2018 ccs

ABSTARCT

连通性的增加增加了攻击向量。这也适用于互联车辆，其中的漏洞不仅威胁到数字价值，还威胁到人类和环境。通常，攻击者试图利用控制器局域网（CAN）总线，这是车辆内部通信最广泛使用的标准。一旦连接到CAN总线的电子控制单元（ECU）受损，攻击者可以随意操纵消息。通过CAN总线的设计，丢失的发送者身份验证使对抗性访问车辆功能具有严重后果。为了解决这个问题，我们提出了一种入侵检测系统（IDS），它使用从CAN帧中提取的指纹来识别发送的ECU。Scission利用CAN帧模拟值的物理特性来评估它是否由合法ECU发送。此外，为了检测组成的ECU，建议的系统能够识别来自未受监控和其他设备的攻击。我们表明，在对两辆批量生产的汽车和一个原型装置进行评估期间，Scission能够以99.85%的平均概率识别发送者。由于系统的稳健设计，评估表明所有误报都得到了防止。与以前的方法相比，我们显著降低了硬件成本并提高了识别率，这使该技术得以广泛应用。

1 INTRODUCTION

由于现代系统的开放性和高连通性，车载安全已成为一个主要问题。如果攻击者能够通过物理访问渗透电子控制单元（ECU），则尤其如此。这使得对手能够控制范围广泛的高安全关键功能，完全忽略驾驶员输入，如停止发动机或禁用制动器[27]。

由于要求事先进行物理访问被视为不现实[3]，因此[3,30]的作者系统地分析并利用了其他攻击表面，包括远程连接，如蓝牙和蜂窝无线电。使用这些外部向量，对ECU的攻击变得更加现实，并允许在各种车辆上执行。米勒和瓦拉塞克[31]在一辆切诺基吉普车上的工作证明了这些连接在安全性和安全性方面的缺点，这导致了140万辆汽车的召回。他们能够通过单元连接的主机访问车内网络，使他们能够控制发动机、制动器和转向等功能。

然而，由于大多数车载网络中没有安全功能，因此存在因ECU受损而导致的风险。如果没有足够的安全措施，攻击者可以从渗透的ECU或其他设备发送伪造消息。这尤其适用于控制器局域网（CAN）[10]，这是一种串行广播总线，1983年由Robert Bosch GmbH设计，未考虑任何安全特性[16]。CAN仍然是车内网络中使用最广泛的总线系统，今天的每辆车都可以找到。由于缺乏安全措施，每个总线参与者都可以传输所有可能的消息。CAN上接收此类消息的参与者将无法识别发送者，从而无法验证其真实性。

1.1 Shortcoming of security solutions at a digital level

不幸的是，由于带宽极为有限，且每条消息的有效载荷最长为8字节，因此应用消息身份验证码（MAC）等经典密码算法是不可行的。此外，安全通信需要更多的计算能力，以满足实时要求。这些限制使得在不进行任何深刻更改的情况下，很难将经典密码措施应用于当今汽车的推荐设置。为了尽可能降低安全风险，在开发过程中已经考虑了安全概念，包括硬件安全模块（HSM）或网络分区[25]。

对车辆功能的大量攻击涉及通过车辆网络的通信，因此改变了车辆上的实际流量CAN,通过在消息级别观察网络流量来检测这些变化的系统称为入侵检测系统（IDS）[28]。IDS有两种定义良好的方法，基于特征和异常的检测。前者在生产系统中更常见，根据消息模式和内容检测已知攻击。然而，由于实际攻击的信息高度特定于平台或车辆，并且在实践中很少可用，因此部署非常困难。后者，即异常检测，表征了预期的消息流量，从而可以检测异常和偏差。可以训练或明确指定预期特征[1]，从而识别未知攻击。这些系统通常存在大量误报[34]。

