5G 时代车联网信息物理融合系统综合安全研究

马小博^{1,2}, 彭嘉豪^{1,2}, 薛磊³, 管晓宏^{1,2*}

1. 西安交通大学电子与信息学部, 西安 710049

2. 西安交通大学智能网络与网络安全教育部重点实验室, 西安 710049

3. 香港理工大学计算学系, 香港 999077

* 通信作者. E-mail: xhguan@xjtu.edu.cn

收稿日期: 2019-08-21; 接受日期: 2019-10-08; 网络出版日期: 2019-12-13

国家重点研发计划 (批准号: 2016YFB0901900) 和国家自然科学基金 (批准号: U1736205, U1766215, 61972313) 资助项目

摘要 近年来, 重庆公交坠江、无锡重型卡车超载致高架坍塌等一系列重特大灾难性事故的发生暴露了信息化时代交通工具运行中安全防范与应急处置机制的严重缺失. 5G 通信时代的来临, 无疑为这一问题的解决带来了巨大历史机遇. 本文针对交通工具运行中预防重特大事故及取证分析的需求, 基于 5G 通信技术, 提出基于事件的交通工具运行中信息物理融合安全治理框架. 该框架围绕交通工具运行安全问题的特性——“高速运动状态下网络资源的可用性、信息物理融合下安全目标的复杂性”, 通过精准感知物理层、通信层、社会层 3 个层面的不安全事件, 综合利用泛在智能感知、边缘-云计算等技术, 从交通工具的物理设备信息安全、车辆状态安全、车辆环境安全、网络安全 4 个维度, 构建一体化的交通工具智能安全应对方案, 服务于“事前全时预判、事中即时报警、事后回放取证”的安全目标.

关键词 5G, 车联网, 信息物理融合系统, 综合安全, 事件驱动

1 引言

安全是交通发展的永恒问题. 根据世界卫生组织统计, 2016 年全球有约 135 万人死于道路交通事故, 在所有导致死亡的因素中排名第 8. 交通事故也是导致 5~29 岁人群死亡最主要的原因^[1]. 中国的交通安全状况虽在逐年改善, 但据国家统计局的数据, 2017 年中国仍发生 203049 起交通事故, 造成 63772 人死亡, 209654 人受伤, 直接财产损失达到 121311.3 万元. 截至到 2017 年底, 我国铁路运输业就业人员数 1848032 人, 道路运输业就业人员数 3846122 人, 水上运输业就业人员数 441227 人, 航空运输业就业人员数 624318 人, 民用载客汽车 18469 万辆, 民用载货汽车 2338 万辆, 交通运输业客运量总计 1848620 万人, 大量交通运输业就业人员和旅客的安全需要保障^[2].

引用格式: 马小博, 彭嘉豪, 薛磊, 等. 5G 时代车联网信息物理融合系统综合安全研究. 中国科学: 信息科学, 2019, 49: 1640–1658, doi: 10.1360/SSI-2019-0176
Ma X B, Peng J H, Xue L, et al. Integrated security of cyber-physical vehicle networked systems in the age of 5G (in Chinese). Sci Sin Inform, 2019, 49: 1640–1658, doi: 10.1360/SSI-2019-0176

近年来,公交车、出租车、网约车、火车、轮船、飞机等交通工具所承载的移动公共区域重大安全事件不断发生.典型案例包括重庆公交坠江、无锡重型卡车超载致高架坍塌、空姐乘滴滴遇害、长江邮轮侧翻、马航失联等.党的十八大报告强调“要深化平安建设,完善立体化社会治安防控体系”.在十八大报告指引下,以公共安全视频监控联网应用为重点的群众性治安防控工程“雪亮工程”应运而生、蓬勃发展.自2016年,“雪亮工程”的应用已遍布全国,极大地促进了社会治安防控体系,提高了整体社会安全监控效能.“雪亮工程”主要基于可靠稳定的有线高速宽带网络,通过大规模网格化部署高清摄像头,监控城区、郊区及乡镇等固定公共区域的安全,基本实现“全域覆盖、全网共享、全时可用、全程可控”的目标.然而,针对交通工具所承载的移动公共区域的安全监控,由于信号覆盖、可用带宽等客观因素的制约,可实现性受到极大限制.这使得移动公共区域发生重大交通、治安、刑事,甚至恐怖袭击等案件后,难以在第一时间开展高效的取证分析,且存在车载数字证据无法恢复、损毁、丢失等不可预期的巨大风险.

交通工具所承载的移动公共区域的安全监控问题,表面上属于社会公共安全管理领域,但其本质上涵盖了信息物理融合系统的综合安全问题.一方面,该问题涵盖车辆终端、路基边缘端 (roadside unit)、车联云端等各种设施的信息系统安全,涉及车辆控制系统、总线系统、舒适系统、娱乐系统、视频监控系統、边缘信息系统、云端信息系统等各种信息系统的的社会安全问题.信息系统的不安全,如被攻击者远程控制,则会引起不可预期的安全风险.另一方面,该问题涵盖车辆设备状态、车内空间司乘行为、车辆周围路况环境等物理系统的安全问题.物理系统的不安全,如车辆设备失效、司乘争抢方向盘等,将直接引发安全事故.因此,交通工具所承载的移动公共区域的安全监控问题,是典型的信息物理融合系统的综合安全问题.信息系统不仅要保障自身安全的能力,更要能够感知、预警物理系统的安全问题.物理系统的安全,反过来从底层进一步支撑信息系统的安全.

当前,针对交通工具所承载的移动公共区域的安全监控,研究相应的信息物理融合系统的综合安全问题,面临以下挑战:

- 安全监控网络化程度低,以本地记录为主、网络传输为辅.虽然现有车辆通过安装车载 Telematics BOX (T-BOX)、行车记录仪等方式,可实现车辆信息的远程监视与控制,但这些功能的设计主要以方便用户对车辆的管理为主,并未针对信息系统及物理系统的网络化安全监控做专门的设计.例如,在重庆公交坠江事件中,存储在车辆本地的视频数据黑匣子在坠江长达63小时之后才通过打捞得以恢复,缺乏网络传输监控数据和报警数据的机制.

- 缺乏系统性网络资源的优化与调度设计,难以大规模扩展.现有车辆远程监控,主要通过物联网卡回传数据,但受限于传输速度,只能传输小规模数据.在现有的网络传输条件下,难以支持大量车辆并发实时回传大规模数据 (如高清视频),供事后根据需要进行安全取证分析.因此,在大规模车辆,尤其是公共交通工具,部署安全监控设施,必须系统性地网络资源优化与调度设计,从而保障安全监控的大规模实时性.例如,可根据车辆的各种状态、所处位置、视频内容等多种信息动态调整车辆回传数据的采样率、解析度等指标,以及动态选择路基边缘设施进行高速数据卸载 (data offloading).通过向附近边缘设施进行高速数据卸载,可有效规避类似重庆公交坠江后数据靠打捞才能恢复的事件.

- 简单车载数据记录,缺乏智能化安全策略,无法主动规避风险.现有车辆安全监控,以简单车载记录为主.例如,现有行车记录仪大多只配置了简单的急刹车时本地快速存储功能,缺乏系统性、智能化的柔性安全策略.又如,在长江邮轮侧翻事件中,可通过融合重力传感器、加速传感器、陀螺仪等运动传感器的实时数据,对超载等可能导致的侧翻,做出风险评估和预警,并根据不同的风险等级,自适应调整监控数据回传的采样频率和解析度.而在重庆公交坠江事故中,也未能利用视频数据检测司乘斗殴行为,利用传感器数据感知车辆异常变道行为、车辆自由落体行为等并进行网络化报警,基于检测

到的各种异常物理行为, 对车辆进行远程控制 (如及时制动), 预防安全灾难发生更是无从谈起。

受限于上述现实挑战, 由于缺乏系统化整体设计、网络化高效传输、智能化实时决策, 相比固定区域安全监控, 交通工具所承载的移动公共区域的信息物理融合系统的综合安全监控, 当前监控效果不容乐观。随着人们出行频次及方式的增多, 移动公共区域安全监控的重要性日益凸显, 移动公共区域安全监控相关技术革新及应用部署迫在眉睫。

5G 通信时代的来临, 将为交通工具所承载的移动公共区域的信息物理融合系统的综合安全监控带来巨大的机遇。5G 无线网络将支持连接 1000 亿台设备, 每台设备拥有 10 Gb/s 的数据速率, 以及超低的时延和响应时间。在 2020 ~ 2030 年之间, 5G 网络将会大量部署^[3,4]。5G 网络的发展将极大地推动万物互联, 催生 Internet of Things (IoT) 设备的发展及 IoT 应用的部署, IoT 的发展将促使越来越多的移动设备之间交流信息, 为社会的发展带来巨大的改变, IoT 的发展尤其对车联网信息物理融合系统的发展有极大的推动作用^[5]。车联网已被华为连同智能制造、全球物流跟踪, 一并列入 5G 在 IoT 垂直行业的首要切入领域^[6]。

