平台、组件、通信体系，设计了基于全生命周期管理机制的车联网安全架构，提出了面向 LTE-V2X 的数字签名体系，实现了多场景全生命周期内的身份认证服务。安全密钥管理是车联网安全架构的重要组成部分，但文献[31]提出的架构中并无安全密钥管理，因此该架构无法保证基础数据的安全性；在进行终端、云端加密认证时，没有针对所采用的加密算法进行论述，仅针对系统认证过程进行阐述，因此其仍有改进空间。Huang[32]基于匿名认证方式提出了基于区块链的车联网安全技术。虽然区块链具有消息可靠、真实、无法篡改等特性，但是用于区块链认证的密钥以及生成的数字证书的安全性无法得到保障。如果整个密钥颁发体系是由不具备信任的第三方机构颁发，最终可能会导致整套系统信息完全被泄露。Wan 等[33]基于区块链技术提出了车联网安全体系结构的研究思路，综述了区块链技术和车联网层次体系，但是仅谈了区块链技术应用，并未提出完整的车联网体系架构。Wang[34]基于 V2X 安全芯片的 5G 车联网安全，提出建立云-管-端的纵深防御体系，采用基于国密算法的 V2X 安全芯片对车辆数据进行加密和防护，但该架构下未构建基于车联网云平台的安全防御体系，也没有针对密钥的统一管理、销毁、分发等。Chen[35]分析了车联网安全风险与威胁，设计了车联网安全防护体系和统一的安全管理平台，不仅考虑了各层的安全需求和防护措施，还思考了各安全产品功能分散、不能互相协同工作的情况，但是其仅仅探讨了感知层、网络传输层、应用层的网络安全防护问题，未建立车联网终端、云端身份认证和密钥管理安全体系。Li 等[36]总结分析了车联网攻击案例，划分了车联网安全层级，提出了网络级安全、平台级安全、组件级安全防护方案，但文献[36]缺乏针对车联网各节点的身份管理和控制内容的探讨，仅是对面临的威胁和防范措施进行综述性探讨。Gui[37]基于当前车联网的通信需求，提出了车联网安全通信架构及密码应用体系，设计了 V2X 通信协议栈，但是该体系中缺乏证书管理、密钥管理等体系架构的内容。表 2 列出了从方案的类别、技术方法、应用场景、可扩展性等方面对车联网安全管理体系进行对比分析的结果。

表 2　现有车联网安全架构方案比较

Table 2　Comparison of existing IoV security architecture schemes

Research literature	Schemes	Technique methods	Application scenarios	Expandability
[31]	Research on the Security System for Internet of Vehicles based on Digital Signature	1. Iov security system cloud architecture 2. IoV safety system in road 3. IoV security system mobile terminal architecture 4. Vehicle-side architecture of IoV security system 5. LTE-V2X digital signature system	Vehicle-to-Cloud Vehicle-to-Vehicle Vehicle-to-Person Vehicle-to-Infrastructrure In-car communication	High
[32]	IoV Security Technology based on Anonymous Authentication	1. Digital Certificate Certification Center 2. Authorization center 3. Blockchain	Vehicle-to-Vehicle Vehicle-to-Infrastructrure	Low
[33]	Research on IoV Security Architecture Based on Blockchain Technology	1. IoV security system based on block-chain technology	Vehicle-to-Vehicle Vehicle-to-Infrastructrure	Low
[34]	Research on 5G Internet of Vehicles Security Based on V2X HSM	1. Defensive system in depth 2. V2X security chip based on domestic commercial password algorithm	Vehicle-to-Vehicle Vehicle-to-Infrastructrure	Low
[35]	Analysis and Design on Security Protection System of Vehicle Network	1. Unified security management platform in Awareness layer, Network transmission layer, Application service layer, Secu-rity management layer	Vehicle-to-Cloud Vehicle-to-Vehicle Vehicle-to-Person Vehicle-to-Infrastructrure	Middle
[36]	Survey of Internet of Vehicles Security	1. Network level security 2. Platform level security 3. Component level security	Vehicle-to-Cloud In-car communication	Low
[37]	Research of Cryptography Application Technology in Security Communication of Internet of Vehicles	1. V2X secure communication protocol stack 2. IoV security communication system	Vehicle-to-Cloud Vehicle-to-Vehicle Vehicle-to-Infrastructrure	Middle

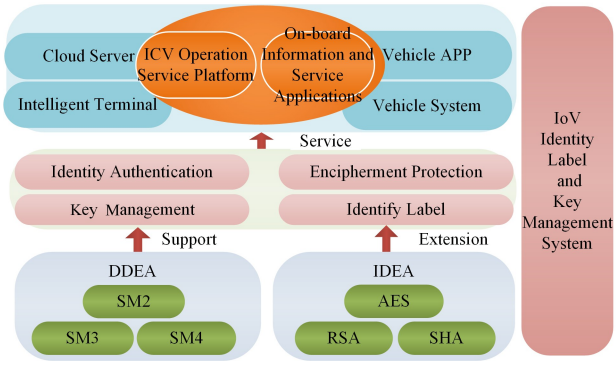

图 7 车联网身份认证标识和密钥管理体系

Fig. 7 IoV identity authentication identification and key management system

基于文献分析，本节提出了一套车联网身份标识和密钥管理体系，用于支撑智能网联汽车与车联网服务平台安全通信、智能网联汽车之间的安全通信、智能网联汽车与智能终端安全通信。通过建立车联网身份标识和密钥管理体系，可以为车联网内的信息传递提供合规、合理、安全的通信机制，车联网身份标识与密钥管理体系架构如图 7 所示。

本体系基于国家商用密码管理体系，支持多种国密算法，同时支持扩展 AES，RSA 等国际标准密码算法[38]。借助密码体系的支撑，建立身份标识、加密保护、密钥管理、身份认证 4 块基础设施，为智能网联汽车运营服务平台、车载信息与服务应用、云平台等提供身份认证与加解密的服务，并将本体系辐射到车载应用、智能终端、车载系统、云端服务等终端设备，以此推进国家汽车电子网络安全相关标准的制定与应用，实现车联网安全的发展。

