计算机人工环境下智能网联车辆信息安全保护系统研究智能技术

案贾
中国汽车信息技术有限公司，天津，
jiayunhui@catarc.ac.cn，通讯作者

Shilan 胡
中国汽车信息技术有限公司，天津 hushilan@catarc.ac.cn

马将尝试
中国汽车信息技术有限公司，天津 mayuchen@catarc.ac.cn

Shunkai 王
中国汽车信息技术有限公司，天津
wangshunkai@catarc.ac.cn

Zonghao 马
中国汽车信息技术有限公司，天津 mazonghao@catarc.ac.cn

宏宇妞妞
中国汽车信息技术有限公司，天津 niuhongyu@catarc.ac.cn

摘要

为了充分了解智能网联汽车面临的信息安全风险，提高智能网联汽车的信息安全防护水平，有必要从智能网联汽车架构的特点出发，综合分析其面临的威胁、挑战和潜在风险。智能网联汽车由多功能、松耦合、动态的复杂子系统组成。子系统的可用性、可靠性和信息安全性的特点直接影响着系统间交互的安全性。传统的分析方法无法满足这些需求。为此，设计并实现了智能网联汽车信息安全风险控制系统，包括信息安全防护系统安全、移动应用 APP 安全、服务器安全分析平台。通过实验，测试了信息安全防护原型抵御 DoS 攻击和网络 SYN 攻击的能力，验证了所提出的信息安全风险控制体系的有效性。

CCS 的概念

• **信息系统**信息系统应用→·算平台。

关键字

计算机、人工智能、车联网、信息安全防护系统

ICCSIE2022, 2022 年 9 月 23-25 日，布里斯班，昆士兰，澳大利亚
& # 169;2022 年计算机协会。Acm isbn 978-1-4503-9741-4/22/09…$15.00
https://doi.org/10.1145/3558819.3565231

ACM 参考格式:
贾云辉，胡世兰，马宇晨，王顺凯，马宗浩，牛宏宇。2022.计算机人工智能技术下的智能网联汽车信息安全保护系统研究。第*七届网络安全和信息工程国际会议(ICCSIE2022)， 9 月 23 日至 25 日，2022，布里斯班，昆士兰，澳大利亚*。ACM，纽约，美国，6 页。https://doi.org/10.1145/3558819.3565231

1 介绍

近年来，随着汽车智能化程度的不断提高，汽车各种系统被攻击的可能性越来越大，其安全风险也越来越大。因此，汽车的安全性能受到了广泛的关注。为了减少交通事故的发生，大多数汽车公司都在致力于汽车安全防护系统的研究和开发。智能网联技术已在智能交通领域得到应用[1]。智能联网系统是车辆与车辆、车辆与人、车辆与道路、车辆与云(平台)之间按照约定的系统架构及其通信协议和数据交换标准进行通信和信息交换的信息基础设施。智能网络系统的安全运行取决于系统内各子系统的安全性和各子系统之间的互操作性。因此，设计一个安全可靠的智能网络化系统架构至关重要。

2 icv 系统架构的特点

ICV 涉及多个专业技术领域和应用领域，其产业由“三跨”发展而来。“芯片模块+终端+车企”;2018 年要“新四跨度”;“芯片 module"2020 年“+终端+车企+ CA 平台”，产业化进程进一步加快[2]。常见的智能网联汽车系统架构层如图 1 所示(图片引用自《车联网网络架构》): 回顾，协议分析，挑战和问题: 第五届 IOV 国际会议，2018;