本文将基于 5G 技术和车联网信息物理融合系统技术, 提出并探讨基于事件的交通工具运行信息物理融合综合安全治理框架。该框架考虑了网络资源的可用性、物理设备信息安全、车辆状态安全、车辆环境安全、网络安全等问题, 从物理设备信息安全、车辆状态安全、车辆环境安全、网络安全等方面讨论了车联网信息物理融合系统的综合安全问题, 构建系统化的车联网信息物理融合综合安全体系。本文提出的车联网信息物理融合系统综合安全体系, 通过精准感知物理层、通信层、社会层 3 个层面的安全事件, 有助于构建一体化的交通工具运行智能安全应对方案, 精准做到“事前全时预判、事中即时报警、事后回放取证”的安全目标, 解决信息化时代交通工具安全防范与应急处置机制的严重缺失等问题。该体系的应用将借助网络化、信息化手段, 通过信息物理系统融合, 开展自动化、智能化的安全监控与策略制定, 有望从根本上降低车联网信息系统安全风险、减少交通安全事故的发生、减少人员伤亡和经济损失、减少不良舆情及不必要的社会恐慌。

2 5G 时代车联网信息物理融合系统综合安全研究框架

车联网信息物理融合系统综合安全研究框架涵盖物理设备信息安全、车辆状态安全、车辆环境安全、网络安全问题, 从这 4 个方面考虑构建完整的车联网信息物理融合系统安全体系, 精准感知物理层、通信层、社会层 3 个层面的安全事件, 构建一体化的交通工具智能安全应对方案。基于各种安全问题与对策, 本文构架了车联网信息物理融合系统综合安全框架如图 1 所示。

本框架自底向上包含事件感知、网络部署、智能决策 3 个层次。事件感知的主要目的是部署车载全息智能传感设备, 从车辆状态安全、车辆环境安全、信息系统安全 3 个方面, 精准感知物理层、通信层、社会层等多个层面的安全事件。在事件感知的基础上, 将全息智能传感设备规模化部署, 并依据网络带宽的可用性及路况等环境因素, 部署路侧网络通信边缘设施、云端网络通信基础设施等, 构建边缘-云结合的网络化安全监控系统。为了能够最大化监控绩效, 在大规模部署的基础上, 进一步为安全监控引入智能决策。解决基于事件的自适应采样频率数据码率、环境感知的通道选择与路侧设施部署、事件分级机制下的数据存储和处理取证、终端即时判定与云端及时判定相结合的异常事件检测等关键科学问题, 为综合安全监控的绩效最大化打造智能化引擎。

本文所提框架的特色在于 3 个方面。一是综合安全感知, 紧密结合车联网的自身特点, 将传统信息安全, 扩展至信息物理融合系统的综合安全。二是基于边缘-云结合的网络部署方式, 提出事件与数据分离的系统设计思路, 其基本目标是通过将安全事件的实时报警与大规模数据的传输存储进行解

图 1 (网络版彩图) 车联网信息物理融合系统综合安全框架

Figure 1 (Color online) Integrated security framework for cyber-physical vehicle networked systems

耦, 实现事件实时报警和大规模数据传输存储的双重目标. 通过基于边缘-云结合的多通道网络传输方式, 根据交通工具的动态轨迹以及沿路固定基础设施提供的可用 4G/5G 基站、WiFi 热点, 优化和动态调整不同交通工具数据卸载的时间和地点, 对所记录的重要视频进行适时的卸载备份, 以补充传统移动网络基站所提供的有限传输带宽. 例如, 针对重庆公交坠江案例, 可通过全息智能传感设备, 在检测到车辆异常运动状态 (如激烈变道、急速坠落) 后, 在实时向云端推送微小数据量报警信息的同时, 将大规模的高清视频及车辆运行等数据卸载到桥边的边缘基础设施中, 既保证了实时报警, 又同时完整备份现场高清视频及车辆运行等数据. 三是基于事件的智能策略. 智能数据采集策略模块负责在网络信号覆盖、可用带宽资源有限的情况下, 通过全息智能传感设备的数据分析, 实时预测和检测车辆异常事件, 自动调整各类传感数据的采样频率及解析度等监控指标. 考虑不同地理位置和时间的治安事件发生的概率, 以及引发安全事件的危害与成本博弈分析, 策略性随机化不同基础设施和车载智能终端的网络带宽和资源分配调度, 使得在有限监控资源下, 能让不同时间、地点及交通工具的监控重点随着环境改变并有针对性地做出智能性的优化调整.

另外, 在所提框架下, 数据高速存储检索也至关重要. 由于车辆在大规模联网后, 存储和数据处理资源不可能无限制增加, 因此非常有必要根据车辆行为及相关安全事件数据, 对监控数据进行分级存储, 提供多种属性的快速检索服务, 以便于事后深入取证和分析. 例如, 可基于检测到的事件, 判断为重要性高的监控数据, 进行高解析度无压缩捕获存储; 判断为重要性相对低的监控数据, 可进行低解析度压缩捕获存储. 最后, 基于数据统计取证分析, 为安全监控提供数据统计、数据取证、热点事件检测报警等功能.

3 车联网信息物理融合综合安全事件感知

图 2 所示为车联网信息物理融合安全事件感知指标体系, 涵盖车辆状态安全事件感知、车辆环境

图 2 (网络版彩图) 车联网信息物理融合安全事件测度体系

Figure 2 (Color online) Security event perception metrics for cyber-physical vehicle networked systems

安全事件感知、信息系统安全事件感知 3 个大类, 分别从车辆内因、环境外因、网络通信 3 个方面, 对各种安全事件进行感知。

3.1 车辆状态安全事件感知

Chen 等^[7]通过车辆上手机的加速度传感器、方向传感器, 结合 SVM (support vector machine) 算法, 可以识别出车辆是否处在蛇形、急转、侧滑、快速掉头、大幅转弯、急刹等异常驾驶状态。通过智能手机上的加速度传感器, 结合车辆实时 GPS 信息, 可以判断车辆是否有坠崖、坠江等不安全状态^[8]。通过摄像头追踪并动态分析车辆行驶轨迹, 可以对车辆轨迹进行建模, 帮助判断车辆是否有穿越双黄线、360 度转圈等异常驾驶行为, 还能对车辆轨迹进行预测, 结合车辆环境, 可以判断车辆是否会出现不安全的状态, 如对车辆碰撞进行预测^[9]。Zaldivar 等^[10]使用手机的加速度传感器、车内安全气囊触发器判断车辆状态和是否发生事故。

车辆可通过车载自诊断系统 (on-board diagnostics, OBD) 检测出车门的状态、发动机转速 (revolutions per minute, RPM) 等信息以判断车辆状态, 并结合车辆速度、加速度等行驶状态信息判断车辆状态安全^[11]。车辆也能够基于车辆的运行状态参数, 估计和检测如刹车片老化程度、轮胎的磨损程度等车辆设备老化情况, 对车辆动力系统、驾驶系统、方向系统、悬挂系统、通信系统和传感器系统进行实时检测。

3.2 车辆环境安全事件感知

不同于传统的其他领域物联网安全问题, 车辆的移动性决定了车辆环境安全至关重要。例如, 司机的精神状态是非常重要的安全因素, 车联网综合安全监控系统应能检测出司机是否疲劳驾驶、危险驾驶。司机驾驶行为可以通过视频传感器、语音传感器、运动传感器进行检测。例如, 通过司机面部表情判断司机是否可能会有疲劳、酒后、吸毒等危险驾驶行为^[12], 对司机眨眼行为的检测可以帮助判断司机是否疲劳^[13], 还可以对司机未来的驾驶行为进行预测^[14]。可以通过驾驶行为^[15]、脉搏^[16]、人脸识别^[17]等方法判断司机身份, 如果同一司机驾驶时间过长, 或某一时间段内驾驶时间过长, 应具有自动安全预警功能。如果发现司机存在疲劳驾驶或危险驾驶行为, 可以实时向司机发出提醒或警告, 也可以同时向周围车辆发送警告消息, 保证周围车辆行驶安全。

通过车内摄像头视频捕捉,可以判断车内是否有抢夺方向盘、斗殴、开枪射击、暴恐等危险行为^[18],如果检测出极端危险行为,可使用远程自动停车技术强制停车,上传危险行为监控数据,如果检测到车内出现明火、烟雾、毒气等危险物品或事件,也应及时判定预警。

对于行驶中的车辆,前方车辆减速、急刹车、视野盲区出现车辆等外在威胁可能会影响车辆安全,综合安全监控系统应将这些构成威胁的信息及时通知给受威胁的车辆。车辆对周围车辆的行驶状态监测可以帮助车辆更加安全地行驶,通过车载摄像头^[19]、道路上的传感器检测其他车辆的行驶状态。车辆之间的通信可以辅助预防事故,警告车辆其运动的外在威胁^[20]。如果车辆之间能够互相发送关于交通拥堵、路况等信息,或在道路边部署传感器检测交通状态并及时通知车辆,也能提高交通效率。但要设计消息的认证机制,防止因为恶意节点发送的虚假信息,导致严重的交通事故^[21]。

车辆应能监测实时天气情况,给司机提供驾驶建议和帮助。例如,使用车载摄像头监测是否下雨^[22],在雨天对交通信号灯的可视性估计^[23],在低可视环境下对交通信号灯进行识别^[24],使用车载摄像头和雷达在雾天对雾的浓度和可见度进行识别^[25]。如果检测到能见度过低或天气过于恶劣,应辅助司机将车速、车距等车辆状态控制在安全范围内。