3.2 车联网安全平台架构设计

车联网身份标识和密钥管理服务平台由云平台端、车载端和移动端 3 部分组成，形成一体化的身份认证和加密保护方案，充分发挥了国家商密算法在保障智能网联汽车网络安全中的作用。

系统总体架构如图 8 所示。

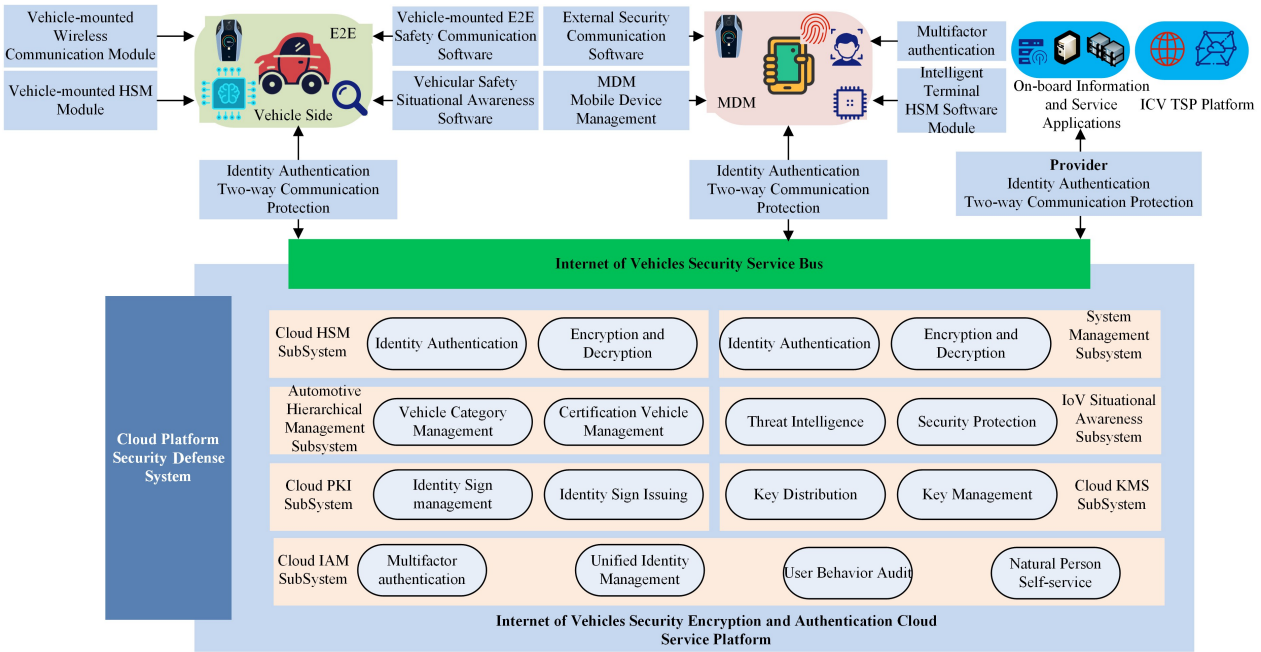

图 8 系统总体架构图

Fig. 8 Overall architecture diagram of system

(1)云端

云端即车联网安全加密及认证云服务平台，该平台由用户证书管理的云 PKI 子系统、用于密钥管理的云 KMS 子系统、用于身份管理与访问控制的云 IAM 子系统、用于保证云端硬件安全的云 HSM 子系统、汽车分级管理子系统、车联网态势感知子系统、系统管理子系统以及车联网安全服务总线组成。云端将面向智能网联汽车、自然人以及车厂、第三方云服务平台，并为这些平台提供身份标识管理、密钥管理等服务，建立“人-车-云”的可信体系[39]。

(2)车载端

车载端组件由车载无线通信模块安全软件、车载 HSM 模块、车载 E2E 安全通信软件、车载安全态势感知软件组成。车载端组件用于确保智能网联汽车的车载系统、车载终端拥有唯一的身份标识，并在内部和外部通信时提供安全加密保护。

(3)智能终端

智能终端组件由对外安全通信软件、智能终端 HSM 软件模块、多因子认证模块、移动设备管理软件组成。智能终端组件为智能终端和移动设备提供安全可靠、快捷易用的身份认证和加密保护的服务，以确保智能终端在与云端及车端通信时的安全性和可靠性[40]。

3.3 车联网认证云平台架构设计

车联网认证云平台架构采用市场主流的互联网架构进行设计，平台划分为负载均衡层、应用层、缓存层和持久化层 4 层，每一层都采用高可用构架，具备良好的横向可扩展

能力，采用独立于中间件平台、数据库平台的开发技术，避免单点故障，保障服务系统的持续性。云平台架构如图 9 所示。

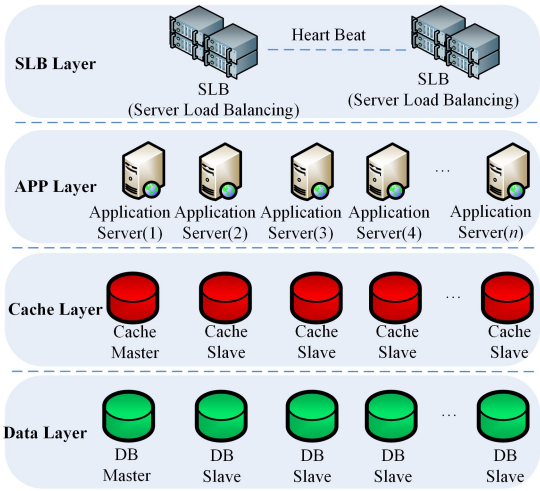

图 9　车联网认证云平台架构图

Fig. 9　Architecture diagram of Internet of vehicles authentication cloud platform