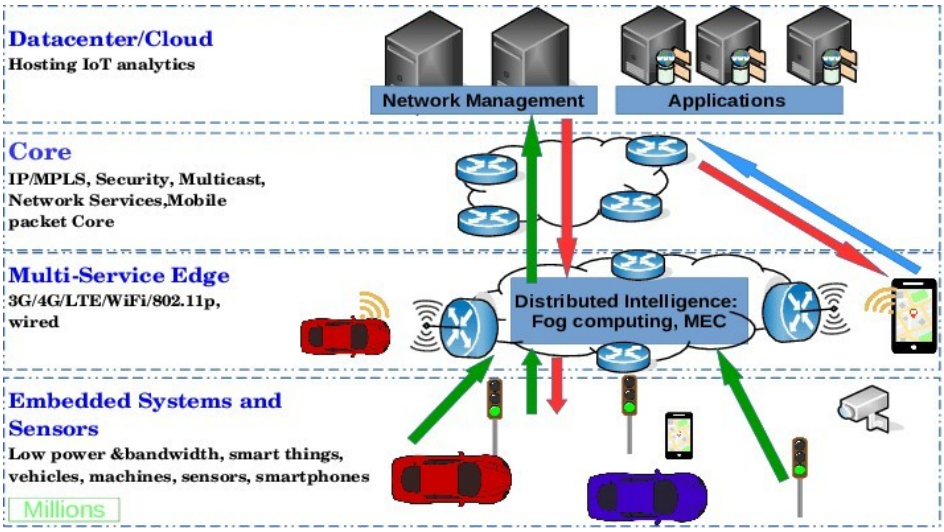

图 1: ICV 系统架构分层

表 1: 智能网联汽车系统的分层功能组成

分层分类组成
感知层智能交通设施交通信号灯、路边单元、交通控制中心等
车载外接设备 wifi、蓝牙、车载终端等。车载外部传感器雷达、超声波传感器、摄像头等。
决策水平 智能驾驶系统传感器融合算法决策算法操作系统
计算平台等软硬件
控制层系统电控单元电控单元软件、硬件等。车辆执行系统发动机/电机、转向电机等。

巴黎，法国，2018 年 11 月 20-22 日，Proceedings)。在物理层，ICV 系统架构可分为四层:交通设备层、车辆智能系统与外部内接口层、车辆网络控制层和车辆组件执行层。从功能上看，智能网联汽车系统分为感知层、决策层、控制层和执行层。各层涉及的设备或部件如表 1 所示。各层之间相互协调分工，其交互安全性极为重要。

3 车联网信息交互系统的安全威胁

车载信息交互系统由信息安全防护(远程信息处理器)和车载信息娱乐系统(IVI)两部分组成。其原理图如图 2 所示(图片引用自《基于边缘计算的路边智能信息交互系统的设计与实现》)。它主要提供对外通信、远程控制、信息采集、定位防盗等功能视听娱乐等功能[3]。由于其系统的复杂性、外部接口的多样性以及 CAN 总线信息的可读写性，更容易被攻击者利用，造成信息泄露，甚至影响车辆的安全驾驶。

车辆信息交互系统面临的威胁包括硬件安全威胁、通信协议和接口安全威胁、操作系统安全威胁、应用软件安全威胁和数据安全威胁。

3.1 硬件安全威胁

汽车零部件厂家在进行信息安全保护和 IVI 时，为了方便调试，在器件 PCB 上预留了一些调试端口，如 JTAG、UART、USB 等调试端口。通常，这些调试端口的信息是不加密的[4]。接口，可以登录系统，甚至获得 root 权限，导致系统中用户数据泄露的风险，更严重的是通过篡改系统内部文件来控制车辆动力系统。