利用车载摄像头和激光检测车道,尤其对于不规则的道路,应能快速识别出车道、可驾驶区域等重要信息。同时,车载路况检测系统还要能检测最适合驾驶的区域,为车辆提供最舒适的驾驶路线建议^[26]。利用车载加速度传感器和 GPS 等传感器,可以识别道路的坑洼地带^[27],判断道路粗糙程度^[28],检测周围是否有悬崖等危险路段。加速度传感器、GPS 传感器、麦克风等传感器也可以帮助检测坑洼等路况信息^[29,30]。如果车辆行驶在陡坡、急转弯、江河湖泊边、桥梁、事故多发地点等位置时,需要提高对监控数据的采样频率和分析粒度,确保安全事件信息实时上传到云端,重要的取证数据及时卸载到路侧网络通信基础设施^[31]。

在各类环境因素中,行人往往更易受到交通事故伤害。因此,在车辆行驶过程中,车辆应能实时检测行人、追踪行人运动、预测行人运动轨迹。如果检测到行人安全可能受到威胁,应及时向威胁行人安全的司机汇报,必要时可辅助司机降低车速、调整车辆行驶状态,进入安全驾驶状态^[32,33]。车联网信息物理融合系统中,如果车辆出现危险状况,应及时向行人、非机动车使用者等可能受威胁的人汇报,行人也可实时向车辆汇报自己的位置速度等信息,行人和车辆的信息交流有助于保证邻近区域交通系统中所有人的安全^[34~36]。

3.3 信息系统安全事件感知

车联网相关的信息系统,其安全性涉及硬件、固件、软件、网络等多个方面。首先,为了控制车辆硬件潜在的安全风险漏洞,需要开发设计安全的处理器。攻击者可能攻击车辆的任何电子控制单元(electronic control unit, ECU),从而控制车辆或让驾驶员的操作失灵,其攻击方法包括使刹车失灵、使发动机失灵、让某个轮胎刹车、切断车辆与外界的联系、打开车窗等方法^[37],可能导致严重的交通安全问题。对于不同种类的处理器,应根据处理器的用途和安全威胁对处理器进行分类,从而进行不同程度的保护。安全处理器带来的安全环境对于安全敏感操作至关重要,如密钥生成、管理和存储,防止对系统安全密码的非授权获取、防止对系统信息的非授权解密、防止对系统信息的非授权篡改等安全问题,都会因为安全处理器获得保障,在底层防止信息泄漏^[38,39]。安全的处理器在考虑安全性的同时,也要考虑处理的效率和复杂性等问题。

随着车联网技术的发展,车辆会开放蓝牙、蜂窝网络、GPS、Wi-Fi 等接口,由于 CAN (controller area network) bus 系统缺乏对信息的机密性、真实性、有效性、完整性保护,可能导致攻击者通过 CAN bus 系统进行攻击^[40~44],研究者已经证明攻击者可以通过蓝牙或蜂窝网络完全控制车辆的 CAN bus

系统, 进而控制整个车辆^[45], 还可以通过 DoS 攻击阻止车内网络正常通信^[41]. 攻击者还有可能通过窃听记录车辆的行驶信息, 暴露乘客的个人隐私^[46]. 所以对于 CAN bus 系统需要一定的验证和检验机制来保证车辆系统的安全, 能分类出正常和恶意的 CAN bus 信息^[47, 48], 能对抗针对 CAN bus 系统的攻击^[49~51], 同时因为车辆的处理器计算能力有限, 车辆 CAN bus 自检系统需要轻量化的设计^[52]. 通过收集 CAN bus 系统和车内网络的信息, 可帮助定位车辆安全问题, 实现车辆安全问题自检^[53, 54].

车联网信息物理融合系统需要依靠大量传感器获取车辆位置、速度、加速度、内外部环境安全等信息感知车辆运行状态, 帮助车辆进行导航、驾驶援助、安全状态管理等功能, 传感器安全对于车联网信息物理融合系统至关重要^[55]. 车内部署的雷达、光学雷达、超声波传感器、视频摄像头等传感器在为车辆带来驾驶援助的同时, 也为车辆安全带来了安全威胁, 如致盲、干扰、重放、欺骗等攻击都会给车辆带来巨大的威胁^[56, 57]. 攻击者还有可能使用虚假的或带有诱骗性的交通标志, 传感器应能识别出虚假的交通信息, 避免被攻击者诱骗, 保证车辆安全^[58].

目前汽车厂商推出越来越多的电动汽车, 人们也在购买越来越多的电动汽车, 电动汽车的电池安全问题也是近年来关注的重点. 电动汽车的电池管理系统 (battery management system, BMS) 可以管理电池的电压、电流、温度等特征, 因此安全的电池管理系统对车联网信息物理融合系统十分重要^[59, 60]. 如果攻击者控制了电池管理系统, 就可以控制对于电池的所有操作, 可能的攻击方法包括用巨大的电压电流毁坏电池、忽略电池处于危险状态、未经允许点火启动车辆等, 电池管理系统还要能够鉴别劣质伪造电池, 防止伪造电池影响车辆安全^[60]. 电动汽车在充电过程中可能与充电桩进行信息交互, 必须防止攻击者通过窃听、拦截、篡改信息、注入病毒等方法, 通过充电桩向车辆电池管理系统或其他车内设备进行攻击^[61, 62].

当前, 许多地区已借助无线网络部署了智能无线交通管理系统^[63, 64]. 在车联网信息物理融合系统中, 会使用智能交通灯、智能路标、智能道路交通标线等技术, 虽然这些技术为实时监控和动态交通管理提供了便利, 但是需要保证这些技术的安全, 防止被攻击者攻击导致道路交通出现安全威胁^[65]. 攻击者可能侵入智能交通管理系统的网络, 从而发起拒绝服务、控制交通灯等攻击, 加强无线安全管理、设置防火墙、固件定期升级、加强安全认证都是必要的安全管理措施^[66, 67]. 交通信号应与车辆之间建立完善的双向认证机制, 避免被攻击者使用虚假的或带有诱骗性的交通标志影响车联网系统的安全^[58].

车载移动终端是车联网的载体和入口. 即使是未预装移动终端系统的车辆, 用户也往往会选择后装移动终端使车与网络相连. 车辆与车辆的使用者可以通过移动终端进行通信来传递关于车辆安全、娱乐系统、车辆状态等信息, 车辆使用者也可以通过移动终端上的移动应用软件来控制车辆. 车载移动终端在提供便利的同时, 它的安全问题也变得越来越重要^[68]. 移动终端的安全防护, 可以从终端操作系统、应用软件、网络连接和软件更新 4 个主要方面来考虑.

3.3.1 车载终端操作系统安全

目前, 国际上比较流行的车载终端操作系统有苹果的 Carplay、谷歌的 Android Auto、微软的 Windows in the Car 及黑莓的 QNX. 它们的目的是将现有的便携式硬件设备通过特定的通信协议与汽车相连接, 让用户可以方便地使用车载的屏幕、话筒、音响等设备, 并适时了解汽车状态和控制汽车的某些功能. 这些车载终端操作系统面临着传统嵌入式操作系统所面临的安全问题, 包括系统启动、资源管理、安全防护、安全审计等.

传统的嵌入式设备通常允许用户安装自定义的 ROM, 如果终端启动了被恶意修改过的操作系统, 将会对行车安全带来难以预估的威胁. 例如, 攻击者可通过反编译或重新打包安卓应用的方式, 影响

车联网安卓应用的安全^[69], 为此, 需要终端设备能够在启动操作系统之前, 对操作系统的完整性和安全性进行校验, 实现操作系统的安全启动^[70]. 权限管理在车载操作系统中也至关重要, 如果缺乏良好的权限管理机制, 敏感数据往往会被不该获取的应用程序获取, 带来敏感数据和用户隐私泄露的问题, 进一步威胁行车安全^[69]. 车载终端可以采用合理的权限管理机制管理不同应用程序的访问权限, 利用基于硬件的可信执行环境 (trusted execution environment, TEE) 对敏感数据进行隔离, 同时利用安全元件 (SE 芯片) 进行安全运算 (如数据加解密和身份认证).

车载操作系统难免存在软件漏洞, 这些漏洞可能会被攻击者利用进而对汽车进行远程控制攻击^[42,43]. 攻击者还可利用现有的安卓漏洞, 进行隐私窃取、用户通信监听、DDoS 等攻击^[71]. 为了保证车载终端的安全性, 终端操作系统需要采用必要的安全防护机制, 如及时更新系统, 对发现的漏洞进行打补丁等. 此外, 为了及时发现车载终端潜在的安全问题, 及在安全问题发生时快速定位问题产生的原因, 车载终端操作系统需要有完整的安全审计机制, 能够对系统发生的重要事件进行日志记录, 对记录进行可靠保存和上传备份. 另外, 系统能够根据日志记录, 对车载终端的安全状态进行评估, 在特定事件发生时能够及时根据日志定位事件原因.