车联网认证云平台支持主流的关系型数据库、中间件及硬件平台，并提供了渠道一致的标准认证服务。车联网认证云平台的前端采用 B/S 架构，后台服务采用 NGINX 实现负载均衡[41]，在 NGINX 达到性能瓶颈后，可利用 DNS 多 IP 解析将请求均匀分配到多组 NGINX 高可用节点上。车联网认证云平台架构设计的特点如下。

(1)分布式部署设计

车联网认证云平台支持应用和数据的集中式处理，同时支持数据集中、应用分散的分布式部署架构。分散的节点可以采用物理机、虚拟机、云平台等多种方式部署，以满足实际环境的要求，可以搭建在 OEM 厂，并为 OEM 厂提供服务，实现 OEM 厂对汽车用户的自主可控。

(2)平台高可用扩展

车联网认证云平台支持垂直扩展和水平扩展，垂直扩展可通过服务器硬件升级获得更好的性能，水平扩展可通过添加服务器来获得更好的性能。

(3)身份认证扩容

车联网认证云平台应用层按照架构划分，涉及 3 个核心层，即负载均衡层[42]、Web 应用服务及 REST API 层和微服务集群层。系统提供统一的身份认证服务，用户认证请求首先到达负载均衡层，然后由应用服务层依次调用身份验证、安全策略判断和多因子认证微服务来处理请求，并将执行结果返回给用户。统一身份认证服务承载每一次用户对应用系统的请求，因此当用户量及应用数量增长时，必须进行服务扩容。

负载均衡将对身份认证的请求负载分摊到不同的服务单元，既保证服务的可用性，又保证响应效率。车联网认证云平台负载均衡层采用 NGINX 服务器，当用户请求量上升，NGINX 达到性能瓶颈时，可以增加 NGINX 高可用组，同时可以利用 DNS 多 IP 解析将请求均匀分配到多组 NGINX 高可用节点上[43]。

(4)身份管理服务扩容

车联网认证云平台提供集中身份管理服务，用户认证请求首先到达负载均衡层，然后请求被分配给管理平台应用服务 REST API[44]，最后由应用服务层按需调用身份管理、权限管理、应用管理和身份源对接等微服务来处理请求，并将执行结果返回给用户。集中身份管理服务主要由 IT 身份管理员、IT 业务应用系统管理员、IT 维护人员等使用。当用户量及应用数量增长时，首要考虑用户身份库扩容的问题，然后按需考虑应用层扩容问题。

集中身份管理服务的车联网认证云平台可拆解为身份管理、权限管理、应用管理、应用账户同步和身份源对接等微服务，这些微服务依次处理如下逻辑：1)管理用户身份和组织机构信息，存入用户身份库；2)管理权限及存储；3)管理应用系统单点登录接入配置；4)管理应用账户同步策略，即用户身份信息到应用系统账户信息的映射规则，并将同步推送应用账户；5)身份源接入配置。业务场景的不同使得每个微服务的访问情况不同，因此可以根据使用情况对各个微服务进行水平扩展。

(5)缓存服务扩容

车联网认证云平台使用 Redis 集群提供缓存服务，对访问 session、页面处理表单以及业务逻辑中间数据做缓存处理。Redis 集群在承受高并发访问压力的同时，还需要通过数据分片技术来实现从海量数据中查询出满足条件的数据，并做出快速响应。

3.4　车载终端安全通信设计

车联网车载终端 T-BOX 作为智能汽车实现网络互联和车辆智能控制的核心部件，是车联网的底层硬件入口以及数据交互、传输的关键载体。T-BOX 融合了无线通信、汽车数据采集与传输、安全引导、CAN 通信加密等多项技术，连接了汽车、云端及智能终端，能够实现丰富的车联网应用功能和 CAN 网络入侵检测功能[45]，如图 10 所示。

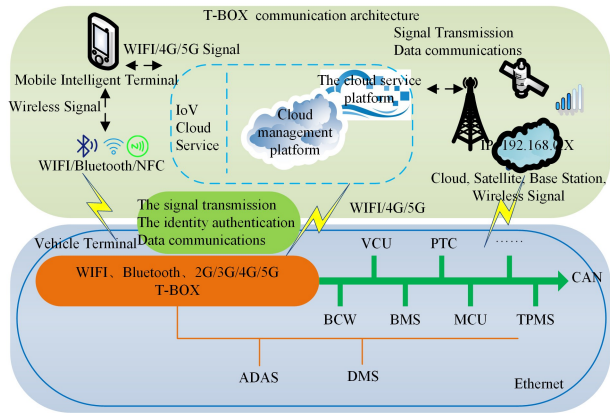

图 10　T-BOX 通信结构

Fig. 10　T-box communication architecture

(1)车载终端(T-BOX)硬件安全设计

车载无线通信模块的硬件安全设计主要包括加密加速和

系统引导前验证两方面。由于车载系统对实时性的严苛要求，因此适配加密算法的加速硬件能节省大量 CPU 开销，提高加密效率。另一方面，安全软件不能保证 T-BOX 在系统未上电前的数据安全，因此必须设计专用硬件设备来解决上电前的数据安全问题，使得在 T-BOX 系统引导之前完成片内数据的完整性验证，保证片内数据的安全。综上所述，为了实现软硬结合的最佳车载无线通信模块的安全，本文针对性地增加了两大专用模块。

1)加密加速专用硬件 CAAM 模块

选用包含加密加速和保证模块（Cryptographic Acceleration and Assurance Module，CAAM）的专用芯片，来提供加密算法加速、加速加密数据导入与导出、专职片上（运行时）和片外存储保护等功能的支持，为国密算法的加速提供硬件基础。

2)T-box 系统数据完整性保护专用硬件 TPM 模块

应用 TPM 模块来保护 T-box 片内数据的完整性[46]。该硬件模块可在 T-box 操作系统引导启动前对片内数据的完整性进行校验，保证 T-box 的核心系统数据不会在系统加载前被篡改。TPM 硬件模块的主要任务为：提供基于硬件的可信根，保证数据的完整性和系统的初始可信性。

