文章编号：2095-2163(2022)05-0129-03 中图分类号：TP319 文献标志码：A

自动驾驶环境下的网络安全预警系统设计

姜明宇，张翠平，金子潇
（北京信息科技大学 计算机学院，北京 100101）

摘 要：目前，智能网联汽车受到了越来越多的关注。与此同时，由于互联网功能的加入，就使得智能网联汽车的稳定安全运行会对人们的生命财产安全带来一定影响。而目前应用的预警系统可能对一些低严重程度的较大规模攻击并不敏感。本文即以 RCRI 与相关理论分析为基础，研究自动驾驶环境下的网络安全预警系统，并实现了基本的视觉预警以测试系统基本可行性。

关键词：自动驾驶；网络安全；预警；系统设计

System design for network security early warning under automatic pilot environment

JIANG Mingyu, ZHANG Cuiping, JIN Zixiao
(Computer School, Beijing Information Science and Technology University, Beijing 100101, China)

【Abstract】 At present, intelligent networked vehicles have received more and more attention. At the same time, due to the addition of Internet functions, the stable and safe operation of intelligent networked vehicles will have a certain impact on the safety of people's lives and property. However, the currently applied early warning system may not be sensitive to some large-scale attacks of low severity. Based on RCRI and related theoretical analysis, this paper studies the network security early warning system in the autonomous driving environment, and implements basic visual early warning to test the basic feasibility of the system.

【Key words】 automatic pilot; network security; early warning; system design

0 引 言

随着交通智能化、自动化的快速发展，自动驾驶已经是未来交通系统的重要组成部分，其在减少尾气排放、交通拥堵与交通事故方面有巨大潜力。而有关自动驾驶安全性研究一直是学术界和工业界共同关注的热点课题。实际上，交通安全与人民的生产生活密切相关。但是，作为一项复杂工程，自动驾驶技术严重依赖于移动互联网，这就使其也有可能成为网络攻击的一个对象。因此，研究自动驾驶环境下的网络安全预警系统具有重要的实际意义。

当前，针对自动驾驶环境下的安全风险方面已经有一些研究[1]。吕颖等人[2]针对自动驾驶车辆项目开发特点，提出一种结合通用软件开发过程标准与敏捷开发过程的面向汽车自动驾驶软件安全开发的流程，并应用在实际自主软件开发项目中。代珊珊等人[3]提出了一种基于动作约束的软行动者-评论家算法对环境奖赏进行了合理限制，使无人车尽量避免陷入危险状态。结果表明，引入安全机制的 CSAC 方法可以有效避开不安全动作，提高自动驾驶过程中的稳定性。陈吉清等人[4]基于国家车辆事故深度调查体系中的事故数据，根据交通环境要素和测试车辆基础信息选取了若干场景要素，通过聚类分析方法对车辆交通事故数据进行了分析，提出并分析了危险事故特征。但是，这些内容都是针对自动驾驶车辆在常规行驶过程中遇到的安全风险展开研究。实际上，黑客攻击一直都是网联环境安全的重要风险因素[5]。对于自动驾驶环境下黑客攻击的交通流演化特性，研究者们从数值模拟[6]和解析分析[7]的角度进行了研究，但是却并未根据这些特性进行系统设计与开发。基于此，本文则是在自动驾驶环境下针对黑客攻击来进行安全预警研究，并进一步就系统设计与开发给出了有效解决方案。以期从实际应用的角度为国内无人驾驶安全风险研究提供有益参考。

基金项目：北京信息科技大学 2021 年大学生创新创业训练计划项目(5102110805)。

作者简介：姜明宇(2000-)，男，本科生，主要研究方向：大数据与智能交通；张翠平(1984-)，女，博士，讲师，主要研究方向：计算机应用技术、大数据与智能交通；金子潇(2000-)，男，本科生，主要研究方向：大数据与智能交通。

通讯作者：张翠平 Email：cpzhang@ bistu.edu.cn

收稿日期：2021-11-22

1 车辆跟驰模型

在 Li 等人[6]的研究中,使用了 PATH 模型。为使得论文具有更好的完整性和可读性,简要介绍 PATH 模型如下:

$$e_k = x_{k-1} - x_k - L_{k-1} - t_{hw}v_k \tag{1}$$

$$v_k = v_{kprev} + k_p e_k + k_d e_k' \tag{2}$$

$$x_k = x_{kprev} + v_k \Delta t \tag{3}$$

其中, e_k 表示目标车辆间隙误差; e_k' 表示间隙误差导数; x_{k-1} 表示前面 $k-1$ 车的位置; x_k 表示目标车辆位置; L_{k-1} 表示 $k-1$ 车的长度; t_{hw} 表示当前设置的时间间隔; v_k 表示目标车辆的速度; v_{kprev} 表示前一次迭代中目标车辆的速度; k_p 和 k_d 为模型系数,在研究中分别为 0.45,0.25; Δt 表示迭代时间步长。