3.3.2 车载应用软件安全

车载终端相关的应用软件既包括直接运行在车载终端上的应用程序, 同时也包括与车辆监控相关的手机应用程序. 应用程序的安全首先涉及到程序来源的安全, 目前的手机应用程序主要来源于 Google Play, Apple Store, 华为应用市场等几大应用市场. 由于近年来应用市场都对提供的应用程序采用了有效的安全检测和管理机制, 因此手机应用程序来源的安全性得到了有效保证. 然而, 车载终端应用程序目前还没有权威的应用市场, 往往由车厂提供, 其来源还存在很大的不可靠性^[72]. 车载终端应用程序安全主要涉及应用软件的隐私管理、病毒防护、权限管理等问题^[73,74], 同时, 要特别注意调用第三方库过程中的安全问题, 验证第三方库是否会带来新的安全性问题^[75]. 应用程序之间的通信有可能泄露重要信息, 如泄露用户隐私^[76], 应注意对应用软件之间通信的管理, 防止信息或权限泄露.

车载终端上的应用程序既与汽车内部 CAN 网络相连又与外部网络相连, 手机终端上的应用程序也可以通过车载终端向汽车 CAN 网络发送特殊请求, 因此, 攻击者会通过逆向分析这些应用程序寻找信息和漏洞侵入汽车 CAN 网络, 对汽车进行远程控制攻击^[77]. 此外, 攻击者也可通过对应用程序进行重打包插入恶意代码来实现攻击目的^[69,78]. 应用程序的安全可以从多种策略进行防护^[71]. 例如, 应用程序开发过程中使用安全的第三方库; 不要在代码中包含加密密钥等敏感信息; 在使用敏感数据时要对数据进行校验 (如加密数字证书); 对于敏感操作, 要实现在 Native 模块中增加逆向难度; 应用程序发布之前要对代码进行混淆和加固, 然后通过安全渠道进行发布.

3.3.3 车辆通信安全

车载网络包括外部网络与汽车内部 CAN 网络, 两种网络没有采取相应的安全防护机制, 都存在潜在的攻击风险. 对于外部网络, 车载终端可以直接通过 WiFi 或者 3/4/5G 与之相连, 也可通过蓝牙与手机相连后利用手机的网络与外部网络相连. 当终端设备直接与互联网相连时, 攻击者可以通过假基站或者伪造的 WiFi 热点来欺骗终端连接从而进行中间人攻击. 当车载终端通过手机网络连接外部网络时, 攻击者既可以使用恶意的应用程序与车载终端相连, 也可以通过侦听蓝牙通信获取敏感信息, 从而进一步实施攻击. 因此, 不安全的外部网络连接既可能被攻击者侦听造成敏感信息泄露, 也可能被利用来实施中间人攻击^[79].

为了确保外部网络通信安全,车厂可以从以下几个方面对外部通信进行安全防护^[80]。如果车载设备与后台服务器直接通过网络相连,通信需要采取端到端的加密方式以保证信息不被泄漏,同时,车载设备与后台服务器要进行双向认证,以防止通信的任何一端被仿冒。如果车载设备通过手机网络与后台服务器相连,手机与车载终端设备要采用安全的蓝牙协议通信,如蓝牙 5.0。手机与后台服务器之间的通信也要加密传输,比如采用 HTTPS 协议。同时手机应用程序与终端设备,手机应用程序与后台服务器都要进行双向认证,防止攻击者利用恶意手机应用程序进行敏感信息获取和远程控制。

内部网络如果没有防护,攻击者可通过存在漏洞的移动终端侵入到汽车内部 CAN 网络。由于传统的汽车内部 CAN 网络相对独立且没有采取相应的防护机制,因此,当攻击者通过车载终端侵入 CAN 网络后可以带来严重的安全威胁^[42~44]。从安全角度考虑,车厂可以采用虚拟化的技术让移动终端上的操作系统和应用程序运行在虚拟环境里,从而与外部网络相关的软件和操作相隔离^[81]。此外,车厂也可以采取相应的机制对进入 CAN 网络的消息指令进行检测和过滤^[54],从而确保内部 ECU 不被恶意控制和攻击。

3.3.4 车载软件更新安全

由于车联网系统的复杂性,无论终端应用程序还是内部 ECU 固件都会不定期更新。目前,智能网联汽车常采用 OTA (over-the-air) 的方式通过无线网络连接更新软件,因此 OTA 升级过程也成为了攻击者的攻击目标^[82]。当 OTA 升级过程存在漏洞并被攻击者利用后,攻击者可以替换更新的软件或者在更新软件中嵌入恶意代码,从而控制更新后的软件,实现攻击目的。如果攻击者控制了 OTA 过程,通过 OTA 向车辆安装恶意程序,攻击者将可以控制车辆,对车辆安全造成巨大的威胁。车厂可以从两个方面来提高 OTA 升级过程的安全性。一是设计使用安全的 OTA 升级协议,采用加密信道传输升级固件,避免攻击者通过中间人攻击来插入恶意代码或者替换更新固件。二是更新前要对将要更新的固件进行安全校验,保证更新固件的完整性和有效性^[44,82~85]。此外,车厂还应注意更新软件分发渠道的保密性,避免攻击者可以直接在网络上获取到更新软件进行分析逆向。车厂可对更新软件进行加密,这样即使更新软件被攻击者获取也难以被逆向。

在保证 OTA 更新过程安全性的同时,还应保证更新过程的可靠性,做到更新后的软件安全可靠^[84,86]。为了确保更新后的软件安全可靠,车厂在软件设计时,可采用双版本并存的方案而非直接用新软件替换原来软件。软件更新完成后,原先版本软件对更新的新软件进行可靠性验证,验证通过后再切换到新的软件上运行。

4 车联网综合安全监控系统规模化部署

在信息物理融合综合安全事件感知的基础上,开展监控系统的规模化部署。车联网信息物理融合系统的运行极大地依赖于车与车通信 (vehicle-to-vehicle, V2V)、车辆与基础设施通信 (vehicle-to-infrastructure, V2I) 和车与外界通信 (vehicle-to-everything, V2X), 高速稳定的网络对于车联网信息物理融合系统十分重要。对于车联网信息物理融合系统,车辆通过 5G 网络通信,满足低延迟、低通信负载、支持多种应用、良好的拥塞控制、公平的资源分配、高可靠性、支持快速移动、无缝隙覆盖等特性^[87~89]。

5G 无线网络将支持连接 1000 亿台设备,每平方千米支持 100 万台设备接入,将提供 10 Gbps 的数据速率,毫秒级的端到端时延,500 km/h 的移动性支持。相比于 4G,5G 网络将在频谱效率上提高 3~5 倍,能源效率上提高超过 100 倍,在 2020~2030 年之间,5G 网络将会大量部署^[3,4]。5G 与 4G

图 3 (网络版彩图) 4G/5G 关键性能比较 [90]
Figure 3 (Color online) Key capabilities comparison between 4G and 5G [90]

表 1 车联网通信技术性能比较

Table 1 Key capabilities comparison among vehicular communication technologies

	Data rate	Frequency band	Range	Mobility support	Coverage
3G [91]	2 Mbit/s	700–2600 MHz	Up to 10 km	High	Ubiquitous
4G [90~92]	1 Gbit/s	Licensed band	Up to 30 km	High (350 km/h)	Ubiquitous
5G [90]	20 Gbit/s	Licensed band	300–400 m	High (500 km/h)	Intermittent
Drive-thru Internet [92]	150 Mbit/s	2.4 GHz/5 GHz	500 m	High (120 km/h)	Intermittent
DSRC [92]	3–27 Mbit/s	5.86–5.92 GHz	300–1000 m	High (140 km/h)	Intermittent
TV white space [92]	420 Mbit/s	470–790 MHz	1 km/17–33 km	High (114 km/h)	Intermittent
Cellular V2X [91,93~95]	3 Gbit/s	5.9 GHz	1.6 km	High (up to 250 km/h)	Intermittent
Wi-Fi [91]	6–54 Mbit/s	2.4 GHz/5.2 GHz	Up to 100 m	Low	Intermittent
Bluetooth 5 [91,96]	50 Mbit/s	2.4 GHz	240 m	N/A	N/A
WiFi direct [91,97]	250 Mbit/s	2.4 GHz/5 GHz	200 m	N/A	N/A
LTE direct [91]	13.5 Mbit/s	Licensed LTE spectrum	500 m	N/A	N/A

的性能比较如图 3 所示, 车联网通信技术性能比较如表 1 [90~97] 所示, 其中移动支持 (mobility support) 中的具体速度数值只是参考, 尚未见到统一标准的公开测试数据结果, 传输速率 (data rate)、覆盖范围 (range) 的数值受建筑分布、用户规模等因素影响.

基于 5G 网络规模化部署车联网综合安全监控系统, 随着越来越多车辆的接入, 伴随着车联网信息物理融合系统的安全问题要充分防范, 除注意对网络攻击的防护、数据安全的保障之外, 同时网络系统自身需要有足够的鲁棒性.