(2)车载终端(T-BOX)软件安全设计

车联网在构建信息化交通网络环境时，须在车载智能终端部署多个无线通信接口，以实现 WiFi、蓝牙等多种网络信号的接入，但是这些部署的通信接口成为了被攻击的对象，攻击者可以通过破解 WiFi 或蓝牙认证口令来接入汽车内部网络[47]，从而窃取汽车内部总线上的数据信息或对车载内部网络实施渗透攻击。

为了增强无线网络的安全性，必须为无线网络通信提供认证和加密安全机制。关于 T-BOX 通信的安全设计示意图如图 11 所示，针对两种机制的解释如下。

1)认证机制

认证机制用于对用户的身份进行验证，以限定特定的用户（授权的用户）可以使用网络资源。

2)加密机制

加密机制用于对无线链路的数据进行加密，保证无线网络数据只被所期望的用户接收和理解[48]。

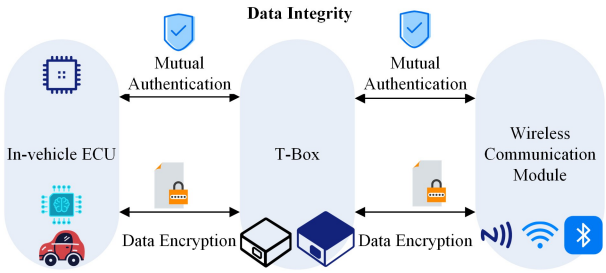

图 11 T-BOX 软件安全加密设计图

Fig. 11 Diagram of T-Box software security encryption design

(3)身份认证方案

车联网身份认证管理平台应向系统中的用户提供身份认证方案、策略和证书服务部署工作，并维护根 CA 服务器。应用提供商须向身份认证管理平台备案，获取身份认证服务，维护应用服务器，管理自己应用下的用户。T-BOX 管理商须向身份认证管理平台备案，获取身份认证服务，维护 T-BOX 管理服务器，管理其下 T-BOX，认证方案如图 12 所示。

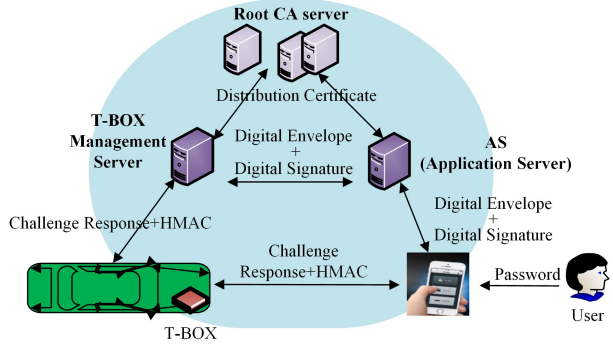

图 12 T-BOX 身份认证方案

Fig. 12 T-Box authentication scheme

3.5 智能移动终端安全通信设计

智能移动终端与云端通信时，黑客可能会通过伪造云服务给智能移动终端发送恶意指令，从而威胁车主的生命安全；也可能会伪造车载终端与智能移动终端连接，窃取移动终端存储的大量数据信息。为了避免身份认证协议因自身存在的漏洞而导致认证失效，需要在双方进行数据交互之前对双方身份进行认证。智能移动终端的身份认证包括智能移动终端与车辆的双向身份认证和智能移动终端与云端的身份认证，如图 13 所示。

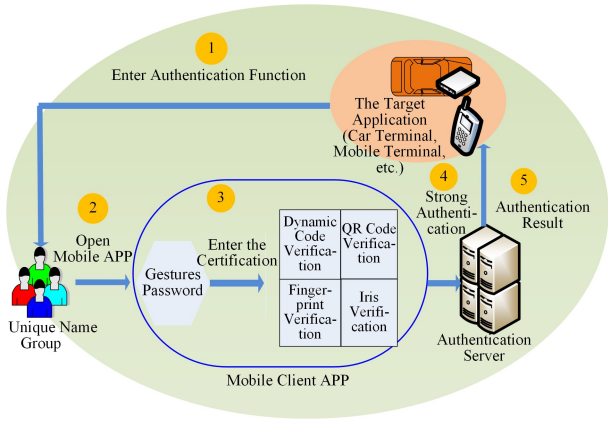

图 13 移动客户端认证架构图

Fig. 13 Diagram of mobile client authentication architecture

3.6 对比汽车信息安全标准

通过以上架构方案的设计，构建了一套全方位的车联网安全加密认证体系，可满足车-云、车-车、车-人、车-路基设备等场景下的安全通信。本节将上文所述架构方案与车联网国标安全体系进行对比分析，以此验证架构方案的合理性。表3列出了国家车联网信息安全标准体系的技术要求[49]与本文方案的对比分析结果，最终得出本文方案符合国家车联网安全标准这一结论。

表3　汽车信息安全标准对比

Table 3　Contrast with automotive information safety standards

Technical Requirement(True/False)		Automotive information security standards	Scheme in this paper
IoV server security protection	Identity authentication(True/False)	True	True
	Access control (True/False)	True	True
	Security audit (True/False)	True	True
	Resource control(True/False)	True	True
	Malicious code prevention (True/False)	True	True
Data security protection	Access control (True/False)	True	True
	Security audit (True/False)	True	True
	Malicious code prevention (True/False)	True	True
Network security protection	Network topology(True/False)	True	True
	Access control(True/False)	True	True
	Security audit(True/False)	True	True
	Malicious code prevention(True/False)	True	True
	Network equipment protection(True/False)	True	True
	Network security monitoring(True/False)	True	True
Platform safety protection	Identity authentication(True/False)	True	True
	Access control(True/False)	True	True
	Security audit(True/False)	True	True
	Open interface security(True/False)	True	True
Apply service security protection	Identity authentication(True/False)	True	True
	Access control(True/False)	True	True
	Security audit(True/False)	True	True
	Resource control(True/False)	True	True
Others	IAM(True/False)	False	True
	CAN-Bus security protection(True/False)	False	True