1.2 On the need for physics based security

物理特性可用于增强车载网络的安全性[5、6、33]。CAN信号特征的差异用于提取适于识别发送者的指纹。基于物理属性的安全性的优点是不需要额外的计算来向通信添加安全特性。信号的特性本质上由所使用的硬件和总线拓扑结构定义。这使得即使对于具有低计算能力的轻量级通信参与者（例如智能传感器），也能够实现安全性。由于这些特征是硬件定义的，因此没有物理访问权限的攻击者也很难绕过这些系统。

这些方法是对经典IDSs[16，34]的有益补充，可以检测额外的攻击并增强其鲁棒性。即使检测到的异常不会触发直接反应，例如向驾驶员发出警告[15，34]，这些发现也可以用于快速调整基于特征的系统。可以实现异常检测，例如在云中通过空中更新规则集。这样，在制造商发现并消除实施中的弱点之前，受影响的车型就可以免受新的攻击。此外，IDS可以更快地识别攻击源，从而加快漏洞消除的取证工作。与通常在车间参观期间进行的软件更新相比，这使得响应速度更快。如果制造商需要召回，这种系统还可以节省大量成本。

1.3 Contributions

在这项工作中，我们提出了SCISION（基于信号特征的发送者识别），这是一种使用CAN信号不变的物理特征来识别CAN消息来源的系统。这使得系统能够识别发送ECU是否被授权发送评估消息。因此，可以检测到异常并识别受损设备，这使制造商能够对检测到的异常做出适当反应，防止可能的重大损坏。与利用多个特性的现有方法相比，我们能够大幅降低采样率。再加上轻量级算法的使用和带宽完全可用的事实，Scission确保了成本效益的可行性。此外，还介绍了预处理步骤和稳健设计使得能够在评估期间实现高检测率而不出现误报。除了受损的ECU外，Scission还能够检测未受监控的ECU，如吉普黑客[31]中使用的，以及通常用于操纵的简单附加设备[14，20]。此外，我们补充了用于识别的不同信号特征的原因。简而言之，我们的贡献是巨大的:

    我们提出了一种基于物理特性测量的IDS，它允许我们确定每个传输消息的源ECU。

    我们提出的IDS可以部署到车内网络，因为它不会减少带宽，并且资源需求低。

    通过在汽车原型装置和两个系列车辆中的广泛测量，我们展示了我们的IDS的适用性和实用性。

1.4 Organization of the paper

在第1节的介绍和概述之后，第2节提供了有关控制器局域网的必要背景信息、信号特性的原因以及ECU之间的差异。第3节对相关工作进行了概述，并与Scission进行了比较。第4节介绍了所考虑的安全模型、指纹识别方法以及如何将其用于检测异常。在第5节中，我们对原型和两辆车的方法进行了评估。在此，分析了检测攻击模型的不同方法。第6节通过描述中断的适用性和局限性来结束本文。在第7节中，我们以最终结论结束本文。

2 BACKGROUD

2.1 Controller area network

CAN是一种广播车辆总线，由Robert Robert GmbH于1983年设计，旨在降低车辆电缆束的成本。它用于用两根双绞线（高、低）互连多个ECU，双绞线在每一端以120Ω 电阻。如果总线上存在隐性位（1），则向两条线路施加2.5 V的电压。在传输主导位（0）的情况下，高压线朝5V方向驱动，低压线朝0V方向驱动。每当传输五个类似位时，为了同步目的插入一个相反的位，称为填充位。CAN帧的信号如图1所示，其中CAN高电平显示为蓝色，CAN低电平显示为红色。

数据通过能够承载8字节有效载荷的CAN帧传输。帧包含唯一标识符，表示以下数据的优先级和含义。不存在节点地址。此外，还可以使用扩展标识符格式，该格式允许将标识符从11位增加到29位。这将导致格式略有变化，因为除了扩展标识符外，还将插入两个附加位。

由于CAN是广播总线，多个总线参与者可以同时访问总线。在这种情况下，占主导地位的比特占上风，比特被覆盖的参与者取消传输。由于标识符仅由一个ECU使用，因此确保在标识符完全传输后，只有一个设备访问总线。一旦总线再次空闲，中断的ECU将重新启动传输。因此，该仲裁阶段的位可能受到多个设备的影响，在使用信号进行识别时必须考虑到这些设备。