在网络攻击防护方面, 5G 车联网网络需要注意用户和设备的身份加密、实体验证、信号数据加

密、信号数据完整性验证、用户数据加密、平台安全等问题^[98~100]。车联网系统需要对 DDoS 有防护功能, 如果对终端用户进行 DDoS 攻击可能导致车辆无法与云端进行通信, 造成数据丢失或车辆失控等问题^[101], 如果对网络资源基础设施进行 DDoS 攻击, 将造成网络瘫痪, 对道路交通造成巨大的威胁^[102]。

如果 5G 车联网实体认证存在问题, 恶意攻击者可能伪装成通过认证的实体, 请求大量资源, 导致合法的车辆节点无法进行通信, 或伪造道路上不存在车辆的数据, 影响车辆正常通行^[103,104]。攻击者还有可能发送大量的无效信息使车辆进行大量不必要的认证, 从而使车辆无法接受正常的信息。如果车联网系统存在数据加密和验证问题, 攻击者可能窃取车联网系统中的数据, 从而伪造错误的 V2X 消息, 误导车辆, 导致交通事故, 或恶意控制车辆的刹车、动力系统、车窗等装置, 干扰驾驶员驾驶, 造成交通事故。

在信息服务平台及数据安全方面, 车联网信息物理融合系统需要借助云平台来完成数据传输、存储、处理等工作, 云平台的安全问题至关重要^[105]。云平台需能满足高速运动车辆的请求, 及时对请求做出响应^[106~108]。云平台的身份认证需要得到保证, 应确认不同用户对云平台使用的权限^[109]。传统云平台的特权用户访问、法规遵从性、数据存储、数据隔离、数据恢复、调查支持和长期生存能力都需要车联网信息物理融合系统考虑。在车联网信息物理融合系统云平台上存储公共数据和私人数据。公共数据包括天气、服务平台数据、车辆内部公共环境数据、车辆运行外在环境数据等。私人数据包括车辆物理状态数据、司机驾驶状态、车况、行驶安全状态数据、车主个人信息、车辆历史位置信息、录音视频数据等。在数据的存储过程中, 要防止数据存储提供商滥用数据, 数据存储提供商只能在用户允许的对数据进行操作, 数据存储提供商必须在保障数据完整性、高质量、读取快捷、加密良好的前提下, 同时做到数据的易于检索^[110,111]。如果在数据的存储过程中引入第三方审查机构, 审查机构在审查数据完整性、正确性的过程中, 不能限制合法用户对数据的操作, 也不能为数据安全带来新的威胁^[112]。

对于公共数据和私人数据, 车联网信息物理融合系统需要进行不同程度的保护。公共数据需保证只有某些授权用户才能进行写操作, 防止对公共数据的恶意篡改。对于某些公共数据, 任何车辆都有可能写入的权限, 例如天气, 道路是否有坑洼、是否拥堵、是否有事故等数据, 对于这样的数据, 为了防止恶意攻击者写入错误的或带有诱骗性的数据, 应做好用户身份验证, 在取得足够多的可信样本数据后才能写入公共数据, 写入后还应不断对数据做验证。公共数据验证工作保证了公共数据的准确性和实时性。如果天气改变或道路状况改变, 数据的验证工作可保证公共数据总是反映最新的天气、道路状况信息。对于私人数据需保证用户访问的认证, 只有某些授权用户才能进行读操作, 如果用户数据可能被截获, 不能让截获者推断出数据内容及车辆信息, 要充分保护用户数据隐私, 防止用户隐私数据被窃取。对于数据的传输和存储, 需有加密机制保证数据的安全, 同时加密算法不能过于复杂, 否则可能过多消耗服务器和用户的资源, 使整个系统的延迟加大。对于数据的访问, 需有足够的验证机制, 避免出现用户身份猜解和伪装, 防止用户数据被越权访问、恶意修改。

在网络系统的鲁棒性方面, 车联网信息物理融合系统的网络需要支持大量网络应用, 如与车辆有关的、与司机有关的、与乘客有关的、与行人有关的应用等。对于这些应用, 应首先保证与交通安全有关的应用的网络需求。车联网信息物理融合系统需保证其网络系统可以连续可靠地运行, 系统应能满足大量车辆接入网络并在车辆高速运动状态下提供可靠安全网络服务的需求。如果车辆的网络连接断开, 需保证能及时快速地重新连接网络。同时, 系统应能应对突然发生的火灾、断电、自然灾害等突发事件。

5 基于事件的综合安全监控智能决策

在车联网综合安全监控系统规模化部署后,需进一步为综合安全监控决策赋予智能.本文提出基于事件的综合安全监控智能决策,采用离散事件动态系统理论模型,对复杂异构系统的工作流程、任务到达模型、服务模型和排队模型等进行形式化建模.离散事件系统理论模型广泛用于交通管理、生产调度、资源利用、计算机网络系统分析和设计方面,可为车联网综合安全监控注入强有力的智能决策能力.

基于事件的综合安全监控智能决策,首先要解决的问题是如何基于观测到的各种安全事件,动态自适应调优各类综合安全事件的采样频率及相应的数据码率,在安全监控资源有限的情况下,优化系统资源的调度和使用,以最大化系统的可扩展性.例如,从车辆运动状态指标的角度,在车辆稳定运行状态下,可动态调低对车辆视频监控的采样率和解析度,直至车辆运动状态趋于激烈.可结合不同地理位置和时间的治安事件发生的概率,以及犯罪分子的引发治安事件的危害与成本博弈分析,策略性随机化对不同基础设施和车载智能终端的网络带宽和存储资源分配调度,使得在有限监控资源下,对不同时间、地点及交通工具的监控重点随着环境改变而有针对性地做出智能性的优化调整.现有的动态调整视频采样率和解析度的研究,主要基于网络可用带宽,而非车辆的状态及所处环境.基于所观测到的各种安全事件,动态自适应调优各类综合安全事件的采样频率及相应的数据码率,可采用增强学习的技术思路,建立从观测 (observation) 到行动 (action) 的动态映射关系.

为了提升车辆对于各种安全事件的智能感知的性能,未来的事件智能感知技术将能够在一套硬件平台集成多种传感器 (包括加速传感器、陀螺仪、重力传感器、地磁传感器、GPS)、高清摄像头、WiFi/4G/5G 通信模块、车内防火墙监控、OBD 监控等,不仅能够实时捕获车辆的细粒度、多维度实时状态数据、高清摄像头的视频数据,而且能够支持通过 WiFi/4G/5G 等与路侧基础设施间进行通信.同时,在硬件内置各种异常事件检测算法,算法的复杂度能够满足事件预测和检测的实时性.一方面,通过多阶运动特征提取,内置机器学习分类算法,检测蛇形、急加速、急减速、急变道、掉头、碰撞、失重、超载等异常突发事件.另一方面,通过内置车辆环境及通信系统的行为特征分析算法,自动检测和提取公共交通工具内发生的安全事件.最终,能够实现在第一时间预测和检测异常事件,进行实时报警.在网络信号覆盖、可用带宽资源有限的情况下,通过运动传感器和监控数据分析,实时预测和检测车辆异常事件,动态调整对危险驾驶行为、公共治安事件的采样频率及解析度等监控指标.例如,在重庆公交坠江事件中,在检测到车辆的下坠行为后,可即时将报警信号发送到云端,同时将大数据量的高清视频数据、细粒度车辆驾驶行为数据卸载到桥边部署的路侧设施中,避免事后打捞黑匣子的被动局面.

在大规模部署环境下,环境感知的通道选择与路侧设施部署非常重要.在未来若干年内,4G, 5G 甚至 3G 网络很可能会共同提供服务.由于不同网络通道的成本不同,在网络资源有限的情况下,动态根据安全监控的任务需求,基于环境感知优化选择网络传输通道,将大大提升综合安全监控的效率,节约网络资源,降低不必要的资源消耗.同时,路侧设施的部署及其与云端间的任务调度也是一项关键科学问题^[113, 114].基于异常事件检测结果,监测到车辆运动状态、治安事件等方面的异常事件后,在带宽资源等的实际约束下,根据车辆运行轨迹和当前所处的位置周围的网络基础设施状况,动态自适应选择传输监控数据传输的通道,包括 4G/5G 基站或者附近 WiFi,基于环境 (包括事件和位置) 感知自适应动态选择监控数据的传输通道.

特别地,针对视频数据,可在硬件产品中封装视频压缩感知技术,结合网络可用带宽和异常事件两方面的因素,实现基于 DASH (dynamic adaptive streaming over HTTP) 的动态调整视频传输码率

图 4 基于事件的综合安全监控智能决策方案

Figure 4 Event-based integrated security monitoring & intelligent decision-making scheme

(bitrate), 在保障视频完整性的前提下最大化清晰度, 保障在异常事件发生的第一时间, 视频数据能够完整备份并及时上传. 与车载移动终端相配合, 在路边、桥边、公交站、江边等路基部署网络通信基础设施, 建立 V2I 的通信模式, 辅助车载移动终端进行数据存储、处理和传输. 依据路况及车辆的运行轨迹, 结合不同时间和地理位置的治安状况数据, 基于安全博弈理论, 优化选择基站、路侧通信设施等网络通信基础设施的部署位置. 这些部署的基础设施具有数据存储和复杂行为分析功能, 一方面可以帮助车载移动终端将大规模数据卸载, 另一方面可补充车载移动终端实时数据处理上的性能不足. 根据交通工具的动态轨迹以及沿路固定基础设施提供的可用 4G/5G 基站、WiFi 热点, 对所记录的重要视频进行适时的卸载备份, 以补充传统移动网络基站所提供的有限传输带宽. 其关键技术在于优化和动态调整不同交通工具数据卸载的时间和地点, 以最大化整体的安全监控效率.