4　关键技术与创新性

近年来，汽车的智能化、网联化发展提升了用户体验，但智能联网汽车遭受的安全攻击不断变化、升级，面临的威胁日渐严重。对智能网联汽车实施安全风险管控，建立适应车联网环境的身份识别和密钥管理体系，已成为目前亟待解决的关键问题。车联网安全加密认证体系架构的建立离不开关键技术的支撑，本节将详细讨论车联网安全加密认证体系架构中涉及的关键技术，具体包括：身份标识和密钥管理一体化技术，多维认证、态势感知技术，基于分布式、高可用、高并发的统一认证技术，国密算法应用技术以及多因子认证技术。

4.1　关键技术

4.1.1　身份标识密码技术

身份标识密码技术基于身份标识的密码系统，是一种非对称的公钥密码体系，其概念由 Shamir 于 1984 年提出[50]。标识密码系统与传统公钥密码一样，每个用户有一对相关联的公钥和私钥。标识密码系统中，将用户的身份标识如姓名、IP 地址、电子邮箱地址、手机号码等作为公钥，通过数学方式生成与之对应的用户私钥。用户标识就是该用户的公钥，不需要额外生成和存储，只需通过某种方式公开发布，私钥则由用户秘密保存。IBC 密码体系标准主要表现为 IBE 加解密算法组、IBS 签名算法组和 IBKA 身份认证协议。

标识密码是一种基于双线性配对和椭圆曲线的公钥密码技术，由传统的 PKI 发展而来，主要解决的问题集中在身份认证、抗否认、完整性、保密性等方面，为实现应用安全提供了保障。标识密码可以应用于以下几个方向：安全电子邮件服务、安全电子政务应用、企业安全应用、安全中间件、服务端设备、安全终端设备等。

4.1.2　密钥管理技术

密钥管理指对密钥进行管理的行为，如加密、解密、破解。密钥管理主要表现在管理体制、管理协议和密钥的产生、分配、更换和注入等。密钥管理技术分为对称密钥管理和非对称密钥管理，具体描述如下。

(1)对称密钥管理

对称加密指采用对称加密技术的贸易双方必须保证采用的是相同的密钥，保证彼此密钥的交换是安全可靠的，同时还需要设定防止密钥泄密和更改密钥的程序。通过公开密钥加密技术实现对称密钥的管理使相应的管理变得简单和安全，同时还解决了纯对称密钥模式中存在的可靠性问题和鉴别问题。双方可以为每次交换的信息(如每次的 EDI 交换)生成唯一一把对称密钥并用公开密钥对该密钥进行加密，然后将加密后的密钥和用该密钥加密的信息(如 EDI 交换)一起发送给相应的贸易方。由于每次信息交换都对应生成了唯一一把密钥，因此各贸易方就不再需要对密钥进行维护，且不用担心密钥被泄露或过期。这种方式的另一优点是，即使泄露了一把密钥，也只将影响一笔交易，而不会影响到贸易双方所有的交易关系。

(2)非对称密钥管理

非对称密钥管理也称为公开密钥管理/数字证书，贸易双方可以使用数字证书来交换公开密钥。数字证书通常包含唯一标识证书所有者(即贸易方)的名称、唯一标识证书发布者的名称、证书所有者的公开密钥、证书发布者的数字签名、证书的有效期及证书的序列号等。证书发布者一般被称为证书管理机构(CA)，它是贸易各方都信赖的机构。数字证书能够起到标识贸易方的作用，是目前电子商务广泛采用的技术

之一。这种加密认证方式可作为车联网平台与终端设备之间的安全认证方式，可很好地保证汽车厂商与车载终端用户的数据安全。

4.1.3 多维认证、态势感知技术

(1)多维认证

多维认证技术是基于安全加密及认证服务云平台实现“人-车-云”三维一体的认证技术。多维认证技术包含 PKI 认证体系、全局身份管理与访问控制和“人-车-云”三维一体认证等功能，提供了多维联合认证服务，实现了差异化的安全防护。

1)PKI 认证

专门负责颁发数字证书的系统称为 CA 系统，负责管理并运营 CA 系统的机构称为 CA 中心。CA 中心管理并运营 CA 系统，CA 系统负责颁发数字证书。该系统的主要功能是绑定证书持有者的身份和相关的密钥对(通过为公钥及相关的用户身份信息签发数字证书)，为用户提供方便的证书申请、证书作废、证书获取、证书状态查询的途径，并利用数字证书及各种相关的服务(证书发布、黑名单发布、时间戳服务等)实现通信中各实体的身份认证、完整性、抗抵赖性和保密性。

2)全局身份管理与访问控制

身份管理与访问控制系统(IAM 子系统)改变了原有分散的、以车厂为中心的认证方式，采用以用户(自然人及智能网联汽车)为中心的统一平台，使原有以系统账户为中心的管理方式上升为以自然人用户及智能网联汽车为中心的统一身份管理方式，让每一个自然人用户和智能网联汽车只有一个唯一的身份，提供对此身份进行完整的生命周期管理、属性管理、身份信息管理等功能。

3)“人-车-云”三维一体认证

三维一体认证体系指采用“人-车-云”3 种身份识别和认证方式进行用户身份校验，以保障认证结果的可靠性。该体系不仅支持传统的 RSA 令牌、CA 认证、USB 指纹、虹膜等生物识别以及 SMS、邮件一次性口令，还支持手机安全令认证，借助移动客户端可实现二维码扫描、动态口令、指纹、声纹及脸纹等生物识别技术。

(2)安全态势感知

安全态势感知技术主要采用基于终端的身份认证与加解密异常日志分析、基于 AI 的入侵检测分析、云端通信异常行为分析、近距离通信异常行为分析和异常行为分析等技术，实现了对车辆异常行为的风险监测的态势感知。

4.1.4 基于分布式系统、高可用、高并发的统一认证技术

分布式系统指拥有多种通用的物理和逻辑资源，可以动态分配任务，使分散的物理和逻辑资源通过计算机网络实现信息交换，且系统中存在一个以全局的方式管理计算机资源的分布式操作系统[51]。分布式系统的主要优点有：资源共享、加速计算、高可靠性和快捷通信。

