**第一章 绪论**

**1.1 研究背景与意义**

随着5G通信、云计算、大数据、人工智能等高新科技在社会的各个领域均得到了大量的应用，传统的汽车行业也朝着智能化网联化的方向发展，智能网联汽车应运而生。智能网联汽车配备先进的车载传感器、控制器、执行器等设备，集成现代通信和网络技术，实现车辆与车辆、车辆与道路、车辆与人、车辆与云等之间的智能信息交换以及共享汽车智能网络连接。

据统计，截至2021年9月，全国机动车保有量达3.9亿辆，其中汽车2.97亿辆；全国机动车驾驶人4.76亿人，其中汽车驾驶人4.39亿人，中国机动车保有量、驾驶人总量及增量，稳居世界第一[1]。从统计数据来看，汽车行业毫无疑问的具有非常广阔的发展前景。面对智能联网汽车发展的大趋势，来自国内外的各大公司纷纷开始布局智能网联汽车行业，国外的以谷歌、苹果、英特尔等美国互联网公司为代表的IT巨头不遗余力地投资于汽车智能驾驶技术领域；国内的例如百度与吉利汽车成立智能汽车公司，以整车制造商的身份进军汽车行业、华为计划与北汽、广汽、长安汽车合作造车以及小米成立小米汽车有限公司宣布正式开始造车等等大型互联网公司纷纷开始进入智能汽车行业。

智能网联汽车的发展趋势使的车辆内部的开放性大大得到增强，车辆内部与外部通信的接口包括USB、蓝牙、WIFI等均得到了广泛应用，使得车辆内部网络与外部信息网络的交互性得到进一步增强，因此，车辆内部受到攻击的风险也随之增加。与此同时，智能网联汽车的发展也促使车内电子系统网络的复杂程度迅速增加。据Strategy Analytics机构报告统计，汽车内部使用的电子控制单元（Electronic Control Unit，ECU）数量在过去的十年间增速很快，当前汽车普遍拥有几十个ECU，更高级的汽车甚至使用上百个ECU，这必然加大了汽车内部相关电子设备以及运行网络被黑客攻击的风险，智能联网汽车也将面临着和互联网相似的信息安全方面的问题。相比于传统的互联网信息安全，智能联网汽车面临的信息安全问题会更加的严峻。2015年两名网络安全专家Valasek和Miller远程攻击了Jeep切诺基的车载娱乐系统，获取了CAN总线报文的收发权限，通过发送一系列错误指令，导致该车冲入路边斜坡，该事件导致菲亚特克莱斯勒汽车公司召回了大约140万辆汽车[2]。2016年,Keen lab入侵了特斯拉汽车的车载中控，对其进行远程操控，使正在驾驶中的Model S突然刹车[3]。2019年，腾讯科恩实验室发现了特斯拉驾驶系统中存在的缺陷，利用图像生成技术来干扰自动雨刷的工作，通过已知漏洞得到车辆的驾驶控制权，进而操纵车辆[4]。

随着汽车与外部进行通信的接口逐渐增加，汽车受到攻击的方式也越来越多，但无论汽车受到何种方式的攻击，若想完全的控制汽车，最终攻击点往往都是破坏或控制CAN总线上正常报文的接收与发送，从而对汽车的正常运行进行控制。CAN总线通信作为汽车底层通信网络，其通信安全直接影响到整车运行的安全。

然而，现实情况是CAN总线协议当初被设计的初衷是用来满足车辆内部的串行实时通信，距今已经有30多年。在设计之时，车辆还仅是一个完全封闭独立的系统，设计之初并没有考虑到如今车辆的网联化和开放化。而且，为了保证车辆内部各ECU之间能够进行实时通信，CAN总线上报文的长度设计的很短而且不存在加密措施。所以，CAN总线上的信息完全的以明文在进行传输，严重缺乏通信安全防护手段。

综上，汽车信息的安全问题正面临着非常严峻的挑战，已经成为不能不重视的问题，车载CAN总线网络信息安全是保障汽车信息安全中非常重要的环节，针对车载CAN总线网络信息安全问题的深入研究将有利于设置相应的安全防护机制，保护车载人员的生命财产安全，还有利于促进智能网联汽车信息安全技术的发展，具有重要的价值以及现实意义。