该模型有物理学理论依据,有一定的参考价值。但是,在实际情况中,可能还有其他因素会对数据造成影响。

2 风险识别

指标 RCRI(Rear-end collision risk indexes)建立了纵向安全与车辆动态行驶轨迹数据间的关系。在 Ye 等人的研究中,使用了基于安全停止距离的 *RCRI* 指标,此处需用到的数学公式如下:

$$SSD_L = S + \frac{v_L^2}{2\,d_m} \tag{4}$$

$$SSD_F = v_F\,t_d + \frac{v_F}{2\,d_m} \tag{5}$$

$$RCRI = \begin{cases} 0(\text{安全}) & SSD_L > SSD_F \\ 1(\text{危险}) & \text{其他} \end{cases} \tag{6}$$

其中, SSD_L 表示前车停车距离; S 表示前车与后车间隙距离; v_L 表示前车速度; d_m 表示减速率; SSD_F 表示后车停车距离; v_F 表示后车速度; t_d 表示延时[1]。

基于此,在生成 IDM 模型的模拟数据中,可根据车辆类型标记,带入不同的延时参数,计算各个迭代周期内的 *RCRI*, 即各个迭代周期内的碰撞风险指数。

3 安全预警

本文的研究目标就是采用基于 *RCRI* 的预警。与传统的基于阈值的预警方式不同, 基于 *RCRI* 的预警可能对针对位置数据的攻击以及攻击程度较轻、但受攻击车辆较多的情况有更可靠的表现。

根据 Li 等人[6]的研究结论可知,较低严重程度的攻击可能对大多数车辆造成影响,从而导致单一某一辆车的风险比例下降,因此,针对位置数据的攻击可能比针对速度数据的攻击影响更大。另外,在更多的车辆受到低严重程度的攻击时,情况可能比更少的车辆受到较高严重程度的攻击时更加严重。这就意味着黑客可能对多辆智能网联汽车发起低严重程度的攻击,其严重程度依然不小。但在这种情况下,传统的基于阈值的预警系统可能无法触发预警,因为攻击的严重程度并未达到阈值。而基于 *RCRI* 的预警系统就可以有效应对这种情况发出预警。

4 UI 设计与实现

本系统开发基于 Qt 开发框架、OpenGL 图形库与 QChart 图表组件。

Qt 是一个跨平台的 C++图形用户界面应用程序开发框架。PyQt 是 Qt 的 Python 绑定。使用 PyQt5,可以在 Qt Designer 中通过拖动快捷的以面向对象的方式构建 UI,再使用 PyQt5 提供的工具编译为 Python 代码,即可通过 Python 进行调用。

OpenGL 是一个用于渲染 2D、3D 图形的开放图形库,利用图形加速硬件得以高效实现,支持多种平台,传入模型数据,使用 GLSL 语言编写着色器程序,即可渲染 2D/3D 图形(参见图 1)。PyOpenGL 是对应的 Python 绑定,支持通过 Python 调用接口函数来高效渲染图形。

