

基于车辆身份的车联网结构与安全

王良民^{1,3}, 李婷婷¹, 陈龙²

(1. 江苏大学计算机科学与通信工程学院, 江苏 镇江 212013;

2. 江苏大学汽车工程研究院, 江苏 镇江 212013;

3. 安徽大学信息保障技术协同创新中心, 安徽 合肥 230601)

摘要: 对车联网安全研究进行了综述, 没有逐一分析车联网应用场景的具体安全需求, 而是着眼于车联网系统本身的特点, 提炼出了当前发展中所存在的主要问题, 进而厘清了车联网在不同发展阶段的概念内涵及网络架构; 在明确的车联网概念与结构的基础上分析其安全问题, 提出了以车辆身份认证为基础的三层安全体系结构, 并以此结构为基础, 分析了相关工作的进展。最后, 指出了随着通信技术与数据服务能力的发展, 车联网结构和安全研究的新领域。

关键词: 车联网; VANET; 安全协议; 身份认证

中图分类号: TP393.0

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00029

Security issues and system structure of internet of vehicles

WANG Liang-min^{1,3}, LI Ting-ting¹, CHEN Long²

(1. School of Computer Science and Communication Engineering, Jiangsu University, Zhenjiang 212013, China;

2. Automotive Engineering Research Institute, Jiangsu University, Zhenjiang 212013, China;

3. Con-Innovation Centre of Information Support & Assurance Technology, Anhui University, Hefei 230601, China)

Abstract: Instead of focusing on concrete security requirements of each IOV applying scenario, the architecture characteristics of the IOV networking systems were summarized, and the main security problems were extracted by analyzing the connotation and network architecture of IOV in different development stages. Then an identity authentication based three-tier security architecture over the clearly analyzed concept and structure was proposed, and the related IOV security research with the view of the presented three-tier security architecture were surveyed. Finally, some new developments and progresses over security of IOV were presented.

Key words: internet of vehicles, VANET, security protocol, identity authentication

1 引言

车联网 (IOV, internet of vehicles) 作为典型的物联网系统, 被称为“可能第一个落地的物联网”^[1], 是智慧城市的重要标志, 也是智能交通的重要组成部分, 有着非常广泛的前景。车联网不仅可以

多个用户与车辆之间进行通信合作, 还可以获取、管理和计算人类、车辆、事物和环境相互之间大规模的数据, 以此来改善复杂的网络系统和信息服务, 进而带动基于车辆运营大数据、交通大数据、驾乘习惯大数据等数据服务产业的发展, 成为经济与社会发展的重要推动力量^[2]。车联网的

收稿日期: 2016-01-08; 修回日期: 2016-02-01。通信作者: wanglm@ujs.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61472001); 江苏省重点研发计划基金资助项目 (No.BE2015136)

Foundation Items: The National Natural Science Foundation of China (No.61472001), The Key Research and Development Plan of Jiangsu Province (No.BE2015136)

一个理想目标就是最终实现人—车辆—事物—环境的深度融合,借此减少社会成本,提高交通效率,保证人类在高效出行的同时享受其带来的增值服务。

然而,车联网从概念的最初提出,到如今若干车联网技术阶段性的应用和在公共服务领域获得巨大成功,如高速公路上ETC不停车收费^[3]、智慧公交系统^[4]中随时随地网络查询公交车到站时间、城市自助式自行车“一卡通”系统^[5],都可以说是车联网概念和技术在某种层面上的意义。但是,这些简单的应用离人们对完全意义上车联网的憧憬还有很大的差距,到目前为止,关于车联网尚有如下问题没有厘清。

1) 车联网的内涵和本质:显然,车联网首先应该实现汽车是网络上的节点,即实现车—车通信,而不是在汽车上放一个手机,通过现有网络来查询一些位置信息;其次,车联网应该方便人们在车辆上的网络生活,如网络办公、网络视频等;更为重要的是,车联网应该以便捷的网络性能提供更完全意义上的交通安全环境,甚至授权的用户可以通过网络直接访问、控制任何一辆车。

2) 车联网的通信标准:车联网是一个复杂的网络系统,包含了车—车通信、人—车通信、车—路通信,不同的通信场景、需求需要不同的通信技术和协议标准,如车内人员的增值服务流量大,车路的访问由于车速快对网络接入速度要求高,认证用户通过网络对车辆的控制,需要封闭性高和安全性强等,至今没有一个好的网络协议和通信技术同时满足这些需求。

3) 车联网的安全技术:车联网不同于普通网络,即使是金融网络的入侵问题,也可以通过事后修复来弥补经济损失,但是车辆和车辆造成交通事故的损失,是不可挽回的生命财产损失,其安全性的重要程度不言而喻。然而,独立汽车电子系统设计的是封闭式系统,设计之初并未考虑接入网络所带来的安全问题,2015年8月黑客大会上,DARPA授权的黑客演示无线入侵一辆汽车或卡车的网络系统,就暴露出这种车联网安全的

先天性缺陷带来的问题^[6]。

4) 车联网的建设主体:车联网也许和高速公路一样,需要很多的基础设施,这些基础设施需要政府投资;然而换一个角度,通信基站宽带之类的基础设施投入是通过运营商承建的,车联网是不是可以让电信运营商来建设?另外,汽车作为车联网的落地物体所在,让汽车制造商建设车联网也是可行的,如通用的安吉星^[7]、中国金龙汽车的G-box等,这些公司已经开始了有益的尝试。政府、运营商和汽车制造商对于物联网建设的话语权及推动作用,尚需要时间和技术发展来决定。

一个基本事实是,在未彻底解决车联网本质内涵、通信标准和安全问题之前,无论政府、电信运营商还是汽车制造商,是不会全力推动车联网发展与产业的落地的。这个基本的事实和人们对车联网必将落地的信心,也决定了各个企业都抢先在某个市场和成熟技术应用上大力宣传车联网,如ETC收费^[8]、智慧城市、智慧路径^[9]、同公司车—车互联等产品^[7]不断推出,但是缺乏统一的车联网体系与建设方案,甚至对其核心的安全技术,也在当前这种产业发展格局下,以市场需求为中心,“头痛医头、脚痛医脚”,以“打补丁”的方式一个又一个地解决系统的安全问题。然而,问题的关键是,车联网的安全问题若以打补丁的方式解决,牵扯着生命安全的车联网产业又如何发展呢?

为此,本文综合考虑到车联网系统推广不可能一蹴而就、汽车电子系统已经在有车联网之前就独立设计好了这2个基本的事实,在此基础上探讨如何逐步建设车联网,车联网的体系结构应该是什么样的?在这样的结构下,车联网安全问题如何系统考虑?

2 车联网的体系结构

什么是车联网?这样的概念争执是没有意义的事情。但是,弄清楚车联网的结构,无论对建设车联网,还是讨论车联网的安全技术,都是一个非常基础的命题。本节从车辆互联技术的发展出发,讨论了通信和网络技术的发展,给车辆互联及车联网概念和内涵带来的变化。

2.1 “类车联网系统”的发展历史

“类车联网系统”是在车联网概念尚未诞生时，人们在实际应用中实现了车—车互联的各类交通管理系统。从车辆之间的通信方式来看，最早的车—车通信应该是车队出行时的对讲机。随后，出租车公司使用的“交通指挥系统”可以认为是车载自组网（VANET, vehicular ad hoc networks）的雏形：每一辆车上都有对讲机，每一辆车都可以广播信息，也都可以接收信息；有一个交通指挥中心，可以把车队的车辆和其他车辆报告的道路情况实时播报到无线电台广播。网络出现之后，“交通综合服务呼叫中心”^[10]被称为最典型的智能交通系统，通过网络把交通呼叫系统变成和形成区划对应的分级网络系统，具体网络结构如图1所示，它充分利用了电话通信技术进行信息采集、实时了解道路交通情况。

无线网络和射频通信的普及，再次推动了这种变化，一些政府机构车队和运输公司，开始在车上装GPS定位系统，通过GSM技术实现对车辆位置信息的实时了解、跟踪和保护，如海关的“电子关锁”系统^[11]、高速公路的ETC不停车收费系统^[8]等，是2个最为经典的应用。当3G、4G通信技术兴起，能支持更大流量的无线信息传输