**1.2 国内外研究现状**

自从智能网联汽车这个概念出现以后，智能联网汽车的信息安全问题越发的引起国内外的关注，而CAN总线网络的信息安全是保障智能联网汽车信息安全的基石，如何能够保证CAN总线信息的安全问题是今后汽车发展的最重要的一步。为此，国内外的专家学者纷纷开始研究CAN总线信息安全的问题，主要包括以下三部分：车辆系统架构、车载CAN总线异常入侵检测以及认证与加密。

**1.2.1 车辆系统架构的发展**

车辆系统架构的最具有代表性的有三个EVITA、OVERSEE以及目前使用最频繁的AUTOSAR架构。其中EVITA是由欧盟于2018年资助的一个项目，该项目的主要目的是为车载网络设计、验证以及车载架构提供一些参考，依据和参考了ISO/IEC15408和ISO/DIS26262的相关标准，起到保护重要电子控制单元免受非法篡改，保护其车载内部网络敏感数据免受损害的作用。而OVERSEE项目主要制定了一个开放式的车载信息平台，该平台提供一个受保护的、标准化的车内运行环境以及车载访问和通信点。因此，该平台的主要目标是可靠性和IT安全性，这意味着在独立应用程序之间实施强大的隔离，并确保任何应用程序都不会损害车辆功能和车辆安全。将首先根据安全风险和可靠性分析进行需求分析，然后指定并实施车载平台架构。最后，AUTOSAR，全称为Automotive Open System Architecture，即汽车开放系统架构。是由来自全球各家汽车制造商、零部件供应厂商以及各种服务、研究机构共同参与的一种汽车电子系统的合作开发框架，并建立了一个开放的汽车控制器标准软件架构。

相比于国外而言，国内这方面的研究起步比较晚。2016年9月13日，我国首个车载信息安全产业联盟（ACIA）正式成立，该联盟发起者包括东软集团、奇瑞汽车、中国信息安全认证中心、中国软件评测中心等单位。旨在建立一个健康有序的、可持续的产业环境，提高车载信息安全产业的影响力。其还将通过开展技术交流去完善业内技术标准以及提高行业整体能力，进而提升其在国际市场上的总体竞争力。2018年6月19日，北京航空航天大学，中国信息通信研究院，中国汽车工程学会等单位发布了《智能网联汽车车载端信息安全技术要求》。2020年11月13日，由中国汽车工业协会联合国内主要汽车企业、零部件供应商及汽车基础软件企业共同编撰的《中国汽车基础软件发展白皮书1.0》正式发布。2021年9月29日，发布《中国汽车基础软件发展白皮书2.0》，旨在承担国内汽车产业发展中的生态完善任务，围绕国内汽车基础软件领域中的关键标准和关键技术研究进行了深入研讨，共同构建产业新生态。

**1.2.2 车载CAN总线异常入侵检测研究**

车载CAN总线入侵检测最开始只是实时观察车内CAN总线的活动，并将其与记录到配置文件中的正常行为进行比较，当与正常配置文件中的行为偏差达到某个阈值时，就会触发下一步操作。根据不同的检测特征，可以将目前关于车辆入侵检测系统的研究主要分为三类：基于车载CAN总线网络流量的分析、基于有CAN总线报文的有效负载的分析以及车载CAN总线的电气特征的分析。

基于车载CAN总线网络流量的分析，通常是从CAN总线网络上传输的报文中提取不同的特征（例如，报文发送频率以及间隔），使用提取的特征来识别入侵或异常行为。文献[10],使用统计属性，例如均值、方差和标准偏差，在建模系统中寻找异常行为。在CAN总线网络入侵检测系统中，可以通过在CAN总线网络流量的时间序列中使用动态窗口来应用基于统计的方法。文献[11]，Müter等人，提出了基于信息熵的适用性检测CAN总线网络中流量的异常。信息熵方法采用信息论概念，通过测量给定数据集并将获得的结果用作车辆入侵检测系统。Cho和Shin[25]构建了一个基于时钟的有效入侵检测系统，它可以检测包括伪装攻击在内的各种类型的攻击。然后，文献[17]证明了基于时钟偏差的入侵检测系统容易遭受隐藏式攻击。利维等人。[6]提出了一种新的基于时间的检测技术，使用隐马尔可夫模型（HMM）和车队回归模型。收集重要数据，然后根据对车辆正常行为进行训练的 HMM 进行测试。回归模型是基于时间特征构建的，然后用于预测估计的对数似然值并将结果与​​实际对数似然值进行比较。