高可用技术指通过缩短日常维护操作(计划)和突发的系统崩溃(非计划)导致的停机时间，以提高系统和应用的高度可用性[52]。该技术主要通过高可用性的软件将冗余的高可用性的硬件组件和软件组件组合，各个主机系统通过网络或其他手段有机地组成集群，共同对外提供服务，目的是消除单点故障。

高并发技术指在同一个时间点，大量用户同时访问同一 API 接口或者 Url 地址[53]。在这种场景下，如果不进行并发处理，则很容易导致接口返回数据异常或服务器崩溃。目前，提高系统并发能力的方式主要有两种：垂直扩展和水平扩展。垂直扩展可通过升级服务器硬件来获得更好的性能，水平扩展可以通过添加服务器来获得更好的性能。垂直扩展的方式为：升级 CPU、扩展内存、提高磁盘转速/使用固态硬盘、切换到存储区域网络(SAN)。水平扩展的方式为：通过程序或者中间件让应用程序达到只需要增加普通的 X86 服务器就可以使能够支撑的用户访问量呈线性增长。通过水平扩展数据库、应用服务器统一身份管理和访问控制可支持百万甚至千万级别的用户量。

4.1.5 国密算法应用

国密即国家密码局认定的国产密码算法，其中包括对称加密算法、椭圆曲线非对称加密算法、杂凑算法，具体包括 SM1，SM2，SM3，SM4 等。国密算法适用于嵌入式、物联网等相关领域，以完成身份认证和数据加解密等功能。

SM1：对称加密算法。该算法的加密强度与 AES 相当。该算法不公开，调用该算法时，需要通过加密芯片的接口进行调用。在门禁应用中，采用 SM1 算法进行身份鉴别和数据加密通信，实现卡片合法性的验证，保证身份识别的真实性。

SM2：非对称加密算法。该算法基于椭圆曲线加密算法(ECC)，已公开，其签名速度与秘钥生成速度都快于 RSA，ECC 256 的安全强度高于 RSA 2048。

SM3：消息摘要算法。SM3 算法广泛应用于数字签名、消息认证、数据完整性检测等领域。该算法是基于 SHA-256 算法改进而来的，其采用 Merkle-Damgard 结构，消息分组长度为 512 位，摘要值长度为 256 位。

SM4：无线局域网标准的分组数据算法。该算法对称加密，密钥长度和分组长度均为 128 位，主要是为了加密保护静态储存和传输信道中的数据。

4.1.6 多因子认证技术

多因子认证(MFA)是一种计算机访问控制方法，用户需要通过两种以上的认证方式才可以使用相关资源，采用多因子认证技术可以大大提高账号的安全性。

最常用的多因子认证是结合静态密码和动态密码的认证方式。

(1)静态密码

静态密码即由用户输入用户名和密码，因为用户设定的密码不会随意改变，相对来说是静止不变的，所以称为静态密码。静态密码依据用户已知的信息进行认证，是最普遍的身份认证方式。

为保证安全性，对静态密码的要求如下。

1)长度要求：8 位以上。

2)复杂度要求：大写字母、小写字母、数字、特殊字符，至少 3 种以上的组合。

3）定期更换要求：最多 90 天要更换密码。

4）重用限制要求：修改密码时不能与近期使用过的 5 个密码相同。

（2）动态密码

动态密码（One-time Password，OTP）根据一定的算法生成随机字符组合，通常为 6 位数字。主流的动态密码有短信密码、硬件令牌、手机令牌。动态密码是一种安全便捷的认证方式，用户无须定期修改密码，安全省心。目前常用的动态密码的认证方式如下。

1）短信密码

短信密码通常也叫短信验证码，是由认证服务生成 6 位随机动态密码，并以短信的方式发送到用户的手机上，用户使用此动态验证码进行身份认证。

2）硬件令牌

基于时间同步的硬件令牌应用广泛，它每 30～60 s 变换一次动态口令，无须与服务器通信。

3）手机令牌

手机令牌同硬件令牌类似，使用手机 APP 来生成和显示动态密码。

4.2　创新性

相比传统的网络安全技术，车联网的安全加密和认证技术具有安全性要求更高、网络稳定性更差、通信场景更复杂、认证需求更频繁等特点。

为了解决车联网身份标识和密钥管理一体化、一站式问题，针对车联网的安全防护需求，本文设计了覆盖车联网中车辆、服务平台、智能终端、路侧设施等场景的安全加密及认证体系，该体系可为智能网联汽车及车联网生态的发展保驾护航；设计了车联网安全加密及认证服务云平台，平台具有 PKI 体系、全局身份管理与访问控制和“人-车-云”三维一体认证等功能，并通过大数据、云计算等技术手段，为车联网网络安全提供态势感知服务；解决了适配车车通信、车管通信、车智通信、车内通信等多元化加密认证场景的问题。该架构支持符合国家标准商密算法以及国际标准加密算法，便于推广应用。通过非对称与对称加密算法的结合，制定了车内 E2E 通信安全机制，为车辆提供内外双重安全保护。

本文提出的车联网加密认证平台采用分布式系统部署方式，结合高可用、高并发技术，支持应用和数据集中式处理，支持数据集中、应用适当分散的分布式部署架构。分散的节点可以采用物理机、虚拟机、云平台等多种方式的部署，满足实际环境的要求，同时提供了同城灾备和异地灾备等不同的部署模式。分散的节点可以搭建在车厂，并为车厂提供服务，由车厂自行管理各自的自然人用户、汽车用户。当出现突发情况时，多个节点可以分担其他问题节点的访问请求，实现自动负载均衡、高可靠访问、服务动态分配以及系统横向和纵向的动态扩展。