时，“智慧公交”等开始号称“车联网”的系统也逐步走进了应用^[12]。

从“车联网”以及与车联网有关系统的发展历程可以看出，车联网的每一次发展，都是通信技术发展的结果。从对讲、电话的通信方式发展到网络和无线通信，从简单的信息传输发展到大量信息甚至多媒体信息的传输。同时，也能从车联网的发展历史看出，交通系统^[13]对车联网的需求不仅仅是组成一个网络，而是成为交通系统的重要组成部分，不仅是采集信息的终端网络节点，也包括信息处理后进行车辆调度的系统工程。这些也是组成车联网概念和内涵的不可或缺的部分。

2.2 VANET 结构

VANET 是一种典型的车联网系统^[14]，甚至在很多学术期刊上并不怎么区分 VANET 和车联网的概念，在交通领域，为了方便起见，通常将 VANET 表达为狭义上的车联网。VANET 结构如图2所示，所有的车辆都通过 Internet 连接在一起，其通信方式分为两类：一类是车—车（V2V, vehicle to vehicle）通信；另一类是车—路边通信单位（V2R, vehicle to road side unit），路边通信单位（RSU, road side unit）就是建设在路边的基础设施（infrastructure），用来实现车辆和因特网之间的连接。

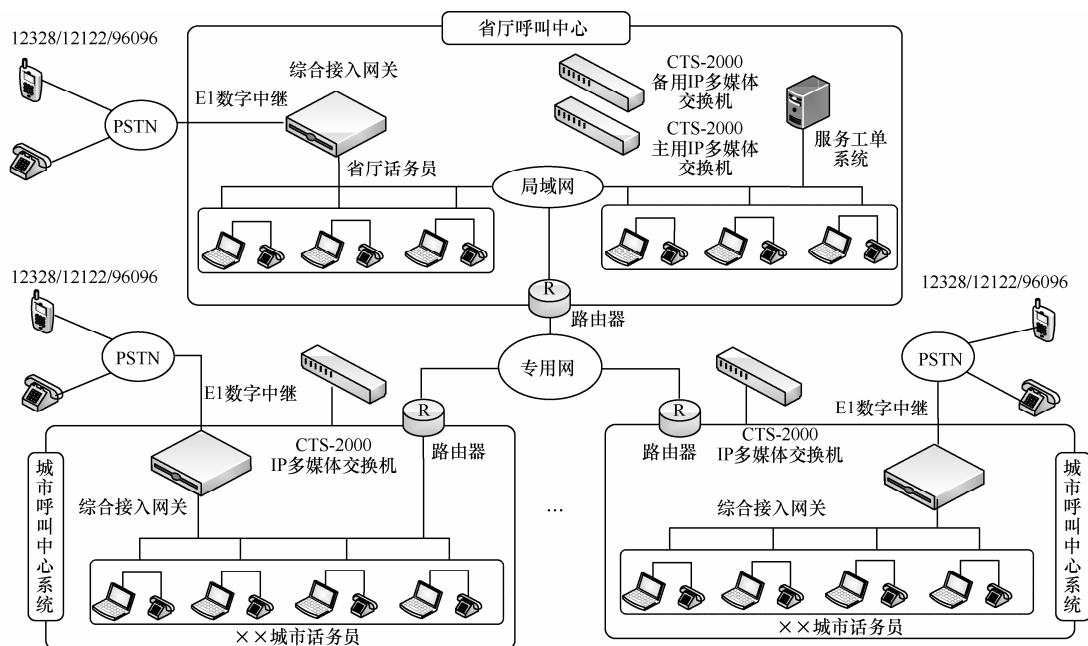


图1 “呼叫中心”的分级网络系统

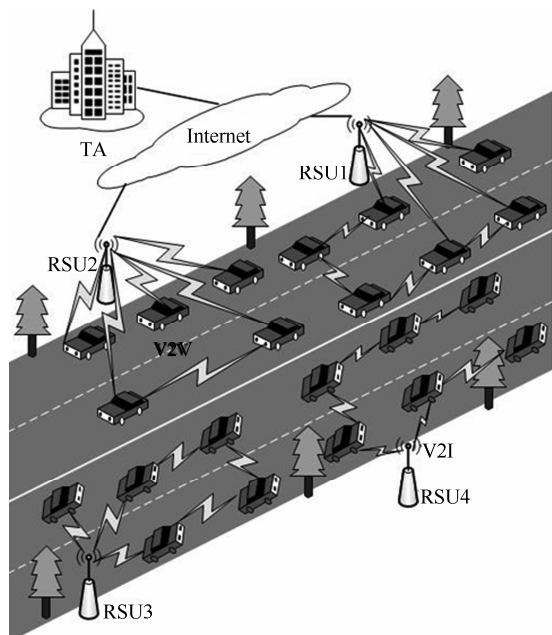


图2 VANET 架构

车辆的高速运动是车联网的一大特点，VANET 之所以被广泛地当作“车联网”，最主要的原因就是它适合车辆在运动中的互联要求。一方面作为自组网，适应车一车之间因为车辆运动会发生拓扑变化；另一方面车辆不断地接入路边单元，路边单元作为因特网存放在路边的基站（或者称为热点、中继节点），承担着将运动的车联网与因特网连接的责任。同时，VANET 还具有可延展（scalable）的结构，路边基站可以逐步建设，先建一条路、一个城市，

然后逐步增大范围，这样车联网也可以逐步拓展。这更符合当前建设物联网的现状。此外，VANET 结构实现了功能和发展主题的独立设计，路边基础设施交给政府、车载平台交给汽车制造商、通信和通信载体交给电信运营商，这也使发展车联网所涉及到的主体责任明确，利于车联网发展。

2.3 多网融合的车联网

VANET对车联网描述中最大的不足在于网络，没有考虑到用户基于车联网的服务要求。既然接入了因特网，一方面增值服务的工作娱乐功能必然成为车联网的商业目标之一；另一方面，用户也希望对车辆的分析和控制可以交给万能的互联网去解决。因此，广义的车联网应该是一种多网融合的网络结构^[15]，如图3所示，包括车内网、车际网和车载移动互联网。“车内网”就是汽车电子系统集成和网络系统，从汽车制造商的角度实现车辆内部所有的信息都连网；“车际网”就是VANET，通过无所不在的因特网实现了车一车互联；“车载移动互联网”，一种通俗的说法就是“把一个手机放在汽车上”，然后基于手机的功能和部署的3G/4G网络，方便车内用户把车载单元（OBU，on board unit）作为访问互联网的接入热点，享受互联网提供的增值服务，同时，为车辆和交通系统提供各类增值服务。

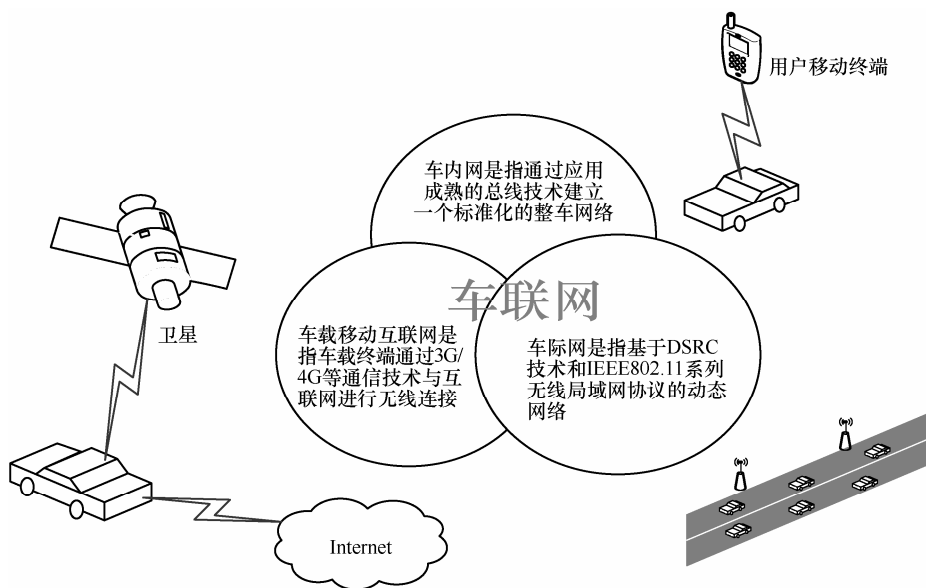


图3 三网融合的车联网系统

3 基于身份的车联网安全体系

根据第2节分析,车联网的概念和内涵需要全面兼顾各类用户的服务需求,同时也被赋予网络自组织、结构可延展、多网融合等特点。这些特点也使车联网相比一般移动网络,面临着更严峻的安全威胁。鉴于目前非常缺乏这种关于多网融合结构的车联网安全的系统研究,本节并不分析现有系统的安全漏洞和不足,而是从一个全新系统的角度分析用户需求,特别是在现有的车辆生产和管理机制下车联网安全应该考虑的因素,进而提出一种基于身份的安全体系。