在安全数据取证分析方面, 建立安全事件分级机制下的数据存储处理取证非常必要. 其目的在于在云端、边缘端建立监控流量的策略化接收、存储、检索与重放等功能. 一方面, 能够对真实网络视频流量进行长时间完整捕获和存储, 对捕获到的监控流量进行实时还原, 对原始监控流量中传输的内容及其语义快速查询检索, 对流量中数据包的 IP 以及会话中的域名进行快速查询检索, 以及将捕获的真实监控数据流量进行还原回放. 同时, 监控流量的高速捕获、存储与重放需能够做到长时间无丢包, 对监控流量实时还原, 对监控流量进行审计与分析, 将真实监控流量按照指定速率等多种可控场景进行保序还原回放. 对后台所记录的监控数据, 根据驾驶行为及相关治安数据, 进行分级存储, 并提供多种属性的快速检索服务. 例如, 可基于检测到的安全事件, 判断为重要性高的监控数据, 则进行高采样率高解析度无压缩捕获存储; 判断为重要性相对低的监控数据, 可进行低解析度压缩捕获存储. 基于事件的综合安全监控智能决策方案如图 4 所示, 该方案能基于所观测到的各种安全事件和环境, 动态自适应调优事件感知、网络传输和数据处理策略, 再根据事件观测进行状态估计、预测、异常检测和决策下发, 并根据决策进行事件感知策略调优及对车辆的远程控制 (如对车辆本身运动行为、车辆维保、紧急情况报警、OTA 升级等多方面的远程控制).

6 总结

随着 5G 通信时代的来临, 交通安全领域无疑将会出现巨大的机遇. 本文针对交通领域预防重特大事故及信息物理融合综合安全取证分析的需求, 基于 5G 通信技术, 提出基于事件的车联网信息物

理融合安全治理框架. 在该框架下, 从“车辆状态安全、车辆环境安全、信息系统安全”等角度, 综合分析和探讨了物理层、通信层、社会层不同层面的不安全事件, 并讨论了 5G 技术为车联网综合安全监控系统规模化部署带来的支持和车联网网络安全性、鲁棒性的挑战, 最后提出了基于离散事件动态系统理论模型的安全监控智能决策方案, 为该框架注入智能决策能力. 本文所提框架, 具有事件与数据分离的技术特色, 有利于构建一体化的车联网信息物理融合综合安全应对方案, 服务于“事前全时预判、事中即时报警、事后回放取证”的安全目标.

参考文献

- 1 World Health Organization. Global status report on road safety 2018. 2018. <https://apps.who.int/iris/bitstream/handle/10665/276462/9789241565684-eng.pdf?ua=1>
- 2 National Bureau of Statistics of China. China Statistical Yearbook-2018. 2018 [国家统计局. 中国统计年鉴 -2018. 2018]. <http://www.stats.gov.cn/tjsj/ndsj/2018/indexch.htm>
- 3 Gupta A, Jha R K. A survey of 5G network: architecture and emerging technologies. *IEEE Access*, 2015, 3: 1206–1232
- 4 Jiang D J, Liu G Y. An overview of 5G requirements. In: *5G Mobile Communications*. Berlin: Springer, 2017. 3–26
- 5 Li S C, Xu L D, Zhao S S. 5G Internet of Things: a survey. *J Industrial Inf Integration*, 2018, 10: 1–9
- 6 Huawei. Top Ten Application Scenarios in the 5G Era White Paper. 2017
- 7 Chen Z Y, Yu J D, Zhu Y M, et al. D³: abnormal driving behaviors detection and identification using smart-phone sensors. In: *Proceedings of the 12th Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, Seattle, 2015. 524–532
- 8 Fang S H, Liang Y C, Chiu K M. Developing a mobile phone-based fall detection system on android platform. In: *Proceedings of Computing, Communications and Applications Conference*, Hong Kong, 2012. 143–146
- 9 Morris B T, Trivedi M M. A survey of vision-based trajectory learning and analysis for surveillance. *IEEE Trans Circ Syst Video Technol*, 2008, 18: 1114–1127
- 10 Zaldivar J, Calafate C T, Cano J C, et al. Providing accident detection in vehicular networks through OBD-II devices and Android-based smartphones. In: *Proceedings of the 36th Conference on Local Computer Networks*, Bonn, 2011. 813–819
- 11 Zhang M M, Chen C, Wo T Y, et al. SafeDrive: online driving anomaly detection from large-scale vehicle data. *IEEE Trans Ind Inf*, 2017, 13: 2087–2096
- 12 Jabon M, Bailenson J, Pontikakis E, et al. Facial expression analysis for predicting unsafe driving behavior. *IEEE Pervas Comput*, 2010, 10: 84–95
- 13 Ahmad R, Borole J N. Drowsy driver identification using eye blink detection. *Int J Comput Sci Inf Tech*, 2015, 6: 270–274
- 14 Jain A, Singh A, Koppula H S, et al. Recurrent neural networks for driver activity anticipation via sensory-fusion architecture. In: *Proceedings of IEEE International Conference on Robotics and Automation (ICRA)*, Stockholm, 2016. 3118–3125
- 15 Hallac D, Sharang A, Stahlmann R, et al. Driver identification using automobile sensor data from a single turn. In: *Proceedings of the 19th International Conference on Intelligent Transportation Systems (ITSC)*, Rio de Janeiro, 2016. 953–958
- 16 Wu J D, Ye S H. Driver identification using finger-vein patterns with Radon transform and neural network. *Expert Syst Appl*, 2009, 36: 5793–5799
- 17 Barr J R, Bowyer K W, Flynn P J, et al. Face recognition from video: a review. *Int J Patt Recogn Artif Intell*, 2012, 26: 1266002
- 18 Deniz O, Serrano I, Bueno G, et al. Fast violence detection in video. In: *Proceedings of International Conference on Computer Vision Theory and Applications*, Lisbon Portugal, 2014. 2: 478–485
- 19 Sivaraman S, Trivedi M M. Looking at vehicles on the road: a survey of vision-based vehicle detection, tracking, and behavior analysis. *IEEE Trans Intell Transp Syst*, 2013, 14: 1773–1795
- 20 Kumar S, Shi L, Ahmed N, et al. Carspeak: a content-centric network for autonomous driving. In: *Proceedings of ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer*

- Communication, Helsinki, 2012. 259–270
- 21 Sakiz F, Sen S. A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV. *Ad Hoc Netw*, 2017, 61: 33–50
- 22 Halimeh J C, Roser M. Raindrop detection on car windshields using geometric-photometric environment construction and intensity-based correlation. In: *Proceedings of IEEE Intelligent Vehicles Symposium*, Xi'an, 2009. 610–615
- 23 Sato R, Domany K, Deguchi D, et al. Visibility estimation of traffic signals under rainy weather conditions for smart driving support. In: *Proceedings of the 15th International IEEE Conference on Intelligent Transportation Systems*, Anchorage, 2012. 1321–1326
- 24 Liu W, Maruya K. Detection and recognition of traffic signs in adverse conditions. In: *Proceedings of IEEE Intelligent Vehicles Symposium*, Xi'an, 2009. 335–340
- 25 Mori K, Takahashi T, Ide I, et al. Recognition of foggy conditions by in-vehicle camera and millimeter wave radar. In: *Proceedings of IEEE Intelligent Vehicles Symposium*, Istanbul, 2007. 87–92
- 26 Li Q Q, Chen L, Li M, et al. A sensor-fusion drivable-region and lane-detection system for autonomous vehicle navigation in challenging road scenarios. *IEEE Trans Veh Technol*, 2014, 63: 540–555
- 27 Eriksson J, Girod L, Hull B, et al. The pothole patrol: using a mobile sensor network for road surface monitoring. In: *Proceedings of the 6th International Conference on Mobile Systems, Applications, and Services*, Breckenridge, 2008. 29–39
- 28 Chen K Y, Lu M M, Fan X P, et al. Road condition monitoring using on-board three-axis accelerometer and GPS sensor. In: *Proceedings of the 6th International ICST Conference on Communications and Networking in China (CHINACOM)*, Harbin, 2011. 1032–1037
- 29 Mohan P, Padmanabhan V N, Ramjee R. Nericell: rich monitoring of road and traffic conditions using mobile smartphones. In: *Proceedings of the 6th ACM Conference on Embedded Network Sensor Systems*, Raleigh, 2008. 323–336
- 30 Bhoraskar R, Vankadhara N, Raman B, et al. Wolverine: traffic and road condition estimation using smartphone sensors. In: *Proceedings of the 4th International Conference on Communication Systems and Networks (COMSNETS 2012)*, Bangalore, 2012. 1–6
- 31 Glaser S, Nouveliere L, Lusetti B. Speed limitation based on an advanced curve warning system. In: *Proceedings of IEEE Intelligent Vehicles Symposium*, Istanbul, 2007. 686–691
- 32 García F, Jiménez F, Anaya J, et al. Distributed pedestrian detection alerts based on data fusion with accurate localization. *Sensors*, 2013, 13: 11687–11708
- 33 Gámez Serna C, Ruichek Y. Dynamic speed adaptation for path tracking based on curvature information and speed limits. *Sensors*, 2017, 17: 1383
- 34 Hussein A, García F, Armingol J M, et al. P2V and V2P communication for pedestrian warning on the basis of autonomous vehicles. In: *Proceedings of the 19th International Conference on Intelligent Transportation Systems (ITSC)*, Rio de Janeiro, 2016. 2034–2039
- 35 Nkenyereye L, Liu C H, Song J S. Towards secure and privacy preserving collision avoidance system in 5G fog based Internet of vehicles. *Future Generation Comput Syst*, 2019, 95: 488–499
- 36 Kokuti A, Hussein A, Marín-Plaza P, et al. V2X communications architecture for off-road autonomous vehicles. In: *Proceedings of IEEE International Conference on Vehicular Electronics and Safety (ICVES)*, Vienna, 2017. 69–74
- 37 Koscher K, Czeskis A, Roesner F, et al. Experimental security analysis of a modern automobile. In: *Proceedings of IEEE Symposium on Security and Privacy*, Berkeley/Oakland, 2010. 447–462
- 38 Sau S, Haj-Yahya J, Wong M M, et al. Survey of secure processors. In: *Proceedings of International Conference on Embedded Computer Systems: Architectures, Modeling, and Simulation (SAMOS)*, Pythagorion, 2017. 253–260
- 39 Bécsi T, Aradi S, Gépár P. Security issues and vulnerabilities in connected car systems. In: *Proceedings of International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*, Budapest, 2015. 477–482
- 40 Wang Q Y, Sawhney S. VeCure: a practical security framework to protect the CAN bus of vehicles. In: *Proceedings of International Conference on the Internet of Things (IOT)*, Cambridge, 2014. 13–18
- 41 Avatefipour O, Malik H. State-of-the-art survey on in-vehicle network communication (CAN-Bus) security and vul-