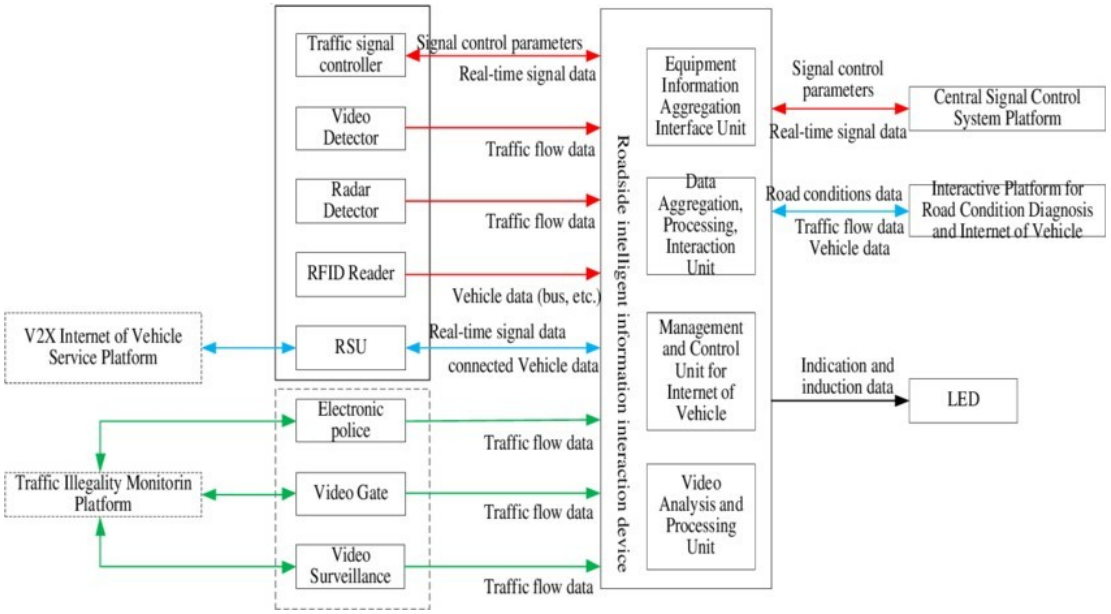

图 2: 车辆信息交互系统

3.2 通信协议的安全威胁

通信协议包括外部通信协议和内部通信协议。外部通信协议包括公共远程通信协议(如 HTTP、FTP 等)、私有远程通信协议、蓝牙通信协议、Wi-Fi 通信协议等。内部通信协议主要是 CAN 总线协议和以太网协议。无论是外部通信协议还是内部通信协议，都面临着被攻击的安全威胁。

3.3 操作系统安全威胁

网联汽车的操作系统主要是嵌入式 Linux、QNX 和 Android 操作系统。然而，这些操作系统使用的代码非常复杂，不可避免地会导致安全漏洞[5]。因此，操作系统存在安全漏洞，这将导致车联网。系统面临被恶意入侵和控制的风险。操作系统除了面临自身漏洞的威胁外，还面临系统权限升级、操作系统升级文件被篡改等威胁。某些汽车操作系统保留了管理员权限，攻击者可以通过命令获取管理员权限，查看或修改系统中的文件。

3.4 应用软件安全威胁

调查显示，目前市场上车载信息交互系统配套的应用软件和联网汽车远程控制应用软件普遍缺乏软件保护机制和安全保护机制。大多数车辆都是这样不限制安装未知应用软件，甚至保留浏览器的隐藏入口，使黑客可以通过浏览器下载恶意软件，从而对车载信息交互系统发动攻击。

3.5 数据安全威胁

车联网数据安全也面临着各种威胁。联网汽车数据包括车主的个人敏感数据、位置信息和 Wi-Fi 密码。大多数联网汽车数据都是通过分布式技术存储的。但是，有些厂家在存储数据时没有对数据进行加密，攻击者很容易通过系统漏洞窃取、访问和非法使用数据。

4 智能网联车辆信息安全防护系统设计

4.1 体系结构设计

本文提出了一种车辆信息安全威胁识别方法，通过构建各个层面的攻击面，提高威胁识别的准确性和覆盖范围，从而更准确、全面地识别智能网联车辆面临的信息安全威胁。图 3 显示了基于计算机的智能网联汽车分层安全威胁识别方法的流程(图片引用自 C-ITS 环境下自动驾驶汽车传感器大数据处理系统实现)。