3.1 安全需求

车联网首先也是一个网络,车联网的安全自然要包含网络安全需要的绝大部分内容,如保密性、认证性、完整性等^[16-20],安全的手段也包括密码认证、访问控制、以可用性保障为目标的容错容错机制^[21]等。然而,车联网存在的多网融合环境由多重不同的网络组成:车间网包含了车辆与车辆之间的自组网结构、车辆与路边基站之间的无线接入网络结构;车内网不仅包括以总线和数据感知设备之间的有线网络,还包括车内环境感知和车内驾乘人员与车联网连接的无线网;再加上车载移动物联网,至少包括5种不同类型的网络结构。这种网络融合的特性是导致车联网系统安全新问题的最主要原因。

1) 首先是“短板效应”,这些网络因为功能的不同,对安全性有不同的要求,安全不同的网络融合常常会出现整个网络的安全是由安全性最低的网络所决定。

2) 其次是组合安全的问题^[22],也就是说2个网络协议在各自的网络结构里使用没有问题,但是一旦一起使用,会让一个网络里的协议恰好为另一个网络的安全协议充当了随机预言机——替它的攻击者计算加密和解密运算的结果这一完成破解安全协议的最核心环节。

3) 最后就是客观的安全背景,在车联网以前,汽车电子系统是独立设计的安全体系,并未考虑到网络接入及其可能带来的脆弱性,更未考虑到最后汽车的控制会放在互联网这么一个攻击者随时随地都会出现的巨大体系里。

此外,车联网因为参与主体和参与角色的不同,往往还存在隐私与安全的内在需求关系矛盾的。如车联网在把车辆接入因特网的同时,也让每一辆车成为信息的发布者和接收者^[23]。作为信息的发布者,希望匿名以保护隐私;作为信息的接收者,希望有信息发布的源头认证来保证信息的真实性;同样,作为车联网的用户出于隐私考虑需要匿名性和不可追踪,但是作为网络服务的提供者为了保证有偿服务的收费,又希望所有的服务都是可追踪且不可抵赖的。

3.2 基于身份的安全体系

从车辆管理的传统方法来看,各国现有车辆管理体系均是以身份为基础的管理体制——要求所有车辆在管理部门进行强制登记注册,给车辆具有唯一性的编号。车联网作为对现有车辆与交通管理手段的发展,自然需要对所有车辆进行统一编号并提供身份认证,这样才能保证作为通信对象的车辆或者RSU至少是一个合法用户或者可靠的基础设施,而不是攻击者伪造的虚拟场景中的车辆或者路边单元。从而,车辆可以对通过认证的车辆赋予足够的信任,这成为车联网安全的可信基础。

很多与车联网安全相关的组织也纷纷成立并启动了一系列研究项目来促进车联网的安全发展:IEEE 1609.2工作组^[24]着重探讨了车联网中的安全问题并为工业界制订了相应的规范建议;由大学研究机构和汽车生产商组成的SeVeCom项目^[25],针对车辆通信中存在的各类安全问题展开了全面的研究;C2C-CC^[26]与NOW^[27]项目针对车联网中的通信协议和如何保证数据安全性的问题,研究其解决方案;PRECIOSA项目^[28]则着重针对车联网系统中的隐私保护问题进行了研究。在上述各安全相关研究中,车辆身份及其认证技术是车辆安全的基础。所以,本文认为身份认证是车联网安全的基础。

3.3 基于身份的安全问题

从当前基于号牌管理车辆的身份,过渡到以唯一的数字ID管理基于VANET的车联网中的车辆身份,这是一个自然而然的想法,也是众多安全项目采取的研究基础。然而,车联网与Internet连接,具有可随时随地接入、访问的特性,这也给这项成

功的传统管理方式带来了新的问题。

1) 身份安全和身份认证的效率问题。必须建立一套严密的机制来防止身份的伪造和盗取。通常,注册机构会采用高安全强度的密码机制,保证身份不可能被伪造;进而,采用不可复制硬件^[29](physical proofed)作为密钥的保存模块,保证象征身份的密钥一旦被接触就自动销毁,从而不可能被复制。在身份安全的前提下,需要有高效的机制和高安全性的协议来提供高速运动中的车辆接入身份认证,显然在通常的情况下,认证效率和安全性之间是一对难以调和的矛盾需求。

2) 合法身份转借滥用的内部攻击问题。车联网中车辆的移动性使车辆需要通过不同的RSU接入访问,基于身份的管理方式,不允许不同车辆采用同一身份接入访问。然而,攻击者可以以合法的方式加入车联网,然后从消息上复制合法身份,发送给同伙车辆,用复制的合法身份信息,进行破坏性活动,如Sybil攻击^[30],一辆车辆通过伪造的多个身份在同一位置获取不当利益。

3) 位置与身份关联的隐私泄露问题。车辆通过不同位置的RSU获取服务,使车联网中的用户可以根据不同时间车辆的位置信息关联获得其他车辆的运动轨迹。进而跟踪车辆身份及车主行踪,形成严重的隐私泄露问题;但是,如果车辆身份采用匿名、假名以及防跟踪等隐私保护技术,结合车辆节点高速移动性等特点,使在身份认证过程中及时鉴别身份的滥用更加困难。

根据上述问题的分析,结合车联网中身份问题的重要性,建议车联网中采用以身份为核心的安全体系结构,进而在身份认证的基础上考虑基于身份的攻击防范等网络安全问题。最后,从通常网络攻击威胁隐私的角度,防范隐私攻击,在身份安全的基础上,考虑服务安全问题,以这样的三层安全结构保护车联网的安全。

4 车联网安全研究

本节在基于身份的车联网三层安全体系结构下,综述现有车联网安全技术研究,并且归纳其特点,指出不足。

4.1 身份认证技术

车辆自组网中车辆可自组织地构成对等网络

相互通信,也可通过路边单元访问服务提供商的应用服务器获得服务。为了保证通信安全,车辆通信需要对每条信息进行身份认证。一些服务甚至需要RSU与车辆的双向身份认证,因为RSU可能是不可靠的、虚假的。通常来说,车辆的双向身份认证协议需要满足下述4个基本性质。

1) 高效性:由于车辆速度较快、RSU覆盖范围较小,使车辆需要频繁地进行身份认证;同时,RSU提供认证服务的处理需要一定的时间。因此,为避免车辆较多情况下的认证拥堵,高效的认证服务是VANET认证所必需的。

2) 隐私性:车辆在通过一个RSU覆盖区域享受服务时,应该具有匿名和不可跟踪等隐私性,无需担心在获得服务时带来隐私泄露问题。

3) 不可否认性:认证中心能鉴别所有车辆认证的身份信息,且可追溯到认证实体,即服务发生后,所认证车辆不可抵赖行为的发生,可以确保服务提供商能够正确地扣费。

4) 可撤销性:车联网通信中,接收方需要查询发送者的身份是否被撤销。当恶意车辆被发现后,网络管理者需要向整个网络披露恶意车辆的身份。RSU和OBU会保存恶意车辆身份构成的撤销列表,从而隔离恶意车辆。

在早期的认证研究中,V2I通信中主要是使用公钥基础设施^[31~34](PKI, public key infrastructure)来为每个用户颁发相关密钥及公钥证书,而V2V通信则借用这种V2I通信的安全措施,保证用户之间的安全通信。但是这种方法会在通信过程中产生很大的计算开销和传输开销。随着车辆数目的激增,这种传统方案的缺点越来越不可接受。