另一方面，基于有CAN总线报文的有效负载的分析，大部分的研究人员采用了机器学习的算法分析报文有效负载的异常行为。文献[42]提出了一种使用深度神经网络(DNN)的入侵检测系统。检测模型基于从ECU之间交换的车载网络数据包的比特流中提取的高维特征进行训练。一旦特征被训练并存储在分析模块中，所提出的系统就会检查车辆网络中交换的数据包，以确定系统是否受到攻击。Theissler [45]提出了一个集成 ML 模型来检测不同驾驶场景中的已知和未知故障。所提出的模型由两类和一类分类器组成，用于检测单变量和多变量时间序列数据中的异常。

一些研究人员通过对车载CAN总线的电气特征的分析,来识别CAN总线上被注入的恶意报文。[13]Murvay等人根据CAN总线信号的电气特性（接线电阻以及电缆长度）提出了一种基于CAN总线物理特征的入侵检测方案，该方案检精度高，但是处理过程非常耗时。[2]Choi等人提出了一种称为VoltageIDS的新型汽车IDS，它检查与CAN 总线报文对应的电子CAN总线信号的不同特征，以识别消息的发送者。从概念上讲，如果两个不同的 ECU 发送相同的消息，则由于电缆长度和布线电阻不同，物理层中的两个信号之间会出现不一致，并且随着线长的增加而增加。

在国也有很多人在这方面进行研究，浙江大学的凌从立等人[7]，提出了一种算法作为检测方案，来处理CAN总线通信流量出现的主要漏洞，主要包括DoS攻击和错误标志误用。在文献[9],哈尔滨工业大学关亚东提出基于DACHE（data field and change of）特征的入侵检测算法，即将报文数据场及其变化量作为检测特征，选择BP神经网络为入侵检测算法的分类模型。文献[55]，北京交通大学的董琛提出了两种检测算法，其中基于熵的ID入侵检测算法用来针对高量级的攻击，使用决策树的数据域来检测低量级攻击。文献[66]哈尔滨工业大学的谭凯，研究了AdaBoost和K近邻两种算法用于检测异常，并利用其模糊测试技术对该两种检验算法进行了评估。文献[12]大连理工大学的彭海德提出了一种基于ID熵和支持向量机数据关联性（SVM-DR）的检测方案，设计了车载CAN网络入侵检测装置，能够准确地应对典型CAN网络攻击。

**1.2.3 车载CAN总线认证与加密研究**

加密认证方法使用安全密钥对消息进行加密，只有拥有密钥的合法ECU才能正确解密消息，从而实现消息的加密隐藏和节点的身份认证。

[5]提出了一种简单的向后兼容广播认证协议，称为 CANAuth，它也基于 MAC。在该解决方案中，MAC 在带外通道上传输，在该通道中，比特以更高的时钟速度插入到标准 CAN 总线的采样点之间。然而，这需要修改标准 CAN 收发器。Farag [7]提出了一种解决方案，其中每条消息的有效负载都使用网络内所有节点中存在的对称密钥进行加密/解密。密钥是动态的，因为它们随着总线上的每次传输而改变，并通过建议的方案同步，例如为总线上的每次传输递增的计数器。然而，没有详细说明安全密钥再生，并且网络仅限于总线上所有消息的加密/解密密钥。最后，在这一类别中，[8] 中提出了一种基于 MAC 和有效载荷加密相结合的解决方案。计算 MAC 并将其附加到负载，然后使用对称密钥加密对连接进行加密。但是，密钥不会动态更改；它们在被视为无效之前用于一定数量的传输。这可能会导致攻击者最终通过反复试验来猜测加密密钥。[99] Halabi等人出了一种轻量级加密解决方案，该解决方案基于 CAN 帧的有效载荷和先前的密钥生成密钥，从而提供了一个强大的解决方案。每个加密密钥都与帧标识符本身相关联。每次传输带有该标识符的帧后，都会重新生成标识符的加密密钥。【101】Yeom等人提出了一种混洗算法，数据帧被分成bit，并被构造成块，然后将它们打乱以进行数据隐藏。[102]Paul等人提出了一种基于人工神经网络的异常检测方法来识别CAN总线中的非法消息。使用两种类型的攻击训练模型，使其可以有效地识别攻击。经测试，该算法在检测拒绝服务攻击和模糊攻击方面表现出很高的性能。