2.2 Cause of the signal characteristics

模拟信号偏离理想的理论平方信号有几个原因。如[41]所述，其中一些原因是母线端接、直流和交流电压以及接地。

我们的实验表明，我们可以通过包含不同ECU的电压源来扩展该列表。Cho等人[5]的工作中描述了电压输出的变化。在那里，由于ECU电压调节器的车内变化，使用电源和接地电压的变化来识别消息源。它们还描述了CAN收发器标称电源电压的这些变化如何导致不同的CAN高主电压和低主电压，以及导通电阻的瞬态变化如何反映到CAN总线

此外，CAN总线的所有内置部件都会发生自然变化。例如，电阻器的误差容限为行业典型的5%，这也会导致CAN总线指纹的变化。除了先前解释CAN总线上模拟信号变化的工作外，我们还指出了信号反射的方向。当信号在电缆上传输时，会发生信号反射，其中一些信号功率由于引起阻抗失配和电缆特性非线性变化的缺陷而反射。例如，这些缺陷的一个原因是振铃，这在汽车行业是众所周知的，特殊收发器试图将振铃降至最低[23]。但是，尽管做出了所有努力，由于混合总线拓扑、终端和短截线长度的变化，信号反射只能最小化[32]。总之，我们确定了可用于提取can指纹的以下信号特征源：

i） 电源电压的变化，

ii）接地的变化，

iii）电阻器、终端和电缆的变化，

以及iv）总线拓扑中导致反射的缺陷

3 Related work

由于需要额外的资源或需要复杂的硬件修改，在CAN上应用消息身份验证的已知方法[12、29、40]无法轻松应用

Herrewege等人[40]提出了一种通过使用CAN+协议提供消息认证的方法[43]。由于拟议的协议变更，在不进行深刻修改的情况下应用这样一个系统是不可行的，需要对每个ECU进行软硬件调整。

Groza等人[12]和Lin等人[29]通过发送额外的消息来提供消息身份验证。这会导致更高的总线负载，从而减少特定于应用程序的数据的可用带宽。CAN中可用带宽的减少，特别是对于现有系统，具有潜在的广泛后果。这是由于这样的情况，即此类通信系统经过精心规划，包括定义的带宽储备，以满足实时和安全要求。在设计通信时，必须考虑带宽的减少，因此需要对现有系统进行重新设计。这可能导致额外的分离总线，以提供足够的带宽储备来满足安全要求。

另一种方法是使用位于数据字段中的截断MAC[38]。一般建议对MAC标签使用至少64位[8]，以确保安全性并避免冲突，这对应于CAN帧的最大有效载荷。此外，密钥管理和新鲜度计数器的开销增加，这是避免重放攻击所必需的。即使只使用了32位，可用的有效载荷和带宽也将大大减少。除了减少可用带宽的缺点外，所有相关ECU都需要更多的计算资源来计算和验证这些MAC，以满足实时特性[42]。使用截断MAC进行安全车内通信的标准是AUTOSAR模块安全车载通信（SecOC）[35]。即使应用了MAC，它们也不提供不可抵赖性，因此通常无法防止伪造消息。因此，能够验证消息的ECU也能够篡改消息。为了使用密码算法提供不可否认性，数字签名是不可避免的，它使用了更多的资源和带宽，因此无法用于CAN通信。

4]的作者介绍了一种基于时钟的入侵检测系统（CIDS），该系统利用ECU的时钟偏差来检测CAN总线上的恶意行为。歪斜的变化影响帧的预期到达时间和测量到达时间的差异。然后从这些用于检测入侵的结果偏移中利用倾斜。由于系统无法观察到非周期性信息的方法，因此应如何处理因温度变化引起的倾斜变化是一个突出的问题，并且不可能可靠地确定攻击安装在哪个ECU上。此外，Sagong等人[36]证明了该方法的脆弱性，即攻击者还可以观察时钟偏差，并相应地调整其传输，从而使目标ECU绕过CIDS。