随后,基于身份的公钥加密体制成为身份认证的基础方案^[35~38],该方法减少了对公钥证书的计算过程,缓解了计算开销和传输开销。文献[35]提出了一种具有隐私保护性的批量认证的方法,它的问题是不能抵御签名重放攻击,没有考虑V2V通信,也没有提出合理的V2I通信机制,所以认证效率不高。而文献[36]提出了一种有效的隐私保护方案,减少了V2I双向认证过程中假名的大小,但是,这种改善不能满足认证高效性的需求。文献[37]提出了一种双向认证的密钥管理方案,可以缓解计算开销,但对可撤销性和不可否认性缺乏考虑。文献[38]

提出了一个无证书公钥 V2I 通信协议，但是只限于车辆对 RSU 的单向认证。

为突破车辆网络认证的物理瓶颈，批认证方案中 RSU 接收来自车辆的认证消息后，用一次运算同时给一批车辆提供认证服务，以此来取代车辆逐一通过 RSU 认证的传统方法，该方案将多次运算和广播发放合并为一次，大大提高了认证的效率。文献[39]提出了一种批量认证的密钥管理方案，加快了服务密钥的协商速度，但同样缺乏对可撤销性的考虑；文献[40]提出了双向认证方案，其认证速度是每秒可以验证 2 540 个信息，是目前最高效的认证协议，但从下文可以看出它依然没有达到要求，RSU 瓶颈依然存在；最近，江苏大学的 Liu 等^[41]提出了代理身份认证的方案，将该速度提高到 2 650 条/秒，实现了认证效率的本质突破。

另外，身份的撤销是通过撤销车辆网中的非法车辆来保证群组的安全，证书撤销链表是一种常见的技术。文献[33]和文献[42]都采用证书撤销链表公布非法车辆的撤销信息，对非法车辆进行排除，进而保证车辆网用户的安全性。前者撤销链表的大小只和车辆的个数呈线性关系，与车辆用户的假名多少无关；而后者采用二分搜索的方式加快了对撤销链表中信息的查询速度。但是当撤销链表中的信息较多时，上述方案会产生较大的存储开销以及查找时延。为此，对快速运动的车辆网络来说，证书撤销链表的身份撤销方法存在不足。江苏大学的 Zhu 等提出采用短散列链^[43]和布隆过滤器的方法来更新列表，可在保证安全性的情况下，大大提高撤销链表的效率。

表 1 给出的是一些方案在各种性能方面的比较，其中，“—”表示没有考虑这种性能，“×”表

示未能达到所列性能的要求，“√”表示满足所列性能的要求。

需要指出的是，表 1 中 EMAP 方法主要用于 V2V 通信，它可以加快车与车之间会话密钥的协商，但是没有考虑车辆与基站的接入。更为重要的是，相关研究在未能综合考虑提高身份认证协议 4 个方面性能的同时，更没有考虑 RSU 的物理瓶颈问题——RSU 的物理处理能力是有限的。RSU 不仅承担车辆的身份认证服务，还提供安全交通服务和娱乐服务等增值服务，如图 4 所示。

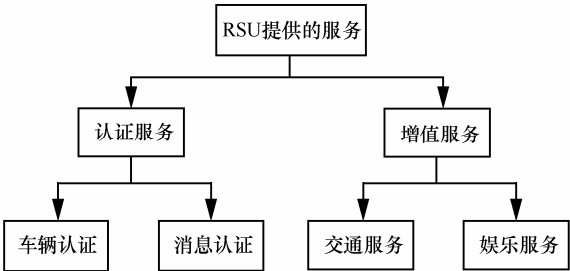


图 4 RSU 的认证工作负荷分解

然而，仅认证服务，RSU 就承担了过于繁重的工作量。通常，RSU 的覆盖半径是 10 km，以高速公路车辆速度为 120 km/h 计算，则 RSU 每隔 6 s 就需要提供一次车辆身份认证服务；另外，根据 DSRC 标准，车辆每 100~300 ms 发送一条安全消息，设车距为 200 m，车辆每 200 ms 发送一条安全消息，则 RSU 每秒需提供 500 次安全消息认证，然而事实上车距远远小于 200 m。可以看出，RSU 已经成为决定 VANET 服务质量高低的物理瓶颈。RSU 认证服务的压力巨大，认证服务占用了较多的 RSU 通信资源，为此，认证服务——包含直接加入子网的身份认证和消息中的消息源身份认证，以其巨大的验证工作量及其对服务质量的巨大影响，形成了一个亟待解决的

表 1 各方案性能比较

典型协议	批量认证	双向认证	可撤销	不可否认	隐私保护
ESA2006 ^[31]	×	×	—	—	×
SPECS2011 ^[32]	√	√	×	×	√
EMAP2013 ^[33]	×	√	√	√	√
IBV2008 ^[35]	√	×	—	√	×
ECPP2008 ^[36]	×	√	—	×	√
AKA2009 ^[37]	×	√	—	—	√
ABAKA2011 ^[39]	√	√	—	√	√
CPAS2012 ^[40]	√	×	—	√	√

RSU 认证瓶颈问题。Liu 等^[41]提出的代理身份认证方案可以缓解这一瓶颈问题,但是依然未能彻底解决这个认证问题。期待未来 5G 通信时,车与车之间直接的 D2D 通信方案^[44]能彻底丢掉 RSU,从而解决这一瓶颈问题。

4.2 身份攻击及检测技术

车联网络中基于身份的内部攻击可以归纳为 2 种类型。一种是 Sybil 攻击,指恶意节点通过虚假注册、伪造偷窃等方式获取多个合法身份参与网络通信,以达到自己的非法目的。例如恶意车辆为独享道路,可以通过声称的多个虚假身份制造交通拥堵的假象。由于车联网的开放性允许新的车辆不断加入,这样攻击者可以通过多次注册获得多个合法身份,此外,合法注册车辆得不到集中式的照料,其身份也可能被偷窃伪造。另一种是恶意节点拥有一个合法身份,利用网络传输快于车辆运动的特性,在多处使用相同的身份以获利,类似现代交通管理中的套牌攻击,同一个身份在多地的消费及恶意行为,将带来追究取证的困难性。

由于基于身份的攻击均建立在已经获得了合法身份的基础上,已经突破了基于密码学的身份认证技术的保护。目前,关于身份攻击的检测方法,主要有基于邻居关系、基于真实位置、基于行车路径 3 类方法。

Grover 等^[45]提出了一种利用节点间邻居信息的相似性检测 Sybil 攻击的方法。该方法中每个节点周期性广播指示消息告知周围车辆自己的信息,车辆计算自己的邻居节点信息,并交换邻居节点集合,计算集合的交集。由于车辆的运动特性,使它们不会一直拥有许多相同的邻居节点,从而检测一个车辆拥有多个不同身份的行为。Abbas 等^[46]通过分析邻居车辆的时间和 RSS 强度,得到邻居车辆的 TIME-RSS 序列。由于 Sybil 节点并不是真实存在的,在它的 TIME-RSS 序列中, RSS 呈现出突发增长,而正常车辆的 RSS 增长则较缓慢。这种方法的优点是不需要 RSU 的帮助,但是,车辆间交换邻居信息的真实度,依赖于恶意车辆的忠实行为,检验的前提是一个悖论。

一个身份只能有一个位置,同样一个相对精确的位置只能有一辆车。为此,如果将车的身份

和位置信息绑定,可以发现身份攻击行为。针对车辆可能对身份造假的问题, Yan 等^[47]提出采用车辆雷达验证邻居的真实位置,获得车辆周围的局部安全,这并不能从全局角度消除攻击,也增加了硬件成本; Abbas 等通过分析邻居车辆的信号强度来检测 Sybil 攻击,通过 TIME-RSS 增长速度来判定恶意攻击,但是如果攻击者有多个 OBU,检测效率将大大降低; Yu 等^[48]利用预定的无线信号传播模型和收到的信号强度分布模型计算邻居节点的估计位置,验证位置信息的准确性;同时在 RSU 的帮助下选用相反方向的车辆作为证明车辆,消除了验证车辆造假问题。然而,这种方法增加了 RSU 的负荷,而且考虑到车辆的动态性,这对全局的时间同步以及计算速度有相当高的要求。