通过该方法，可以识别 ICV 体系结构各层的信息泄露、信息篡改、拒绝服务、欺骗、重放攻击和拒绝操作。

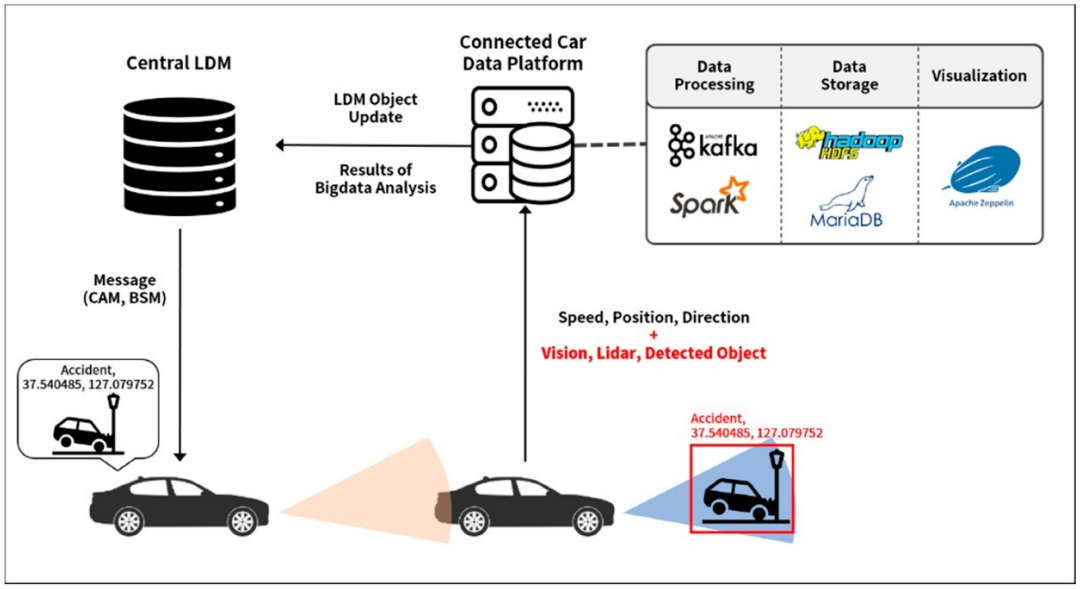

图 3: ICV 安全识别方法

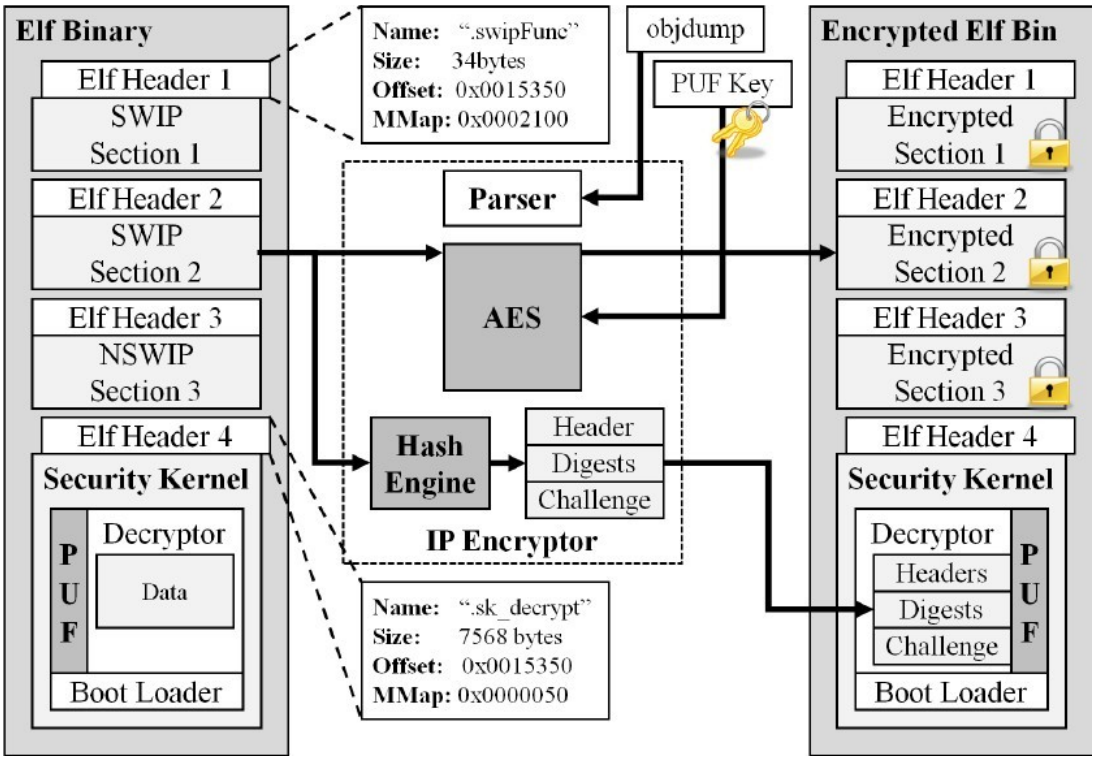

图 4: ELF 二进制保护功能图

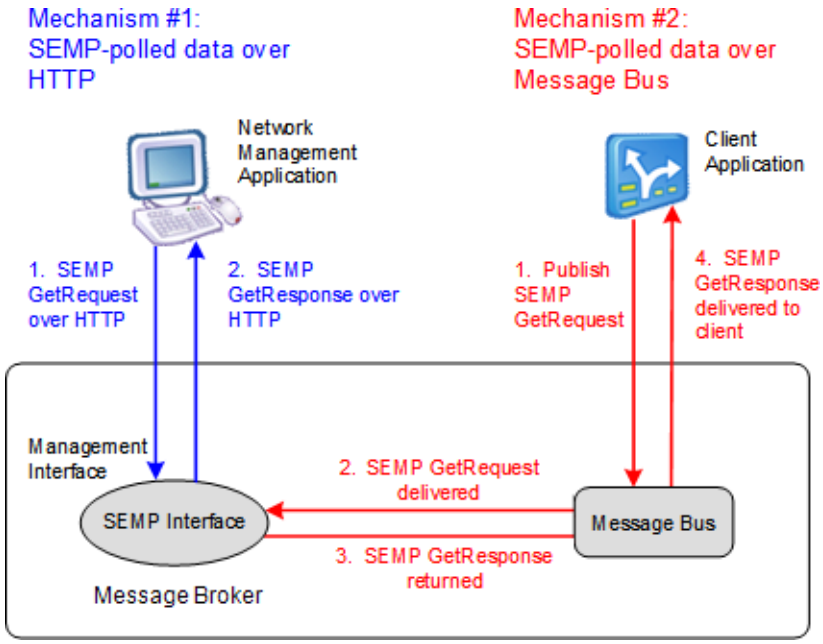

图 5: 总线消息处理机制

4.2 功能设计

4.2.1 信息安全保护系统的安全监控功能。端口扫描检测、本地权限升级检测、系统库篡改检测、流量监控、进程注入检测、进程调试检测、缓存文件篡改、恶意程序扫描、系统登录用户检测[6]。端口扫描检测是对信息安全保护系统中运行的端口进行自检，关闭部分存在安全隐患的端口服务;同时，根据服务器的配置策略，可以限制外部访问的 IP，以保证信息安全保护系统的安全性。本地权限升级检测是对信息安全保护系统中运行的程序的权限进行合理的分类和组织，从而发现具有不合理权限的隐藏安全程序。　系统库篡改检测是针对系统中的 I/O 库、ssl 库等关键系统库，对其他动态运行的二进制哈希值与内存扩展后文件形式的二进制哈希值进行匹配、挂钩检测和篡改检测。进程调试和注入检测是检测系统中运行的程序的状态位，查找可疑的停止状态位;同时，对程序映射空间的快照进行比对，找到被注入的程序。缓存文件篡改是为了识别程序缓存安装目录中每个文件的用户 ID。如果发现异常的用户 ID 文件，则说明缓存文件已被篡改。恶意软件扫描是基于服务器端安全知识库的比对和检测。