Murvay和Groza[33]表明，CAN信号的特征适合于识别帧的原点。不同ECU的信号显示出微小的变化，例如上升沿的建立速度或信号的稳定性。他们还观察到，这些特征在几个月内保持不变。利用这一观察结果，Choi等人[6]介绍了一种系统，该系统能够使用扩展标识符字段中的附加固定18位值来识别消息的来源。

应用他们的方法，需要重新编程每个设备，以发送可选扩展标识符字段中的固定值，从而减少可用带宽。由于比特填充和扩展帧格式，他们使用由18个主要比特组成的比特串实现了最佳结果，从而导致总共额外传输24个比特。因此，他们的方法将每条消息传输的比特总数增加了20%以上，并且只有在扩展标识符不用于其他目的的情况下才能实现。此外，由于主要使用主导位，该方法强烈基于电压电平，这意味着其他特性，如上升沿的斜率，不太受重视。相反，Scission使用消息的差分信号的特性，独立于传输的内容，允许完全保持可用带宽。通过这种方法，提取的特征可以更具体地用于识别，平均识别率为99.85%。与Choi等人[6]的工作相比，我们通过显著降低资源需求，大大增强了我们方法的可行性。这是由于使用更轻的算法进行识别时，采样率降低了125倍，因为我们使用Logistic回归而不是神经网络。Scission还分析计算出的发送者概率，以降低误报率，从而完全防止评估中出现误报。此外，我们强调检测不同类型的攻击者，例如检测攻击吉普切诺基时使用的未受监控的ECU[31]。最后，除了原型装配外，我们还在两辆生产车辆上评估了该方法，从而证明该方法在非实验室条件下也有效。

Cho等人[5]引入了Viden（基于电压的攻击者识别），这是一种识别攻击安装在哪个ECU上的方法。Viden本身是IDSs的扩展，就像前面提到的CIDS[4]。系统根据几个CAN信号的几个观察到的主导位产生的平均电压电平创建模型，该模型适用于识别操纵的ECU。由于只需要少量测量，系统的硬件要求较低。Viden仅使用一种信号特征，这就是为什么我们认为在电池充电或电磁兼容性等条件变化的情况下，Scission更可靠，特别是因为Viden使用高和低信号而不是差分信号。与差分信号相反，CAN高电平和低电平的电压水平受到电磁干扰的影响，例如由用电设备引起的电磁干扰，如图2a所示。此外，一些ECU在主位传输期间具有其电压电平的变化，如图2b所示。

ECU可能暴露在不同的条件下（热发动机舱与冷却内部），这会导致不同的温度变化，从而导致不同的电压变化。这与Viden更新机制的假设相反，因为作者假设ECU的电压水平在不断变化的条件下均匀变化。

相关指纹识别方法的比较如表1所示。

4 SCISSION

在下一节中，我们描述了识别CAN帧发送者的系统的各个阶段，以及如何将这些信息用于入侵检测。在仔细研究Scission之前，我们描述了我们正在考虑的网络架构、安全目标和威胁模型。

4.1 Security and threat models

4.1.1 system model.我们假设网络可能由几个独立的总线组成，几个ECU连接到这些总线。不同车型的车辆网络结构不同。在复杂的网络中，ECU根据功能进行分离，例如动力传动系统、舒适性和车身。各个总线通过网关连接，网关可以提供额外的安全机制。在总线较少的简单网络中，由于可以使用更多的ECU发送伪造消息，因此攻击者的努力也相应降低。图3示出了两种变体的示例性架构。

我们认为Scission要通过附加ECU集成到网络中，其物理连接到待监测的总线。为了防止攻击者简单地绕过系统，我们假设实现系统的ECU由经典安全机制（如HSM）保护，因此被认为是可信的。例如，为了将系统集成到现有ECU中，可以使用网关来确定接收到的消息是否已从有效ECU发送。