5　车联网安全面临的问题与挑战

随着智能网联汽车技术的发展和产品的广泛应用，其在驾驶辅助系统、V2X 应用方面影响着驾乘人员的安全性和舒适性，因此在智能网联汽车行业内建立统一的身份认证和统一的证书、密码管理体系对车联网安全的推广和发展非常有利。我国拥有全球最大的智能网联汽车市场，汽车智能化技术已广泛应用于多种车型，人们已经意识到智能网联汽车安全的重要性。我国智能网联汽车近年来发展迅速，但仍然处于起步阶段[54]。虽然各 OEM 厂和研究机构加强了自主创新投入和技术研究，但是在身份认证与密码体系建设方面与国际领先水平仍有明显差距，且国内缺乏健全的技术研发体系，创新能力和技术突破能力不足，也没有将国家标准的密码体系与认证体系应用于智能网联汽车的经验。

智能网联汽车相关标准和安全认证体系的研究面临着巨大挑战。首先车联网安全认证体系和标准的建立需要立足我国国情，符合我国密码标准体系与身份认证体系的规定，其次需要对国际车联网安全态势、身份认证标准、密码体系、风险现状、市场分析等进行深入研究，最后对比分析各类身份认证技术、密码体系技术及产品的适用性，从而确定适合我国智能网联汽车安全体系建设的方案。

结束语　随着 5G 商业化及大数据、人工智能的发展，国内车联网产业结构日益丰富。在汽车电动化、网联化、智能化、共享化的浪潮下，车联网发展呈现出了前所未有的崭新态势，同时也为车联网的安全防护带来了新的挑战。在车联网多网融合通信过程中，不仅要满足车联网业务的可靠性，还需要保障车联网通信的安全性。在面临新型安全威胁和挑战时，国内各安全公司、主机厂、运营商应协同合作构建车联网主动安全防护体系，搭建可信身份认证平台，对智能网联汽车和车主进行实名认证，同时加强通信数据安全和车主隐私数据保护。通过建立车联网安全加密认证体系，来促进车联网安全行业标准的制定和技术创新，增强车联网安全防御水平，提升车联网自适应防御能力，推动我国车联网安全发展。

参 考 文 献

[1] WANG Y H. Research on the Authentication Technology and Algorithm for Internet of Vehicles[D]. Chongqing: Chongqing University of Posts and Telecommunications, 2017.

[2] YE P, HAO T L, ZHAO D H, et al. Research on the Information Security Technology of Car Networking from the Perspective of Automobile Enterprise[J]. Journal of Automobile Technology, 2019(5): 59-63.

[3] LIU X L. Research on OBU-based Multilevel Security Architecture and Communication Scheme for Internet of Vehicles[D]. Zhenjiang: Jiangsu University, 2018.

[4] China Institute of Communications. Internet of Vehicles Security Technology and Standards Development Frontier Report (2019)[EB/OL]. https://www.docin.com/p-363483387.html.

[5] China Academy of Information and Communications Technology. White Paper on Internet of Vehicles Network Security (2018)[R/OL]. [2018-05-20]. https://max.book118.com/html/2018/1224/6004040055001241.shtm.

[6] China Academy of Information and Communications Technology. White Paper on Internet of Vehicles Network Security (2017)[R/OL]. [2017-09-21]. http://www.caict.ac.cn/kxyj/qwfb/bps/202001/t20200102_273007.htm.

[7] ZHAO X B. Research on Network Security and Standardization of Connected Vehicles[J]. Network Security Technology and Application, 2020, 229(1): 141-142.

[8] YANG N, KANG R B. Network of Vehicles Security Threat Analysis and Protection Ideas[J]. Communications Technology, 2015, 48(12): 1421-1426.

[9] WANG C Q. Network of Vehicles Security Threat Analysis and Protection Ideas[J]. Computer Products & Circulation, 2020 (2): 132-135.

[10] HUANG Y X. Research on Internet of Vehicles Network Security Technology [J]. Electronic World, 2018, 553(19): 51-52.

[11] YUAN K. Research on Routing Algorithm of Vehicle Network in Urban Environment [D]. Chongqing: Chongqing University of Posts and Telecommunications, 2019.

[12] National Technical Committee on Information Security of Standardization Administration. Technical requirements and test evaluation method of network intrusion detection system: GB/T20275-2013[S]. Beijing: Standards Press of China, 2013.

[13] XIE K L, LU Y. Discussion on Current Situation and Development Trend of Information Security of Vehicle Network System [C]// Proceedings of the 14th Henan Province Automotive Engineering Science and Techno-logy Symposium. 2017.

[14] LI X L. Strategy Research of Private Equity Fund Participating in Private Placement [D]. Wuhan: Hubei University of Technology, 2020.

[15] Channel industry. China's information security market development pattern and the information security market development demand trend analysis (2019)[OL]. [2019-11-01]. https://www.chyxx.com/industry/201911/800523.html.

[16] XIE K L, LU Y. Brief Discussion on the Current Situation and Development Trend of Information Security of Internet of Vehicles System[C]// Proceedings of the 14th Henan Provincial Symposium on Automotive Engineering Science and Technology. 2017: 7-8.

[17] GB/T 25066-2010. Information Security Product Category and Code[S]. Beijing: Standards Press of China, 2010.

[18] WANG Q. Research on Safety Mechanism and Key Technology of Internet of Vehicles[D]. Nanjing: Nanjing University of Science and Technology, 2016.

[19] FENG T. Research on Information Security in Internet of Vehicles Technology[J]. Information Security and Technology, 2011 (8): 28-30.

[20] China Academy of Information and Communications Technology. White Paper on Internet of Vehicles Network Security (2018)[R/OL]. [2020-09-24]. https://download.csdn.net/download/dipolar/14020028?utm_source=iteye_new.

[21] ZHU K Y, SONG J, YE L, et al. Research on Evaluation Index System of Vehicular Terminal Information Security [J]. Industrial Technology Innovation, 2018, 29(6): 11-17.

[22] WANG S L, JIANG F, GU Y Y. Research on Internet of Vehicles Test Based on TBOX Test[J]. Automotive Electrical Appliance, 2018, 362 (10): 38-39.