- nerabilities. *Int J Comput Sci Netw*, 2017, 6: 720–727
- 42 Keenlab. Experimental security assessment of BMW cars: a summary report. 2018. <https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/>
 - 43 Nie S, Liu L, Du Y. Free-fall: hacking tesla from wireless to CAN bus. 2017. <https://paper.seebug.org/papers/Security%20Conf/Blackhat/2017.us/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf>
 - 44 Eiza M H, Ni Q. Driving with sharks: rethinking connected vehicles with vehicle cybersecurity. *IEEE Veh Technol Mag*, 2017, 12: 45–51
 - 45 Checkoway S, McCoy D, Kantor B, et al. Comprehensive experimental analyses of automotive attack surfaces. In: *Proceedings of the 20th USENIX Security Symposium*, San Francisco, 2011. 447–462
 - 46 Rouf I, Miller R, Mustafa H, et al. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: *Proceedings of the 19th USENIX Security Symposium*, Washington, 2010. 11–13
 - 47 Markovitz M, Wool A. Field classification, modeling and anomaly detection in unknown CAN bus networks. *Vehicular Commun*, 2017, 9: 43–52
 - 48 Marchetti M, Stabili D. READ: reverse engineering of automotive data frames. *IEEE Trans Inform Forensic Secur*, 2019, 14: 1083–1097
 - 49 Pawelec K, Bridges R A, Combs F L. Towards a CAN IDS based on a neural network data field predictor. In: *Proceedings of ACM Workshop on Automotive Cybersecurity*, Dallas, 2019. 31–34
 - 50 Olufowobi H, Ezeobi U, Muhati E, et al. Anomaly detection approach using adaptive cumulative sum algorithm for controller area network. In: *Proceedings of ACM Workshop on Automotive Cybersecurity*, Dallas, 2019. 25–30
 - 51 Young C, Olufowobi H, Bloom G, et al. Automotive intrusion detection based on constant CAN message frequencies across vehicle driving modes. In: *Proceedings of ACM Workshop on Automotive Cybersecurity*, Dallas, 2019. 9–14
 - 52 Koyama T, Shibahara T, Hasegawa K, et al. Anomaly detection for mixed transmission CAN messages using quantized intervals and absolute difference of payloads. In: *Proceedings of ACM Workshop on Automotive Cybersecurity*, Dallas, 2019. 19–24
 - 53 Song H M, Kim H R, Kim H K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In: *Proceedings of International Conference on Information Networking (ICOIN)*, Kota Kinabalu, 2016. 63–68
 - 54 Choi W, Joo K, Jo H J, et al. VoltageIDS: low-level communication characteristics for automotive intrusion detection system. *IEEE Trans Inform Forensic Secur*, 2018, 13: 2114–2129
 - 55 Gerla M, Lee E K, Pau G, et al. Internet of vehicles: from intelligent grid to autonomous cars and vehicular clouds. In: *Proceedings of IEEE World Forum on Internet of Things (WF-IoT)*, Seoul, 2014. 241–246
 - 56 Petit J, Stottelaar B, Feiri M, et al. Remote attacks on automated vehicles sensors: experiments on camera and lidar. *Black Hat Europe*, 2015, 11: 2015
 - 57 Yan C, Xu W, Liu J. Can you trust autonomous vehicles: contactless attacks against sensors of self-driving vehicle. In: *Proceedings of the 24th DEF CON Conference on Hacking*, Las Vegas, 2016. 1–13
 - 58 Sitawarin C, Bhagoji A N, Mosenia A, et al. Darts: deceiving autonomous cars with toxic signs. 2018. ArXiv: 1802.06430
 - 59 Rahimi-Eichi H, Ojha U, Baronti F, et al. Battery management system: an overview of its application in the smart grid and electric vehicles. *IEEE Ind Electron Mag*, 2013, 7: 4–16
 - 60 Sagstetter F, Lukasiewicz M, Steinhorst S, et al. Security challenges in automotive hardware/software architecture design. In: *Proceedings of Conference on Design, Automation and Test in Europe*, Grenoble, 2013. 458–463
 - 61 Falk R, Fries S. Electric vehicle charging infrastructure security considerations and approaches. In: *Proceedings of the 4th International Conference on Evolving Internet*, 2012. 58–64
 - 62 Mustafa M A, Zhang N, Kalogridis G, et al. Smart electric vehicle charging: security analysis. In: *Proceedings of IEEE PES Innovative Smart Grid Technologies Conference (ISGT)*, Washington, 2013. 1–6
 - 63 Siemens. Traffic control via the Siemens private cloud. 2014. www.siemens.com/press/pool/de/events/2014/infrastructure-cities/2014-03-intertraffic/background-private-cloud-e.pdf
 - 64 Tennessee Department of Transportation. TDOT smartway. www.tdot.state.tn.us/tdotsmartway/
 - 65 Liu J, Li J T, Zhang L, et al. Secure intelligent traffic light control using fog computing. *Future Generation Comput Syst*, 2018, 78: 817–824

- 66 Ghena B, Beyer W, Hillaker A, et al. Green lights forever: analyzing the security of traffic infrastructure. In: Proceedings of the 8th USENIX Workshop on Offensive Technologies, Berkeley, 2014. 7
- 67 Laszka A, Potteiger B, Vorobeychik Y, et al. Vulnerability of transportation networks to traffic-signal tampering. In: Proceedings of the 7th International Conference on Cyber-Physical Systems (ICCPs), Vienna, 2016. 1–10
- 68 Mazloom S, Rezaeirad M, Hunter A, et al. A security analysis of an in-vehicle infotainment and app platform. In: Proceedings of 10th USENIX Workshop on Offensive Technologies, Austin, 2016. 1–12
- 69 Jo H J, Choi W, Na S Y, et al. Vulnerabilities of android os-based telematics system. *Wirel Pers Commun*, 2017, 92: 1511–1530
- 70 Wang X, Konstantinou C, Maniatakos M, et al. Confirm: detecting firmware modifications in embedded systems using hardware performance counters. In: Proceedings of IEEE/ACM International Conference on Computer-aided Design, Austin, 2015. 544–551
- 71 Faruki P, Bharmal A, Laxmi V, et al. Android security: a survey of issues, malware penetration, and defenses. *IEEE Commun Surv Tut*, 2015, 17: 998–1022
- 72 Zhou W, Zhou Y J, Jiang X X, et al. Detecting repackaged smartphone applications in third-party android marketplaces. In: Proceedings of the 2nd ACM Conference on Data and Application Security and Privacy, San Antonio, 2012. 317–326
- 73 Mutchler P, Doupé A, Mitchell J, et al. A large-scale study of mobile web app security. In: Proceedings of Mobile Security Technologies Workshop (MoST), San Jose, 2015. 1–11
- 74 Martin W, Sarro F, Jia Y, et al. A survey of app store analysis for software engineering. *IEEE Trans Softw Eng*, 2017, 43: 817–847
- 75 Watanabe T, Akiyama M, Kanei F, et al. Understanding the origins of mobile app vulnerabilities: a large-scale measurement study of free and paid apps. In: Proceedings of the 14th International Conference on Mining Software Repositories, Buenos Aires, 2017. 14–24
- 76 Sbirlea D, Burke M G, Guarnieri S, et al. Automatic detection of inter-application permission leaks in Android applications. *IBM J Res Dev*, 2013, 57: 10:1–10:12
- 77 Woo S, Jo H J, Lee D H. A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Trans Intell Transp Syst*, 2014, 16: 993–1006
- 78 Rastogi S, Bhushan K, Gupta B B. Android applications repackaging detection techniques for smartphone devices. *Procedia Comput Sci*, 2016, 78: 26–32
- 79 Hsueh S C, Li J T. Secure transmission protocol for the IoT. In: Proceedings of the 3rd International Conference on Industrial and Business Engineering, Sapporo, 2017. 73–76
- 80 Granjal J, Monteiro E, Silva J S. Security for the Internet of Things: a survey of existing protocols and open research issues. *IEEE Commun Surv Tut*, 2015, 17: 1294–1312
- 81 Pelzl J, Wolf M, Wollinger T. Virtualization technologies for cars. 2008. <https://pdfs.semanticscholar.org/542e/6a33be07ef419193ba663368aad3cd395267.pdf>
- 82 Le V H, den Hartog J, Zannone N. Security and privacy for innovative automotive applications: a survey. *Comput Commun*, 2018, 132: 17–41
- 83 Jeong E, Park J, Son B, et al. Study on signature verification process for the firmware of an android platform. In: Proceedings of International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, Matsue, 2018. 540–545
- 84 Petri R, Springer M, Zelle D, et al. Evaluation of lightweight TPMs for automotive software updates over the air. In: Proceedings of the 4th International Conference on Embedded Security in Car USA, Detroit, 2016. 1–15
- 85 Luo Q, Liu J J. Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions. *IEEE Wirel Commun*, 2018, 25: 113–119
- 86 Chawan A, Sun W, Javaid A, et al. Security enhancement of over-the-air update for connected vehicles. In: Proceedings of International Conference on Wireless Algorithms, Systems, and Applications, Tianjin, 2018. 853–864
- 87 Ashraf M I, Liu C F, Bennis M, et al. Towards low-latency and ultra-reliable vehicle-to-vehicle communication. In: Proceedings of European Conference on Networks and Communications, Oulu, 2017. 1–5
- 88 Shah S A A, Ahmed E, Imran M, et al. 5G for vehicular communications. *IEEE Commun Mag*, 2018, 56: 111–117
- 89 Engoulou R G, Bellaïche M, Pierre S, et al. VANET security surveys. *Comput Commun*, 2014, 44: 1–13