4.1.2 security goal.CAN没有提供第1节所述的验证消息真实性的机制。因此，每个总线参与者都能够使用所有可用标识符，而其接收者无法验证消息是否来自有效的发送者。为了弥补这一缺陷，系统中集成了Scission，以便根据其信号的物理特性确定接收到的CAN帧的发射器。系统监控网络流量，从而检测通过受损、未知或附加ECU发送的未授权消息。

由于Scission基于标识符确定信号的特征和ECU的权限，因此只有当受损或未知的ECU发送伪造的can帧时，才能检测到攻击。对于检测为主要目标的远程受损ECU，系统还能够确定发起攻击的控制单元。

4.1.3 compromised ECU.我们考虑的第一个攻击向量是通过现有ECU的漏洞访问受监控的CAN。这些可能具有额外的连接接口，如蜂窝、WiFi或蓝牙，攻击者可以利用这些接口[3,30]。使用这种入侵，可以远程发送各种CAN帧，可能无需事先进行物理访问，并且对车辆或乘客隐藏。攻击者可以使用所有可能的标识符和任何消息内容。

4.1.4 unmonitored ECU.第二次攻击通过对切诺基吉普[31]的攻击引起了注意，是恶意使用被动或未受监控的设备。研究人员利用ECU的更新机制插入恶意代码，将被动、只监听的设备变成发送设备。通过这种方式，他们能够向网络发送消息。

4.1.5 additional ECU.第三个攻击向量是将额外的总线参与者连接到受保护的网络。一旦攻击者能够物理访问车辆，他就可以用很少的硬件连接设备 例如，盗窃车辆[20]，禁用AdBlue系统或执行发动机调整[14，20]的努力。

攻击者可以将其他设备直接连接到网络，或使用车辆的易于访问的车载诊断（OBD）-II端口。这些端口为诊断目的而标准化，允许获取有关车辆状态的各种信息。OBD-II端口通常位于仪表板下方，可用于连接其他设备（如笔记本电脑或智能手机）以发起攻击。

这种策略与使用未受监控的ECU进行的攻击非常相似，但有一点不同。如第2.2节所述，除其他因素外，利用的信号特性由总线拓扑定义。拓扑结构的变化（如在本例中）会导致所有连接的ECU的特性发生变化。

4.1.6 Scission-aware attacker.由于基于远程的攻击检测是主要目标，我们还考虑了感知Scission的攻击者可能试图误导IDS的内容。由于Scission使用接收到的帧的物理特征，远程攻击者可能试图通过影响其信号来误导IDS。定义信号形状的特征，特别是上升沿和下降沿的特征，主要由没有物理访问的情况下不可影响的原因定义。远程攻击者可以通过耗尽电池或加热或冷却ECU来影响电源电压，这主要影响信号的绝对电压电平，而不是其总体形状。蓄电池放电会极大地影响所有ECU的电压水平，因为它们由相同的能源供应，因此温度变化主要影响各个ECU的信号。

4.2 Fingerprinting ECUs

在本节中，我们描述了识别接收帧来源的方法。相位概述如图4所示。我们首先对信号进行采样，然后进行预处理，这使我们能够独立于传输数据估计发射机。在那里，接收到的帧被划分为各个比特，并根据特征进行排序。随后，从这些特征中提取不同的时域和频域特征，表示实际指纹。在系统的第一步，训练来自这些指纹的模型，然后分别用于分类和概率计算。这使系统能够将发送ECU分配给接收到的帧，然后由入侵检测进行评估。根据可用数据，检测到攻击时会触发警报。

4.2.1 Sampling.在第一阶段，记录接收帧的模拟信号。为此，可以分别使用差分信号或两个信号高和低。直接使用差分信号需要额外的电路，但具有系统需要较少资源的优点，因为临时存储的数据较少，并且两个信号不必组合。使用差分信号很重要，因为分离信号可能受到电磁干扰或其他变化的影响。否则，这些影响可能导致错误的预测。差分信号V的优点是这样的信号噪声可以彼此补偿 如第3节图2所示。每比特测量值的数量取决于采样率和波特率。我们以20MS\/s的速率采样，在500kb\/s CAN上每符号进行40次测量。有关采样率选择的讨论，请参见第6.3节。