[23] WANG L M, LI T T, CHEN L. Structure and Security of Internet of Vehicles Based on Vehicle Identity[J]. Journal of Network and Information Security, 2016, 2(2): 41-54.

[24] DU X J. Design of Integrated Circuit Based on CAN Bus for Automotive Electronic Control Unit (ECU) [D]. Tianjin: Tianjin Polytechnic University, 2007.

[25] LIAO F, HUANG J, LI J H. Discussion on the application of automobile OBD interface [J]. Automobile and Driving Maintenance: Maintenance Edition, 2017(12): 143.

[26] ZENG F. Research and Implementation of Intrusion Detection System for Connected Vehicles [D]. Chengdu: University of Electronic Science and Technology of China, 2018.

[27] SEKAR R, GUPTA A, FRULLO J, et al. Specification-based anomaly detection: a new approach for detecting network intrusions[C]// Proceedings of the 9th ACM Conference on Computer and Communications Security. ACM, 2002: 265-274.

[28] SHUKLA A S, MAURYA R. Entropy-Based Anomaly Detection in a Network[J]. Wireless Personal Communications an Internaional Journal, 2018(99): 1487-1501.

[29] WANG D B. The Hierarchical Architecture and Cloud Resource Management of IoV Cloud System [D]. Guangzhou: Guangdong University of Technology, 2015.

[30] YANG N, KANG R B. Network of Vehicles Security Threat Analysis and Protection Ideas [J]. Communications Technology, 2015(12): 1421-1426.

[31] YANG Z Q, ZHENG Y F, XIU J P. Research on Internet of Vehicles Security System Based on Digital Signature[J/OL]. Computer Engineering and Application. https://kns.cnki.net/kcms/detail/11.2127.TP.20210331.1554.034.html.

[32] HUANG H X. Research on Security Technology of Internet of Vehicles Based on Anonymous Authentication [J]. Communication Technology, 2020, 338(2): 233-236.

[33] WAN Z L, KUANG F. Research on Internet of Vehicles Security Architecture Based on Blockchain Technology[J]. Jiangxi Communications Science and Technology, 2019(1): 41-44.

[34] WANG X C. Security of 5G Internet of Vehicles Based on V2X Security Chip[J]. Information Security Research, 2020(8): 705-709.

[35] CHEN N. Design and Analysis of Safety Protection System for Internet of Vehicles[J]. Computer Development and Application, 2014, 27(10): 32-35.

[36] LI X H, ZHONG C, CHEN Y, et al. Review of Internet of Vehicles Security [J]. Journal of Information Security, 2019, 4(3): 17.

[37] GUI Z. Research on Cryptographic Application Technology for Secure Communication of Internet of Vehicles [D]. Chengdu: University of Electronic Science and Technology of China, 2017.

[38] HE W F. Common Threats and Control of Cloud Security [J]. Information & Computer,2018(7):179-180.

[39] WU S Z. Research on Identity Authtification Method Based on Vehicle-borne CAN Bus Network [D]. Changchun:Jilin University,2018.

[40] Vehicle Electrical System Security Committee. Cybersecurity Guidebook for Cyber-Physical Vehicle Systems: SAE J3061_201601[S]. Philadephia:SAE International,2016.

[41] PENG Y,RONG H,WANG W Y,et al. T-box password security protection scheme [J]. Automotive Electrical Appliances,2017(5):64-66.

[42] QIN Q L,XIE L B. Network of Vehicles Data Security Risk Analysis and Related Suggestions [J]. Information Communication Technology and Policy,2020(8):37-40.

[43] LU Z,QU G,LIU Z. A Survey on Recent Advances in Vehicular Network Security, Trust, an Privacy[J]. IEEE Transactios on Intelligent Transportation Systemsk,2018,20(2):760-776.

[44] KOO D,SHIN Y,YUN J,et al. An Online Data-oriented Authentication Based on Merkle Tree with Improved Reliability [C]// 2017 IEEE International Conference on Web Services (ICWS). 2017:840-843.

[45] YU T Q,HU J L,JIN J,et al. Mobile Edge Computing Based In-vehicle CAN Network Intrusion Detection Method[J]. Computer Science,2021,48(1):34-39.

[46] LIU Y,WU G X. Research on Connected Car Connectivity Model Based on 802.11 p/WAVE and Its Application[J]. Journal of Communications,2017,34(6):85-91.

[47] HE X. Distributed Database Security Architecture Based on Intrusion Tolerance [D]. Changsha: Central South University, 2010.

[48] RAWAT A,SHARMA S,SUSHIL R. VANET:Security Attacks and Its Possible Solutions[J]. Journal of Information and Operations Management,2012,3(1):301.

[49] GB/T 20271-2006. Ministry of Industry and Information Technology,People's Republic of China. Technical Requirements for Security Protection of Information Service Platform of Internet of Vehicles [S]. Beijing:Standards Press of China,2020.

[50] SHAMIR A. Identity-Based Cryptosystems and Signature Schemes[J]. Lect. notes Comput. ,1985,196(2):47-53.

[51] CHEN P,GAO T G. Multi-topic and Multi-correlation Automatic Negotiation and Its Application in Distributed Decision Environment [M]. Harbin Engineering University Press,2013.

[52] CHEN W. Quantitative Analysis Method for High Availability System Design [D]. Hangzhou:Zhejiang University,2006.

[53] TANG X D,LIANG H B,ZHE F P,et al. Computer Operating System[M]. Xi'an:Xidian University Press,2007:1-20.

[54] KARAME G,CAPKUN S. Blockchain Security and Privacy[J]. IEEE Security & Privacy,2018,16(4):11-12.

SONG Tao, born in 1992, Ph.D candidate, is a student member of China Computer Federation. His main research interests include IoV application, IoV security, cloud computing and deep learning.

LI Xiu-hua, born in 1987, Ph.D, professor, Ph.D supervisor, is a member of China Computer Federation. His main research interests include mobile edge computing/caching, big data analysis and machine learning.

(责任编辑:柯颖)