文献[],吉林大学刘毅设计了CAN总线通信安全协议，并将该协议分为初始化阶段和通信阶段，使用了RSA算法在汽车打火启动阶段完成了密匙初始化，融合了DES算法和BKDE-Hash算法来加密保障CAN总线通信过程中报文的传输。

文献[]，中国计量大学的齐攀提出了一种动态密钥生成算法。所有ECU在汽车启动时获取自己的瞬态值和当前时间戳，通过ECC算法完成主密钥MK的生成，并结合时间戳生成当前会话密钥对消息进行加密。当汽车熄火时，所有密匙将被删除，并在汽车下次启动时重新生成。

文献[]，湖南师范大学的罗禹使用AES加密算法，加入了同步计数器，修改帧格式，取CAN帧数据场最后一字节存放同步计数器和算法标识，虽然也起到了很好的加密效果，但是其只有一个字节的验证信息，过于短小。

文献[]，浙江大学的姚新宇等人提出了一种加密CAN报文的优化方法。首先将N位明文按照128位分成几组，然后使用AES密钥对每个组单独加密，形成密文。然后将密文按照48位分成几组，如果最后一组小于128位，低位加0。将时间戳和随机数（8 位）和哈希值（8 位）添加到每个组的低位。

文献[]，湖南师范大学的于洛等人针对汽车电子系统多功能混合特性，提出一种基于动态加密的车载CAN总线通信网络安全协议，设计了加密算法等级表以及修改消息格式并构建基于动态加密的安全协议，通过同步计数器来判断接收报文的时序逻辑。

总的来说，国内外的学术界和企业界对于智能联网汽车内部CAN总线网络信息安全的研究均取得了一系列的成果，智能网联汽车内部CAN总线网络信息的安全得到了很高的提升，但是要想实现CAN总线网络信息安全的防护变得无懈可击，这仍然还需要大量的研究与探索。

**1.3 本文主要研究的内容**

随着网联车的不断发展，汽车与外界的交互方式也变得越来越多，汽车内部信息安全问题变得越发的突出，其中车载CAN总线信息安全是保障车辆信息安全的关键点，针对于此，本文设计一种适用于车载CAN总线网络的信息安全防护机制，包括对车载入侵检测系统、安全认证以及报文加密等技术的研究和设计。本文的研究工作如下：

(1)在陈述了国内外关于车载CAN总线网络的信息安全问题的研究进展、车载CAN总线网络信息安全问题的研究现状之后，进一步的分析了CAN总线相关内容，包括车载CAN总线的体系结构、协议标准等内容。基于此分析了CAN总线协议目前所存在的安全问题以及几种常见的攻击方式。对此，提出了针对车载CAN总线网络信息安全的防护体系框架，包括车载入侵检测系统、安全认证以及报文加密技术，从而实现全面保障车载CAN总线网络的信息安全。

(2)本文设计的入侵检测系统中，不仅对报文的健康程度做出了检测，还提出了基于报文发送速率的相对熵入侵检测方案。该方案主要有三重环节：首先检查CAN总线报文的健康程度；然后分析每一个报文的发送速率，并标定正常的发送速率阈值；最后将标定好的正常报文发送速率值作为相对熵的输入数据，以此来对报文做出最终的检测并判断出其是否异常。

(3)设计了CAN总线的安全认证与加密方案。根据汽车安全完整性等级ASIL设计了对应的CAN总线报文发送安全协议；利用Blowfish对称加密算法和MD5信息加密算法实现了对CAN总线报文的加密传输；提出了一种对特定报文数据长度缩小的方案，能够很好的应用密文传输。

三角稳固技术，检测是前端，后两者为后端

ID+流量+频率

**与架构**