4.2.2 Preprocessing. 在该步骤中，对仲裁后记录的消息的每个位的信号进行单独处理。这导致大量包含多个模拟值的集合。由于单个ECU振荡器的漂移，一条消息中可能会出现多个边缘偏移。为了补偿这些位移并减少数据量，仅使用每个位的一段。例如，如果出现上升沿，则窗口从超过1 V的第一个值开始。

结果集（代表一个位）随后将根据其形状分布到三个组中的一个组中。如果表示显性位（0）的集合包含上升沿，则将其排序为G10组。如果不包含上升沿的集合位于G00组中。如果前一位为隐性位，则显性位集合包含上升边。包含下降沿的代表隐性位（1）的集合被分类为G01组。如果前一个为显性，则隐性位集合包含下降沿。由于这些比特不适合分类，所以丢弃其先前比特也是主导的主导比特。这是因为组G11的所有值几乎为零，而与发送ECU无关。在对整个接收到的CAN帧进行预处理后，由多个测量电压值表示的所有位被分配到三个组中，如图5所示。

该过程使得可以在仲裁后使用所有比特进行识别，并且独立于传输的数据。此外，通过单独考虑各个组，重要特征可能更容易观察到。如果不单独考虑各组，不同组的可区分特征可能会相互抵消。这提高了系统的鲁棒性和准确性。

4.2.3 Feature extraction. 在对信号进行预处理之后，系统为每个先前准备的组提取统计特征。由于不同的特征与群体相关，我们对这些特征进行了单独分析。评估了每个装置的培训材料的几个统计特征（见表2）。

除时域外，还考虑了频域的幅值。这些特征对于发送者识别的一般可用性已经显示出来[6]。在这项工作中，显著的差异在于考虑了与个体群体相关的这些特征。如果为更长的不同符号序列计算特征，则可能隐藏重要特征。这可以通过平均值的例子很好地说明。为此，针对菲亚特500的两个不同ECU计算了由三个符号组成的序列的特性。每个序列由每组的一个符号组成，如图6所示。两条曲线之间的差异，如较低的电压水平和ECU 1的过冲，是显而易见的。但这并没有明显反映在曲线的平均值中，ECU 0为1.286 V，ECU 1为1.28 V。但是，如果单独计算三个符号的平均值，则可以看到较大的差异。对于ECU 0，它们是µ。这可能不是序列中的情况，并且将防止超调被包括在分类中，这是一个特别重要的特征。

对于特征的选择，我们使用了Weka 3工具包[39]中的Relief-F[26]算法。Relief-F算法是一种过滤方法，用于计算每个特征的得分，可用于排序和选择最重要的特征。我们已经为每个测试设置进行了功能选择。由于对整个网络的强烈依赖性，结果略有不同选择最佳功能。因此，我们结合了测试设置的最佳特性，得到了一个通用特性集，如表3所示，以及它们各自的等级。然而，评估清楚地表明，最重要的特征可以在G10中找到，其中包含上升沿。总的来说，这会产生一个特征向量F（V），它表示从接收到的CAN信号中提取的指纹。

4.2.4 Model Generation and classification.从哪个ECU发送接收帧的识别是一个分类问题。因此，可以使用几种机器学习算法来识别新观测值属于哪一类。在我们的系统中，我们使用Logistic回归来预测帧的发送者。其主要优点是简单，这在资源有限的ECU上的实现中起着重要作用。这适用于培训和分类。

在能够预测接收到的CAN帧的来源之前，需要训练分类算法。为了实现这一点，我们为所考虑的每个ECU生成多个CAN帧的指纹。然后将所得指纹一起用于训练每个ECU i的分类器Θi∈ 在该监督学习阶段之后，分类器可用于将新接收帧的特征与为模型生成而收集的特征进行比较。