4.2.2 信息安全防护体系性能监控

荷兰国际集团(ing)的功能。　包括 CPU 占用率、内存占用率、资源占用率等相关信息，为服务器平台的信息安全保护提供辅助数据。

4.2.3 信息安全防护网络监控功能。流量攻击监控为服务器分析平台评估信息安全防护网络异常提供了可靠的数据源。连通性攻击是识别信息安全防护系统网络接口的 SOCKET 连接类型，阻断 SYN flood 攻击，以保证信息安全防护系统的安全。

4.2.4 车载应用保护。对于信息安全保护的核心程序，提供 ELF 二进制保护和应用安全加固，防止信息安全保护的核心程序被逆转后泄露隐私数据[7]。ELF 二进制保护功能如图 4 所示(图片引用自保护商品和遗留嵌入式系统的软件知识产权)。

4.3 网关的设计

在标准的汽车网络中，网关采用 CAN、LIN、Flex Ray 等实现各 ECU 之间的数据交换。基于 CAN 本身的数据广播机制和无数据验证的缺陷，它很容易受到 DoS 攻击。为了对车辆起到保护作用，采用最安全的车辆网络模型。为了保护车辆总线不受外部网络攻击的干扰，在总线应用程序中选择了一个安全控制节点。基于车载自动诊断系统(ODB)和互联网汽车总线的应用

系统的信息安全保护接口，它利用安全控制中的机制拦截系统外部信息，从而直接控制汽车总线[8]。 该部分主要通过独立网关对 DoS 进行过滤。的攻击;需要控制的合法请求可以添加到可信类型模型中。网关采用硬件隔离技术，隐藏网关信息，不暴露网络通信。无线通信与网关之间采用不同的微控制器，同时进行隔离，并且必须保证总线网络与无线网络之间的物理隔离，然后进行单元判断和转发，在中断程序中判断诊断请求的来源，然后开始做出特定的转发响应，避免总线信息泄露和转发错误。并有效保护用户车辆数据信息的保密性和安全性。它的处理机制如图 5 所示(该图引用了使用 SEMP 管理和监视事件代理)。

5 结论

本文提出了基于人工智能技术的智能车联网数据保护解决方案，将基站连接到分布式人工智能技术中，有效地解决了时延高、可扩展性差、时延低等问题

保证了用户数据存储的统一性和协调性，为车联网的数据安全防护提供了新的思路。

参考文献

[1] 郝晶晶，韩光兴。智能网联车辆信息安全威胁识别与防护方法研究。现代电子技术，第 44 卷，第 65-71 页，23 2021。
[2] 李芳丽，吴小建。智能网联汽车通信终端信息安全加密方法仿真计算机仿真，vol.37, pp. 54-59, 2020 年 5 月。
[3] 赵世嘉，徐可，宋娟，等。我国智能网联汽车操作系统开发实施策略科技管理研究，第 40 卷，第 59-61 页，2020 年 9 月。
[4] 李玉峰，陆晓远，曹晨红，等。智能网联车辆的网络安全分析。电信科学，第 36 卷，第 108-114 页，2020 年 4 月。
[5] 陈义松，邢云祥，熊晓琴，等。基于专利分析的智能网联汽车技术经济评价体系研究。汽车工程，第 43 卷，第 79-82 页，2021 年 9 月。
[6] 李克强，常学阳，李佳文，等。智能网联汽车云控制系统及其实现。汽车工程，第 42 卷，第 111- 115 页，2020 年 12 月。
[7] 陈伟，杜鲁尧，孔海洋，等。智能网联车辆定位的协同地图匹配算法。交通信息与安全，vol.39, pp. 10-15, June 2021。
[8] 吴武飞，李仁发，曾刚，等。智能网联汽车网络安全研究综述。通信学报，第 41 卷，第 14-19 页，2020 年 6 月。