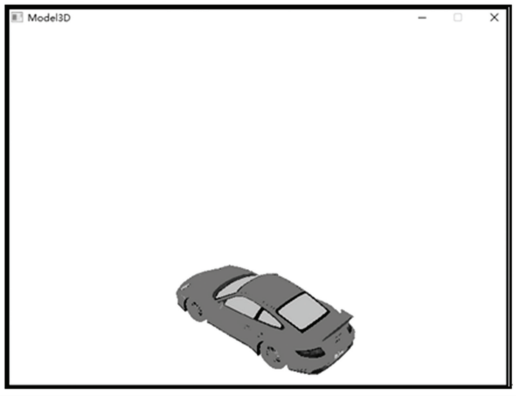

图 1 OpenGL 渲染 3D 图像示例

Fig. 1 An example of rendering 3D images by OpenGL

QChart 是一个易用的图表组件,可通过简单的接口调用,就能快速实现如折线图、柱状图、雷达图、饼图等图表。

UI 示例如图 2 所示。在图 2 的预警系统 UI 中,左边部分使用 PyOpenGL 实时多线程渲染每一

个模型，可视化显示周围行车信息。在模型渲染区域上方，叠加 QPainter 渲染层，显示当前车辆的速度、转向指示等基本信息。

UI 右边部分为数据可视化区域，包含着网络状况、车流密度、速度、跟车间隙等关乎安全的信息，在数据图中间，放大的数据图显示最终计算的 *RCRI*，这是主要的预警基础，下面亦会提及。除此之外，数据图表还支持基本的交互，如互换位置实现不同数据的放大显示、某一个数据图表的单独放大显示。

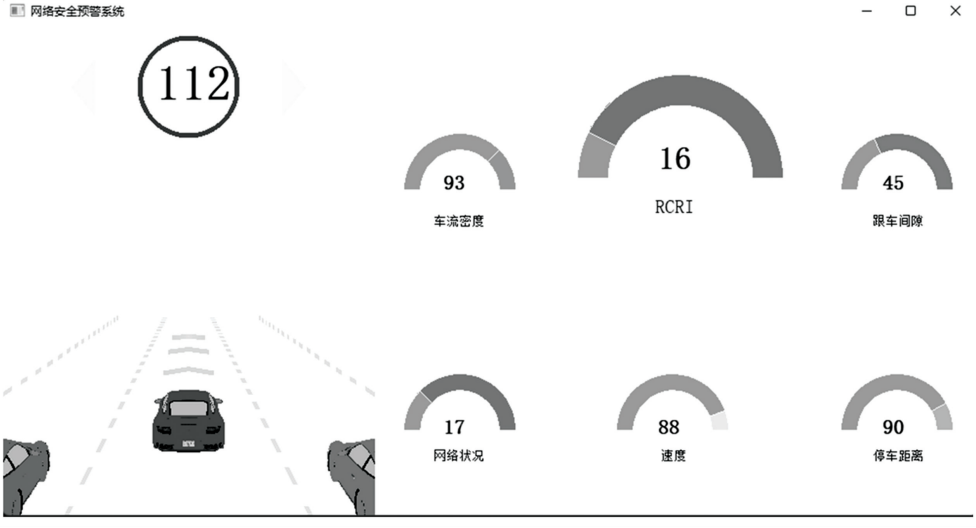

图 2　UI 示例

Fig. 2　The example of UI

在 UI 设计中，最基本的实现预警的方法就是视觉预警。在数据图表部分，通过简单的颜色变换，实现了基本的视觉预警，以满足研究阶段验证系统可行性的需求。在实际应用中，还可以根据硬件条件，结合其他领域的方法，实现声音预警、触觉预警等。

5　结束语

在本次的研究中，设计了一个自动驾驶环境下的网络安全预警系统，并实现了基本的视觉预警以测试系统基本可行性。但实际应用中，仅研发出视觉预警还远远不够，预警方式也并非本次研究的重点，论文在研究中主要是进行了跟驰模型的建立、以及从识别风险到发出预警的技术实现。将来，还要结合人机交互学、生物学、生理学等方面的经验对预警方式进行研究。

参考文献

[1] 窦文悦，胡平，魏平，等. 无人驾驶安全风险的识别与度量研究[J]. 中国工程科学，2021，23(06)：167-177.

[2] 吕颖，厉健峰，杨斯琦，等. 面向汽车自动驾驶安全软件的开发流程[J]. 汽车文摘，2021(10)：47-51.

[3] 代珊珊，刘全. 基于动作约束深度强化学习的安全自动驾驶方法[J]. 计算机科学，2021，48(09)：235-243.

[4] 陈吉清，舒孝雄，兰凤崇，等. 典型危险事故特征的自动驾驶测试场景构建[J]. 华南理工大学学报(自然科学版)，2021，49(05)：1-8.

[5] 刘宝旭，许榕生. 黑客入侵防范体系的设计与实现[J]. 计算机工程，2003(12)：34-35，44.

[6] LI Ye，TU Yu，FAN Qi，et al. Influence of cyber-attacks on longitudinal safety of connected and automated vehicles[J]. Accident Analysis and Prevention，2018，121：148-156.

[7] WANG Pengcheng，WU Xinkai，HE Xiaozheng. Modeling and analyzing cyberattack effects on connected automated vehicular platoons[J]. Transportation Research Part C：Emerging Technologies，2020，115：102625.