acknowledgement

我必须感谢我的导师Shreejith教授以及他的学生Shashwat博士，感谢他们在这个工作中为我提供的支持，没有他们热情耐心的帮助与指导，我无法完成这项工作。当然也非常感激他们向我提供的研究所用的软件和硬件的资源支持，以及参加行业领先技术交流会的机会以及在学术会议上发表论文的机会。非常感谢我的服务在我最需要心理和资源支持的时候，永远能够成为我最坚强的后盾。同时也要感谢我们专业的其他同学们，这让我在此工作中感到没有那么孤单。

I must thank my mentor Professor Shreejith and his student Dr. Shashwat for their support in this work. Without their enthusiastic and patient help and guidance, I would not be able to complete this work. Of course, I am also very grateful for the resource support they provided me with for the software and hardware used in my research, as well as the opportunity to participate in industry-leading technical exchanges and publish papers at academic conferences. I am very grateful for their service, which has always been my strongest backing when I need psychological and resource support the most. I also want to thank other students in our major, which made me feel less lonely in this work.

Abstract

近年来，为了提升性能和用户体验，车载智能设备的开发逐渐复杂化，这也意味着更多关键、安全的功能将被集成到系统中。系统的可靠性和安全性是必须考虑的因素，任何针对车载系统关键功能的攻击都可能带来严重后果，甚至危及乘客的生命。本研究提出了一种用于汽车总线的灵活的硬件在环仿真系统，用于在FPGA上模拟和测试多个ECU之间的CAN总线通信，并建立了自动化攻击注入平台，并通过引入成熟的量化神经网络攻击检测模型对此硬件在环仿真系统进行了验证，这对于加速车载总线结构更新后的硬件在环仿真测试和辅助更新及验证既往研究的攻击检测模型具有一定的意义。

In recent years, in order to improve performance and user experience, the development of in-vehicle smart devices has become increasingly complex, which also means that more critical and secure functions will be integrated into the system. The reliability and security of the system must be considered. Any attack on the critical functions of the in-vehicle system may have serious consequences and even endanger the lives of passengers. This study proposes a flexible hardware-in-the-loop simulation system for automotive buses, which is used to simulate and test CAN bus communications between multiple ECUs on FPGA, and establishes an automated attack injection platform. This hardware-in-the-loop simulation system is verified by introducing a mature quantitative neural network attack detection model, which is of certain significance for accelerating the hardware-in-the-loop simulation test after the in-vehicle bus structure is updated and assisting in updating and verifying the attack detection model of previous studies.

* 1. Introduction

硬件在环 (HIL) 是一种实时仿真技术，用于测试复杂的嵌入式系统，特别是在汽车、航空航天相关领域。它将实际硬件组件与模拟模型集成在一起，以创建闭环测试环境，从而能够在全面部署之前全面验证和确认系统性能。

近年来，随着智能汽车工业的迅猛发展，为了满足日益复杂的智能驾驶与交互需求，提高汽车产品的智能化、舒适性，越来越多的车载设备被集成到汽车总线中，并且其物联网程度的提升也丰富了其通讯接入方式，这同时也对通信过程的安全性提出了挑战。为了解决车载总线快速迭代以及随之而来的硬件在环仿真可靠性测试的困难，本研究通过在FPGA上集成灵活的ECU软核，提出了一种新的面向汽车总线的硬件在环仿真解决方案。同时，本研究实现并集成自动化攻击向量注入功能并借用成熟的量化神经网络对该系统进行的功能验证，为加速汽车产品通信测试进程、提高车载总线安全性提供了更为可实践的解决方案。

* 1. Aim of the project

在这项研究中，我们的目标是为车辆 ECU 构建一个硬件在环仿真环境，使用microblaze软核处理器作为每个 ECU 的计算内核，构建虚拟的CAN总线网络。基于此硬件在环仿真车载总线网络，在仿真框架中整合自动化攻击注入能力，例如DoS、重放和欺骗攻击，并借用量化神经网络模型进行攻击检测，对该仿真环境予以验证。

该系统主要由三部分组成，系统结构如下图所示，分别是用于硬件仿真的 FPGA 部分、用于数据采集监控和测试的计算机软件部分、用于仿真和测试的网络部分以及用于仿真和测试的外部传感器设备和其他可扩展的硬件在环仿真系统。

第一部分，硬件仿真FPGA，我们使用一块Nexys Vedio FPGA板，在板上搭建4个microblaze核心仿真ECU，每个ECU独立运行其应用程序，通过AXI总线与其他外设连接，通过开源CAN控制器核心和CAN总线发送器与接收器建立CAN总线连接。桥接节点用于FPGA仿真环境与软件测试平台间的通信。DNN核心搭载在microblaze核心上，用于我们实时监控并验证CAN总线上发生的数据，并将结果送回仿真软件平台。

在第二部分，也就是PC部分，我们将构建一个自动化测试程序，可以访问我们预先准备的测试配置文件、ECU应用程序目标代码、测试用例和测试数据库。通过人机交互界面，我们可以实现对测试过程数据的实时监控，将我们的基本测试配置和目标代码下载到测试环境中，并执行预先准备的测试用例对环境中的硬件CAN网络进行攻击。

第三部分是硬件在环仿真和其他物理设备的扩展接口，通过这个接口，我们可以协同多个硬件在环仿真系统，加速仿真效率，扩展CAN网络模型的复杂度，从而对抗单个FPGA上LUT数量有限带来的限制，使ECU能够访问真实的传感器和输出设备，从而实现对更复杂环境的仿真。

该项目如期开展，符合项目计划以及里程碑预期，并且在部分先前未规划的部分取得了一些研究成果，无明显的偏差。

车辆系统各子系统ECU通常以总线形式连接，1990年左右出现了许多汽车总线协议，如Flex Ray、LIN、CAN总线等，其中，目前国际上应用最广泛的开放总线是博世公司提出的CAN总线[1][2]。

1. Literature Review

汽车通信领域的硬件在环仿真系统及其通信安全测试问题一直是一个重要且被广泛研究的问题。在本研究中，我们的工作主要涉及以下四个主要方面：硬件在环仿真、虚拟ECU技术、车载攻击注入、车载攻击检测。我们将重点评估和分析先前在这四个方面的研究。

2.1

3.1