由于车辆运动的自主性,网络中没有任何 2 辆车辆会在一段时间内的相同时刻都经过相同的 RSU,一个车辆也不可能同时出现在不同的 RSU 处。根据上述思想,基于车辆运动路径(motion trajectories)^[49~52],利用城市道路的交叉口、路边 RSU 等参照物,计算、对比位置相近车辆的路径,身份相同车辆的距离等,来判断身份的滥用。但是该方法要求路边基础设置的存在绝对可信,同时会泄露车辆的路径信息和位置隐私。

由此可见,车联网对隐私保护性质的要求,往往进一步增加了身份攻击的可能性和检测的困难性。例如,假名机制中车辆不使用真实身份发送消息,而是使用分发的假名发送消息,恶意车辆对假名的非正常使用(使用多个假名发送相同或类似的消息),形成了多个合法身份的 Sybil 攻击。针对恶意车辆滥用假名引起的 Sybil 攻击问题,文献[53]中提出了“车辆一次只能拥有一个有效的假名”的方案,在这个假名即将失效前,车辆通过请求 TA 或 RSU 在线获得新的有效假名。但是车辆更新假名时,需要请求 TA 和 RSU,增加了网络的负载。为避免每次更换假名的周期性开销, Zhou 等在文献[54]中提出了一种新的假名分配机制 P2DAP。该方法中 TA 通过使用粗粒度和细粒度密钥对假名进行 2 次散列计算分别得到假名的粗粒度散列值和细粒度散列值,以此来区分假名滥用的身份欺骗行为。但是,该方法要

求 RSU 和 TA 多次计算粗粒度散列值和细粒度散列值,给网络带来了较大的计算与传输开销。

表 2 给出了当前研究中基于身份攻击的检测方法,可以看出,检测方法通常都会利用 RSU,增加了 RSU 的负载,或者会导致隐私泄露问题。为此,本文认为这些基于身份的攻击问题也必须得到解决或者一定程度的缓解。

但是,更为严峻的事实是当前研究尚未考虑到的是,针对一个车辆采用多个合法身份和多辆车辆采用一个合法身份这 2 种攻击模式,可以组合成合谋攻击,即 m 个恶意节点用 n 个合法身份,形成非同时参与攻击 (non-simultaneous participation),攻击者在某段时间内不使用全部虚假身份,而是使用其中的一部分参与网络通信,以躲避追踪。由于车辆可以在网络上交流,合谋攻击也是容易实现的,进一步可以形成新型高级持续性威胁 (APT, advance persistent threat) 攻击,攻击者将多次非法行为分配给其拥有的多个身份,平均每个身份的非法行为次数减少,甚至伪装成合法行为,那么网络就很难检测出这些非法行为。Feng 等^[55]采用基于信任和信誉的方法,结合环签名方案,实现了对多种来源 Sybil 攻击的检测,也能基于信誉的角度提升降低合谋攻击的成本。但是,鉴于信誉和信任系统自身的特点,如事后追求、查询需要时间积累、准确率低等特点,并未彻底解决这一问题。

4.3 位置隐私保护技术

保护车辆隐私方法有很多,但其本质都是隐藏车辆和其通信过程中身份之间的一一映射关

系,以达到车辆匿名、隐藏车辆、车辆身份模糊等目的^[56]。最常见方式有 2 类:一类是 Mix-zone 假名方案,避免身份与车辆位置的关联;另一类是群 (环) 签名方案,混淆通信关系与车辆身份。车联网中的位置隐私,也包含了通信关系隐私。因为车联网提供基于位置的服务,在某辆车到达某位置前或离开后,就不能获得服务的内容,因而位置隐私可能以“通过通信连接重建用户位置信息”的方式泄露。这种通信关系隐私包括 V2V 和 V2R 2 类: V2V 通信隐私,即保护车与车之间通信的整个过程中彼此身份、位置、信息内容不被泄露或各自的身份与位置不被关联; V2R 通信隐私,即保护车与路边单元的通信过程中的消息内容、车辆身份、位置不暴露或车辆的身份与位置不被关联。

Mix-zone 假名方案是指在 Mix-zone 内更换假名。假名 (Pseudonyms) 是随时间 (或速度) 而改变的短暂身份标识。车辆配有无关联的多个假名,通过某种机制阶段性地更换,达到隐私保护的目。Mix-zone 的概念和模型架构首先由 Beresford 提出,其思想是通过混合、混淆网络中的节点,变换消息的编码和顺序,达到难以关联消息发送者与接收者的目的。在车联网中, Mix-zone 的选取与设计,与混淆效果密切相关,目前,常见的方式有基于特殊位置^[57]、基于安静时段^[58]、基于加密空间^[59]和基于通信代理^[60]等 4 种典型方式。基于群 (环) 签名的方案,主要是通过混淆群体内个体之间的区分,达到保护车辆匿名的目的。群签名方案中,群体中的任意一个

表 2 基于身份的内部攻击检测方法对比

检测依据	方法	主要手段	优点	主要缺点
邻居关系	Grover ^[45]	车辆邻居节点集合对比	分布式; 不需 RSU 协助	恶意节点不会忠实汇报邻居节点集合
	Abbas ^[46]	车辆邻居节点信号强度变化	分布式; 不需 RSU 协助	恶意车辆可能拥有多个 OBU
位置信息	Yan ^[47]	车载雷达探测对方位置	分布式; 不需 RSU 协助	硬件成本高
	Yu ^[48]	第三方车辆验证位置	分布式; 车辆自主检测	RSU 确定第三方车辆
路径信息	Chen ^[49]			
	Park ^[50]	利用 RSU 等为参照物, 对比车辆路径	集中式; 可全局检测	RSU 绝对可信; RSU 负载增加; 泄露车辆位置隐私
	Grover ^[51]			
	Chang ^[52]			
假名唯一	Studer ^[53]	车辆一次只有一个假名	集中式; 保护隐私	车辆更新/验证假名时, 需要请求 TA 和 RSU
	P ² DAP ^[54]	TA 执行假名对比		

成员可以以匿名的方式代表整个群体对消息进行签名。与其他数字签名一样,群签名是可以公开验证的,而且可以只用单个群公钥来验证;不同的是,群签名保护签名者的匿名性,只有群管理者才可以跟踪签名者。为此,该方案可以用于车联网,一方面,实现匿名认证;另一方面,实现可信中心对特定车辆的跟踪。比较典型的方案有:改进 NF05 方案^[61]、GSIS 协议^[62]、ECPP 协议^[63]和环签名^[64]方案等。

混合方案由于综合使用了多种方法,在综合性能上具有更优的效果。如路径混淆^[65]、随机加密^[66]等淆乱技术也经常用来作为辅助手段,加强隐私保护的效果。AMOEB^[67]是最有代表性的混合方案,采用了3种方式来实现假名、群概念、数字签名的思想,如利用组建车辆的群导航提供匿名,随机安静时段提高目标车辆在导航中的位置隐私,签名密钥管理实现安全与隐私的权衡,达到了减缓车辆的位置跟踪的理想效果。

表3给出了相关的典型方法在隐私保护内容、针对隐私保护的攻击以及隐私保护性能方面的比较^[56]。总体说来,各类隐私保护方案均有自身的优点,也有一定的不足。表3中的NF05方案和环签名方案,同时也是一种基于密码学的身份认证方案。

从表3可以看出,隐私保护终究是一个和身份认证关联的命题,这是一组对立统一的技术概念:一方面在VANET中隐私保护不能变成了无

身份无安全的网络,仍需要确认车辆身份提供服务或追溯其责任;另一方面,好的身份认证协议需要具有隐私保护性能,隐私保护的水平越高,认证的难度与复杂度越高,这给系统提出了更高的要求,让RSU的瓶颈问题更加突出。