- 90 Series M. IMT Vision — framework and overall objectives of the future development of IMT for 2020 and beyond. 2015. https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-1!!PDF-E.pdf
- 91 Poli F. Vehicular communications: from DSRC to cellular V2X. 2018. <https://webthesis.biblio.polito.it/9043/1/tesi.pdf>
- 92 Zhou H B, Xu W C, Bi Y G, et al. Toward 5G spectrum sharing for immersive-experience-driven vehicular communications. *IEEE Wirel Commun*, 2017, 24: 30–37
- 93 Masini B, Bazzi A, Zanella A. A survey on the roadmap to mandate on board connectivity and enable V2V-based vehicular sensor networks. *Sensors*, 2018, 18: 2207
- 94 Nguyen T V, Shailesh P, Sudhir B, et al. A comparison of cellular vehicle-to-everything and dedicated short range communication. In: *Proceedings of 2017 IEEE Vehicular Networking Conference (VNC)*, Torino, 2017. 101–108
- 95 Ancans A, Petersons E, Ancans G, et al. Technical and economic analysis of transport telecommunication infrastructure. *Procedia Comput Sci*, 2019, 149: 206–214
- 96 Woolley M, Schmidt S. Bluetooth 5/Go faster, go further. *Bluetooth SIG*, 2017, 1: 1–25
- 97 Funai C, Tapparello C, Heinzelman W. Enabling multi-hop ad hoc networks through WiFi Direct multi-group networking. In: *Proceedings of 2017 International Conference on Computing, Networking and Communications (ICNC)*, Silicon Valley, 2017. 491–497
- 98 Schneider P, Horn G. Towards 5G security. In: *Proceedings of IEEE Trustcom/BigDataSE/ISPA*, Helsinki, 2015. 1165–1170
- 99 Fang D F, Qian Y, Hu R Q. Security for 5G mobile wireless networks. *IEEE Access*, 2018, 6: 4850–4874
- 100 Zaidi K, Rajarajan M. Vehicular Internet: security & privacy challenges and opportunities. *Future Internet*, 2015, 7: 257–275
- 101 Petit J, Shladover S E. Potential cyberattacks on automated vehicles. *IEEE Trans Intell Transp Syst*, 2014, 16: 546–556
- 102 Ahmad I, Kumar T, Liyanage M, et al. Overview of 5G security challenges and solutions. *IEEE Comm Stand Mag*, 2018, 2: 36–43
- 103 Malla A M, Sahu R K. Security attacks with an effective solution for dos attacks in VANET. *Int J Comput Appl*, 2013, 66
- 104 Jeske T. Floating car data from smartphones: what google and waze know about you and how hackers can control traffic. In: *Proceedings of the BlackHat Europe*, Amsterdam, 2013. 1–12
- 105 Lee E, Lee E K, Gerla M, et al. Vehicular cloud networking: architecture and design principles. *IEEE Commun Mag*, 2014, 52: 148–155
- 106 Boukerche A, de Grande R E. Vehicular cloud computing: architectures, applications, and mobility. *Comput Netw*, 2018, 135: 171–189
- 107 Whaiduzzaman M, Sookhak M, Gani A, et al. A survey on vehicular cloud computing. *J Netw Comput Appl*, 2014, 40: 325–344
- 108 Ning Z L, Wang X J, Huang J. Mobile edge computing-enabled 5G vehicular networks: toward the integration of communication and computing. *IEEE Veh Technol Mag*, 2019, 14: 54–61
- 109 Eiza M H, Ni Q, Shi Q. Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks. *IEEE Trans Veh Technol*, 2016, 65: 7868–7881
- 110 Sun Y C, Zhang J S, Xiong Y P, et al. Data security and privacy in cloud computing. *Int J Distrib Sens Netw*, 2014, 10: 190903
- 111 Nafi K W, Kar T S, Hoque S A, et al. A newer user authentication, file encryption and distributed server based cloud computing security architecture. *Int J Adv Comput Sci Appl*, 2012, 3: 181–186
- 112 Wang C, Wang Q, Ren K, et al. Privacy-preserving public auditing for data storage security in cloud computing. In: *Proceedings of IEEE Infocom*, San Diego, 2010. 1–9
- 113 Zhang W Y, Li S G, Liu L Y, et al. Hetero-edge: orchestration of real-time vision applications on heterogeneous edge clouds. In: *Proceedings of IEEE Conference on Computer Communications*, Paris, 2019. 1270–1278
- 114 Taleb T, Samdanis K, Mada B, et al. On multi-access edge computing: a survey of the emerging 5G network edge cloud architecture and orchestration. *IEEE Commun Surv Tut*, 2017, 19: 1657–1681

Integrated security of cyber-physical vehicle networked systems in the age of 5G

Xiaobo MA^{1,2}, Jiahao PENG^{1,2}, Lei XUE³ & Xiaohong GUAN^{1,2*}

1. Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China;

2. MOE Key Lab for Intelligent Networks and Network Security, Xi'an Jiaotong University, Xi'an 710049, China;

3. Department of Computing, The Hong Kong Polytechnic University, Hong Kong 999077, China

* Corresponding author. E-mail: xhguan@xjtu.edu.cn

Abstract In recent years, a series of serious catastrophic traffic accidents, such as the Chongqing bus crash and Wuxi Road bridge collapse, revealed some serious issues in the mobile vehicle safety and emergency response mechanisms. The advent of 5G communication has undoubtedly created some great opportunities for solving these issues. In order to fulfill the requirements of serious traffic accident prevention and forensic analysis, this paper proposes an event-based mobile vehicle cyber-physical security governance framework based on 5G communication technology. The proposed framework aims to resolve the issues of mobile vehicle security, including the availability of network resources in high-speed motion and the complexity of security objectives within cyber-physical systems. Relying on precise perception of insecure events at the physical, communication, and society layers, this paper constructs an integrated intelligent safety response strategy for physical equipment information security, state vehicle security, environmental vehicle security, and network security by intelligent perception, edge-cloud computing, and other technologies. The proposed framework achieves the goals of real-time event prediction before the event, immediate alarm during the event, and replay for evidence forensics after the event.

Keywords 5G, Internet of vehicles, cyber-physical systems, hybrid security, event driven

Xiaobo MA is an associate professor at the MOE Key Lab for Intelligent Networks and Network Security, the Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. He received his Ph.D. degree in control science and engineering from Xi'an Jiaotong University and was a post-doctoral research fellow at the Hong Kong Polytechnic University. He is a member of IEEE.

His research interests include network security and privacy.

Jiahao PENG is an M.S. student at the Faculty of Electronic and Information Engineering, Xi'an Jiaotong University. He received his B.E. degree from Xi'an Jiaotong University in 2018. His research interests include network measurement.

Lei XUE received his Ph.D. degree in computer science from The Hong Kong Polytechnic University. He is currently a post-doctoral research fellow at the Department of Computing of the Hong Kong Polytechnic University. His current research interests include network security, mobile security, and network measurement.

Xiaohong GUAN works at the MOE Key Lab for Intelligent Networks and Network Security, the Faculty of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China. He is currently a Cheung Kong Professor of Systems Engineering and the Dean of the Faculty of Electronic and Information Engineering. His research interests include allocation and scheduling of complex networked resources and network security. He received his Ph.D. degree in electrical engineering from the University of Connecticut, Storrs, in 1993. Since 1995, he has also worked at the Department of Automation, Tsinghua National Laboratory for Information Science and Technology, and the Center for Intelligent and Networked Systems, TNLIST, Tsinghua University. He is an IEEE Fellow and an academician of the Chinese Academy of Sciences.