最新的研究已经开始对解决上述问题进行探索,如开销更小的条件隐私保护的环签名方案^[68]、合作认证方案^[69]、组认证的条件隐私保护的签名方案^[70]等,为RSU认证瓶颈问题以及提高认证效率提供了可能性;又如新认证模式^[41]及新的认证与攻击检测结合的方法^[71]、新的隐私保护方法^[72]以及可能用于解决离散车辆之间认证问题的不可信平台的验证方法和基于云平台的通信方案^[73]等新技术,也可能为上述问题的解决提供潜在的新途径;当然,车联网安全结构和安全问题的发展会因为网络结构的不同而改变,以多种特性融合的5G技术^[44,74,75]可能会给车联网从结构到安全带来完全不同的问题和解决方案。

5 车联网研究的未来发展

车联网渐渐地进入到人们的视野,车联网市场在国内被称为有一万亿级市场,正受到人们越来越多的重视,不可估量的商业机会和发展潜力隐藏在车联网技术中。在2015年,我国拥有4000多万汽车互联网技术服务用户,成为了全球车载信息服务业最大的市场,政府也出台了相关技术大力支持车联网产业技术的发展。车联网技术给

表3 位置隐私保护方法比较

位置隐私保护方法		方法属性特点								
		保护内容			预防攻击		隐私性能水平比较			
		车辆身份	通信内容	轨迹	被动	主动	匿名性	无关联性	不可跟踪	顽健性
Mix-zone	特殊地形 ^[57]	√	×	√	√	/	√	中	中	低
	安静时段 ^[58]	√	×	√	√	/	√	中	中	低
	加密 Mix-zone ^[59]	√	√	√	√	/	√	中	低	低
	通信代理 ^[60]	√	√	√	√	/	√	高	中	中
群签名	NF05 方案 ^[61]	√	√	×	/	/	√	高	低	低
	GSIS 协议 ^[62]	√	√	×	√	√	√	高	低	中
	ECPP 协议 ^[63]	√	√	×	√	√	√	高	低	中
	环签名 ^[64]	√	√	×	/	/	√	高	低	低
路径混淆 ^[65]		√	×	√	√	/	√	中	低	中
随机加密 ^[66]		√	√	√	√	/	√	高	中	中
混合方案 ^[67]		√	√	√	√	/	√	高	高	中

人们勾勒出一个美好的场景，即利用先进的技术对道路交通进行全面感知，最终实现人、车、基础设施和网络高效安全地运作。车联网目标的宏伟和美好，还有车联网市场上巨大的经济效益，会让人们持续对车辆网的研究。本文认为车联网后续研究新的增长点应该是由服务计算发展带来的车联网感知大数据研究和以通信技术发展带来的新的5G车联网结构。

5.1 车辆感知大数据

大规模车联网（包括已经走向应用的“类车联网”）将会采集获取大量的数据，随着时间的积累和网络规模的扩展，数据类型和存量会更加广大。大数据的发展不仅将带动交通大数据、驾乘习惯大数据和车辆运营大数据等服务产业的发展，还会给人类带来前所未有的解决交通问题的机遇，如大数据即汽车从生产到销售、从维修保养到运行等各领域信息的联通，推动产业的集成升级。

尽管车联网领域的感知大数据已经被应用于驾驶分析、运输分析等多个交通场合，但目前还有很多挑战。未来交通大数据将在视觉分析、数据处理和数据挖掘等技术的协助下能够处理实时交通信息^[76]。未来大数据将成为众多企业运营车辆的利器，在提供效率的同时也方便用户的出行。但是，由此也会带来更多的安全和隐私问题，如驾乘习惯大数据是针对危险驾驶行为的研究，通过加速、减速、超速、疲劳驾驶等大数据判定车辆是否处于安全驾驶状态。但是，在保障安全的同时，驾驶人员的隐私也就荡然无存，甚至驾驶员的心理反应、下意识行为都在他自己意识到以前被系统窥测。

后台数据安全和隐私将成为车联网安全研究的一个重要方面，不管车联网前端的安全做得如何好，获取的数据被泄密，获取数据的分析出错，分析获取的指挥结论被篡改等，都让前端车联网本身的工作付诸东流。为此，联合车联网及其感知数据，整体考虑交通数据的车联网前端采集、网络传输及后台处理分析，将是未来研究的难点和热点。

5.2 通信方式改变车联网

最近研究领域热门的5G通信技术，具有优

越的通信质量^[77]、高传输速率与高可靠性^[78]等特性，超密集异构网络、D2D通信^[44]、M2M通信等关键技术，正在逐步走向应用。5G的应用，设置可能彻底改变车联网以及以车辆网为基础的驾驶模式，如5G车联网D2D通信、M2M通信逐渐取代路侧单元RSU，车联网中不再需要路边基础设施，则可以在自然灾害发生没有基础设施时，通过5G的D2D技术，自组织车联网搭建临时通信网络开展救援行动。

网络融合的未来5G车联网不仅是对人、车、基础设施、互联网的信息交互融合，可能会彻底改变生活的方方面面，和未来的无人驾驶技术结合，会从从根本上改变目前交通、出行的模式和体验。然而，异构网络融合作为5G通信的一个特点，在满足网络可扩展性、节约开销、用户个性化需求的同时也不可避免改变了安全问题的研究内容，不仅消耗高、速率低、延迟高等多方面的通信问题会有很大程度的改变，因为网络结构不同，基于结构这种通信安全性、跨域认证问题、跨域组合安全问题也许都会有更好的解决方案，更高的通信技术，甚至可能以物理层的方法实现安全的解决方式^[44,79,80]。

6 结束语

综上所述，车联网作为一种多网融合、自组织、可延展（scalable）的网络结构模型，实现了服务和基础设施的分离，可在逐步建设基础设施，发展网络规模的过程中，逐步丰富车联网服务，是一种适合现阶段我国车联网建设现状的、值得推荐的网络结构。在上述结构中，车辆身份认证是维护其安全的基础技术，基于该技术的身份攻击是物联网安全防范的重点，在身份安全之后的，基于位置的隐私保护技术，可以更好地提高服务质量，排除用户的心理担忧，并为后续的源自车联网的大数据提供前端感知保护的基础。而未来车联网安全研究，将主要在以下几个方面展开。

1) 快速高效的安全解决方案。由于车辆在高速运行的环境中，在规定时间内实现信息传输是非常重要的。譬如安全保护的信息获得之后，车祸已经发生，那么安全问题的时间代价太高会导致好的安全方案失去应用上的价值。

2) 适应规模增长的安全理论模型。如果按照车辆的增长速度评估,仅我国车联网的网络节点数目超过 7.5 亿而且还在不断增长。节点数目的增多也随之带来了网络部署和执行的问题,特别是安全和用户的隐私问题在世界上不同的区域呈现出不一样的状态,这需要多样性的安全模型和隐私模型。

3) 异构网络融合的安全研究。异构系统之间认证方式不同、网络结构不同,带来跨域认证问题、跨域组合安全问题、安全算法的时效性等问题。

4) 新通信模式下的安全问题。通信方式会带来车联网结构的变化,新的结构、新的通信方式,可能带来完全不同的车联网安全需求和安全解决方法。

5) 感知数据安全与隐私问题。决定车联网在采集、通信阶段安全和隐私保护的价值,不仅与车联网关联的采集关联,感知数据的传输、存储、处理和后期查询方式等也是非常关键的环节,建立新的数据隐私映射方式可能带来整体安全技术研究的变化,未来可能会将数据隐私研究作为专门的计算方式,区别于数据安全的运算模式,将贯穿于车联网前端的采集传输和后台的大数据处理,成为新的研究领域。

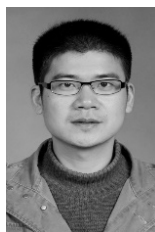
参考文献:

- [1] ANIS L, AMIR Q, SAAD M, NAUFAL M. Vehicular Ad-hoc networks for smart cities[M]. Berlin: Springer, 2015.
- [2] YANG F, WANG S, LI J, et al. An overview of internet of vehicles[J]. China Communications, 2014, 11(10): 1.
- [3] HUANG H, XIAO S, MENG X. Application of RFID and SNMP technology in highway electronic toll collection system[C]// The 3rd IEEE International Conference on Computer Science and Information Technology (ICCSIT). c2010:383-385.
- [4] AGARWAL A, GOEL N. GPS-RDS enabled location based smart transit[C]//The 13th International Conference on Intelligence in Next Generation Networks. c2009:1-5.
- [5] LEE K H. The multiple impacts of the neighbourhood environment on the use of public bicycles by residents: an empirical study of Changwon in Korea[J]. International Journal of Urban Sciences, 2015, 19:1-14.
- [6] 2015 年 8 月黑客大会:演示远程入侵汽车[EB/OL]. (2015-05-04). <http://www.ijandao.com/safe/it/13134.html>. Hackers conference in August 2015:demonstrate the remote invasion of cars[EB/OL].(2015-05-04). <http://www.ijandao.com/safe/it/13134.html>.
- [7] 通用 Onstar (通用安吉星) 服务系统[EB/OL].(2016-02-09). <http://www.chemdrug.com/article/7/2419/12093490.html>.
- [8] 王良民, 茅冬梅, 梁军. 基于 RFID 系统的隐私保护技术[J]. 江苏大学学报, 2012, 33(6):690-695.
- [9] WANG L M, MAO D M, LIANG J. Privacy preservation technology based on RFID[J]. Journal of Jiangsu University, 2012, 33(6): 690-695.
- [10] CHENG Y, DUAN L, ZHANG Q. Routing in internet of vehicles: a review[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(5):1-14.
- [11] REITE J L, ROBERTSON C, WADHERA N. Call center integrated printing device consumable cabinet device service: US8788373[P]. 2014-07-22.
- [12] 陈实武. 海关物流监控系统的电子开锁设计[D]. 武汉理工大学, 2006.
- [13] CHEN S W. Electronic lock design of the customs logistics[D]. Wuhan University of Technology, 2006.
- [14] CHEN Y, DUAN L, ZHANG Q. Financial analysis of 4G network deployment[C]// IEEE Conference on Computer Communications (INFOCOM). c2015.
- [15] VONG C M, WONG P K, WONG K I, et al. Inspection and control of vehicle emissions through internet of things and traffic lights[C]// International Conference on Connected Vehicles and Expo (IC-CVE). c2013:863-868.
- [16] ABBOD K, ZHUANG W. Impact of microscopic vehicle mobility on cluster-based routing overhead in VANET[J]. IEEE Transactions on Vehicular Technology, 2015, 64(12):1.
- [17] ZHOU M. Intelligent monitoring system based on the multi-network integration[C]//International Conference on Intelligent Transportation, Big Data and Smart City (ICITBS). c2015.
- [18] LI X, WANG L. A rapid certification protocol from bilinear pairings for vehicular Ad hoc networks[C]// The 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, IEEE Computer Society. c2012:890-895.
- [19] 王良民, 李晓君, 仲红. VANET 中一种可撤销的车辆群组批认证方法[J]. 中国科学: 信息科学, 2013(10):1307-1325.
- [20] WANG L M, LI X J, ZHONG H. A revocable certification of vehicle group in VANET[J]. SCIENTIA SINICA Information, 2013(10): 1307-1325.
- [21] CHEN L, JIA X, MENG L, et al. Expedite privacy-preserving emergency communication scheme for VANET[J]. International Journal of Distributed Sensor Networks, 2013, 2013(1):59-72.
- [22] DAIMI K, SAED M, BONE S. A multi-level security architecture for vehicular Ad hoc network[J]. Lecture Notes in Engineering & Computer Science, 2014, 2211(1).
- [23] KUMAR P V, MAHESHWARI M. Prevention of Sybil attack and priority batch verification in VANET[C]// International Conference on Information Communication and Embedded Systems (ICICES). c2014:1-5.
- [24] 王良民. 主动反应与自再生的容忍入侵关键技术研究[D]. 西安电子科技大学, 2006.
- [25] WANG L M. Study on key technology of active reaction and self-reproducing tolerance[D]. Xidian University, 2006.
- [26] 王良民, 姜顺荣, 郭渊博. 物联网中移动 Sensor 节点漫游的组合安全认证协议[J]. 中国科学: 信息科学, 2012(07):815-830.
- [27] WANG L M, JIANG S R, GUO Y B. The secure authentication protocol of mobile sensomodes combination in IoT[J]. SCIENTIA

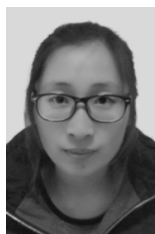
- SINICA Information, 2012(7):815-830.
- [23] 谢晴晴, 仲红, 王良民, 等. 一种基于云平台的车联网RSU数据查询验证方法:CN201410648782.X[P].2015-02-18.
XIE Q Q,ZHONG H,WANG L M,et al.A data query authentication method of internet of vehicles based on cloud platform: CN201410648782.X[P].2015-02-18.
- [24] IEEE. 1609.2-2013 - IEEE standard for wireless access in vehicular environments security services for applications and management messages[J]. IEEE, 2013:1-289.
- [25] Secure vehicular communication project[EB/OL]. <http://www.sevecom.org/>.
- [26] CAR 2 CAR communication consortium[EB/OL]. <http://www.car-2-car.org/>.
- [27] NOW-network on wheels project[EB/OL]. <http://www.network-on-wheels.de>.
- [28] Privacy enabled capability in cooperative systems and safety applications project[EB/OL]. <http://www.preciosa-project.org/>.
- [29] 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.
- [30] RABIEH K, MAHMOUD M M E A, GUO T N, et al. Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs[C]// International Conference on Communications (ICC). c2015.
- [31] RAYA M, AZIZ A, HUBAUX J P. Efficient secure aggregation in VANET[C]//International Workshop on Vehicular Ad hoc Networks. c2006:67-75.
- [32] CHIM T W, YIU S M, HUI L C K, et al. SPECS: secure and privacy enhancing communications schemes for VANET[J]. Ad hoc Networks, 2011,9(2):189-203.
- [33] WASEF A, SHEN X. EMAP: expedite message authentication protocol for vehicular Ad hoc networks[J]. IEEE Transaction on Mobile Computing, 2013,12(1):78-89.
- [34] 李晋国, 林亚平, 李睿, 等. 车载自组织网络中基于椭圆曲线零知识证明的匿名安全认证机制[J]. 通信学报, 2013(5):52-61.
LI J G, LIN Y P, LI R, et al. Automotive self-organizing networks based on the elliptic curve zero knowledge proof in the anonymous security authentication mechanism[J]. Journal on Communications, 2013(5):52-61.
- [35] ZHANG C, LU R, LIN X, et al. An efficient identity-based batch verification scheme for vehicular sensor networks[C]//IEEE INFOCOM. c2008: 246-250.
- [36] LU R, LIN X, ZHU H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[C]//IEEE INFOCOM. c2008: 1229-1237.
- [37] YANG J H, CHANG C C. An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem[J]. Computer & Security, 2009, 28(3/4): 138-143.
- [38] 刘唐, 汪小芬, 肖国镇. 基于无证书公钥的安全V2I通信协议[J]. 计算机科学, 2012, 39(9):20-23.
LIU T, WANG X F, XIAO G Z. Communication protocol of security V2I based on certificate less public key encryption[J]. Computer Science, 2012, 39(9):20-23.
- [39] HUANG J L, YEY LY, CHIEN H Y. ABAKA: an anonymous batch authenticated and key agreement scheme for value-added services in vehicular Ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2011,60(1):248-262.
- [40] SHIM K A. CPAS: an efficient conditional privacy-preserving authentication scheme for vehicular sensor networks[J]. IEEE Transactions on Vehicular Technology, 2012, 61(4):1874-1883.
- [41] LIU Y, WANG L, CHEN H. Message authentication using proxy vehicles in vehicular Ad hoc networks[J]. Vehicular Technology IEEE Transactions on, 2015, 64(8):3697-3710.
- [42] SUN Y, LU R, LIN X, et al. An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications[J]. IEEE Transactions on Vehicular Technology, 2010, 59(7):3589-3603.
- [43] ZHU X, JIANG S, WANG L, et al. Efficient privacy-preserving authentication for vehicular Ad hoc networks[J]. IEEE Transactions on Vehicular Technology, 2014, 63(2):907-919.
- [44] 王良民, 刘晓龙, 陈龙, 等. 一种面向 5G 车联网的可多网接入 OBU 系统:CN201521014778.4[P].2015-12-09.
WANG L M,LIU X L,CHEN L, et al. A multi-access network OBU system oriented 5G IoV:CN201521014778.4[P].2015-12-09.
- [45] GROVER J, GAUR M S, LAXMI V, et al. A sybil attack detection approach using neighboring vehicles in VANET[C]//The 4th International Conference on Security of Information and Networks. c2011: 151-158.
- [46] ABBAS S, MERABTI M, LLEWELLYN-JONES D. Lightweight sybil attack detection in MANET[J]. IEEE Systems Journal, 2013, 7(2):236-248.
- [47] YAN G, BISTA B B, RAWAT D B, et al. General active position detectors protect VANET security[C]//International Conference on Broadband and Wireless Computing, Communication and Applications (BWCCA).c2011:11-17.
- [48] YU B, XU C Z, XIAO B. Detecting sybil attacks in VANETs[J]. Journal of Parallel and Distributed Computing, 2013, 73(6): 746-756.
- [49] CHEN C, WANG X, HAN W L, et al. A robust detection of the sybil attack in urban VANETs[C]//The 29th IEEE International Conference on Distributed Computing Systems Workshops (ICDCS Workshops '09).c2009:270-276.
- [50] PARK S, ASLAM B, TURGUT D, et al. Defense against sybil attack in vehicular Ad hoc network based on roadside unit support[C]// Military Communications Conference (MILCOM 2009). c2009:1-7.
- [51] GROVER J, GAUR M S, LAXMI V. A novel defense mechanism against sybil attacks in VANET[C]//The 3rd International Conference on Security of Information and Networks.c2010:249-255.
- [52] CHANG S, QI Y, ZHU H, et al. Footprint: detecting sybil attacks in urban vehicular networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2012, 23(6):1103-1114.
- [53] STUDER A, SHI E, BAI F, et al. TACKing together efficient authentication, revocation, and privacy in VANET[C]//The 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad hoc Communications and Networks (SECON'09). c2009: 1-9.
- [54] ZHOU T, CHOUDHURY R R, NING P, et al. P2DAP-sybil attacks detection in vehicular Ad hoc networks[J].IEEE Journal on Selected Areas in Communications, 2011, 29(3):582-594.
- [55] XIA F, CHUN Y L, CHEN D X, et al. A method for defending against multi-source Sybil attacks in VANET[J]. Peer-to-Peer Networking and Applications, 2016,29(1):1-10.
- [56] 张建明, 赵玉娟, 江浩斌, 等. 车辆自组网的位置隐私保护技术研究[J]. 通信学报, 2012, 33(8):180-189.

- ZHANG J M, ZHAO Y J, JIANG H B, et al. Study on location privacy protection technology of VANET[J]. Journal on Communications, 2012, 33(8):180-189.
- [57] BUTTYÁN L, HOLCZER T, VAJDA I. On the effectiveness of changing pseudonyms to provide location privacy in VANET[C]//Conference on ESAS. c2007:129-141.
- [58] BUTTYÁN L, HOLCZER T, WEIMERSKIRCH A, et al. Slow: a practical pseudonym changing scheme for location privacy in VANET[C]//IEEE Vehicular Networking Conference (VNC). c2009:1-8.
- [59] FREUDIGER J, RAYA M, FLEGYHZI M, et al. Mix-zone for location privacy in vehicular networks[C]// The 1st International Workshop on Wireless Networking for Intelligent Transportation Systems (WiN-ITS'07).c2007:1-7.
- [60] SCHEUER F, FUCHS K P, FEDERRATH H. A safety-preserving mix zone for VANET[C]//The 8th International Conference on Trust, Privacy and Security in Digital Business. c2011: 37-48.
- [61] ZHANG J, MA L, SU W, et al. Privacy-preserving authentication based on short group signature in vehicular networks[C]// Conference on ISDPE . c2007:138-142.
- [62] LIN X, SUN X, HO P H, et al. GSIS: a secure and privacy-preserving protocol for vehicular communications[J]. IEEE Transactions Vehicular Technology, 2007,56(6):3442-3456.
- [63] LU R, LIN X, ZHU H, et al. ECPP: efficient conditional privacy preservation protocol for secure vehicular communications[C]// Conference on IEEE INFOCOM.c2008:1229-1237.
- [64] CHAURASIA B K, VERMA S. Conditional privacy through ring signature in vehicular Ad-hoc networks[M]. In Transactions on Computational Science XIII, Berlin: Springer, 2011:147-156.
- [65] HOH B, GRUTESER M, XIONG H, et al. Preserving privacy in GPS traces via uncertainty-aware path cloaking[C]// The 14th ACM Conference on Computer and Communications Security. c2007: 161-171.
- [66] WASEF A, SHEN X. REP: location privacy for VANETs using random encryption periods[J]. Mobile Networks and Applications, 2010,15(1):172-185.
- [67] SAMPIGETHAYA K, LI M, HUANG L, et al. Amoeba: robust location privacy scheme for VANET[J]. IEEE Journal on Selected Areas in Communications, 2007, 25(8): 1569-1589.
- [68] LIU J, AU M, SUSILO W, et al. Linkable ring signature with unconditional anonymity[J]. IEEE Transactions on Knowledge and Data Engineering, 2014,26(1): 157-165.
- [69] LIN X, LI X. Achieving efficient cooperative message authentication in vehicular Ad-hoc networks[J]. IEEE Transactions on Vehicular Technology,2013, 62(7):3339-3348.
- [70] HORNG S J, TZENG S F, PAN Y, et al. B-SPECS+: batch verification for secure pseudonymous authentication in VANET[J]. IEEE Transactions on Information Forensics and Security, 2013,8(11): 1860-1875.
- [71] LEE B K, JEONG E H, JUNG I. A DTSA (detection technique against a Sybil attack) protocol using SKC (session key based certificate) on VANET[J]. International Journal of Security and Its Applications, 2013,7(3):1-10.
- [72] FRANCESCO M, CHIASERINI C F, CASETTI C, et al. A-VIP: anonymous verification and inference of positions in vehicular networks[C]// IEEE INFOCOM Mini Conference.c2013:105-109.
- [73] TIMPNER J, SCHÜRMANN D, WOLF L. Secure smart phone-based registration and key deployment for vehicle-to-cloud communications[C]// The 2013 ACM workshop on Security, privacy & dependability for cyber vehicles.c2013: 31-36.
- [74] SHIVALDOVA V, SEPULCRE M, WINKELBAUER A, et al. A model for vehicle-to-infrastructure communications in urban environments[C]// IEEE International Conference on Communication Workshop (ICCW).c2015:2387-2392.
- [75] PHAN-HUY D, STERNAD M, SVENSSON T. Making 5G adaptive antennas work for very fast moving vehicles[J]. Intelligent Transportation Systems Magazine, 2015, 7(2): 71-84.
- [76] ZHENG X, CHEN W, WANG P. Big data for social transportation[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 99:1-11.
- [77] QIAO J, SHEN X M, MARK J, et al. Enabling device-to-device communications in millimeter-wave 5G cellular networks[J]. IEEE Communications Magazine, 2015, 53(1): 209-215.
- [78] MUMTAZ S, SAIDULHUP K M, ASHRAF M L, et al. Cognitive vehicular communication for 5G[J]. IEEE Communications Magazine, 2015, 53(7): 109-117.
- [79] ZHU F, GAO F, ZHANG T, et al. Physical-layer security for full duplex communications with self-interference mitigation[J]. IEEE Transactions on Wireless Communications, 2015:1.
- [80] MUKHERJEE A, FAKOORIAN SA, HUANG J, et al. Principles of physical layer security in multiuser wireless networks: a survey[J]. IEEE Communication Surveys and Tutorials, 2014,16(3): 1550-1573.

作者简介:



王良民(1977-), 男, 安徽潜山人, 江苏大学教授、博士生导师, 主要研究方向为密码学与安全协议、物联网安全、大数据安全。



李婷婷(1993-), 女, 江苏南通人, 江苏大学本科生, 主要研究方向为车联网安全与隐私保护。



陈龙(1958-), 男, 江苏靖江人, 江苏大学教授、博士生导师, 主要研究方向为车辆动态性能、交通安全与管理等。