4.2.5 Deployment and lifecycle.重要的是在训练阶段避免伪造帧，否则系统将无法使用 能够可靠地检测入侵。因此，我们认为车辆在初始部署阶段处于安全环境中，例如在工厂或授权车间。在这个由受保护的诊断访问触发的过程中，为每个ECU分配了一把钥匙，以实现与IDS的安全通信。然后，执行安全训练阶段，其中仅使用经过验证的帧。这方面所需的加密算法可在AUTOSAR模块SecOC[35]中获得

由于预计信号特性会出现波动，例如由于部件老化或腐蚀，学习模型必须适应这种概念漂移[9]。为此，我们提出了一种性能监视器，该监视器持续评估分类器的质量，以便在无法以高概率区分帧时启动安全训练。这允许模型不断适应变化，确保一致的高精度。为了更新现有模型，可以使用随机[2]或小批量算法，这比完全训练需要更少的计算工作量。还可以使用在线机器学习方法[19]，该方法持续适应当前特性。

在生命周期中使用经典密码基本上与第3节中描述的限制带宽的问题相同，但这些消息不会连续使用，并且没有硬实时要求。这使得即使对于资源较少且没有额外硬件加速器的ECU，计算也很现实。

如果无法使用加密算法，则应使用其他对策来防止中毒攻击[7、18、24]。这些过程减少了培训阶段潜在恶意数据的影响。

4.3 Intrusion detection using fingerprints

在本节中，我们描述了分类概率如何用于检测第4.1节中描述的威胁模型。

4.3.1 Detecting compromised ECUs.基于训练的分类器，系统估计接收到新帧时每个ECU的概率。最简单、最直观的方法是选择概率最高的ECU作为帧源。如果被选为源的ECU不允许发送带有接收帧标识符的帧，则将假设攻击。由于车辆网络的通信流是预定义的，因此系统知道关于使用哪些标识符以及允许哪些ECU使用这些标识符的信息。

选择最可能的ECU有一个缺点，即如果系统接收到一个无法以高概率确定原点的单帧，则更可能出现误报。为了避免这一缺点，我们设置了一个阈值tmax，必须以最大概率超过该阈值。仅当所选ECU的概率高于此阈值且控制器不允许使用给定标识符时，才假定存在攻击。否则，框架将被标记为可信。

为了提高对异常值和电磁干扰的鲁棒性并减少计算工作量，我们引入了另一个阈值tmin。第一步是系统计算ECU被允许发送具有指定标识符的帧的概率。此处，由于CAN不允许多个发射器使用同一标识符，因此只能使用一个ECU。如果所选控制器的估计概率低于阈值tmin，则该帧被标记为可疑。在这种情况下，通过选择具有最高概率的ECU作为帧的预期源来计算剩余ECU的概率。如果可疑设备的概率超过阈值tmax，则标记为可疑的帧被分类为恶意帧，从而导致报警。选定的ECU还表示执行攻击的ECU。如果概率不超过阈值tmax，则认为帧是可信的，以减少误报。应注意，可疑但未触发警报的帧用于进一步的检测方法。

有必要将误报率保持在尽可能低的水平，因为这些误报可能引发不必要的干预，或者根据反应，甚至危及乘客的安全[16]。因此，由于我们假设可信帧的数量远高于恶意帧的数量，因此我们使用这两个阈值，即使它们可能导致更高的误报率。此外，执行攻击通常需要几个伪造消息，这增加了检测的可能性。另一个优点是，对于大多数帧，需要的计算更少，因为只有当帧标记为可疑时，才需要计算所有ECU的概率。

4.3.2 Detecting unmonitored ECUs.如果执行攻击的未受监控ECU的指纹与不允许使用接收到的标识符的其他ECU中的一个相似，则检测到攻击，如前一节所述。例外情况是，无法预测攻击的来源。在不太可能的情况下，未受监控的ECU与攻击者想要模仿的ECU具有非常相似的特性，因此Scission无法检测到攻击。在第三种情况下，如果无法分配ECU，则框架被标记为可疑。

为了检测未受监控的和额外的ECU，Scission监控标记为可疑的帧数。为了检测这些攻击，我们为每个ECU i使用一个计数器csuf，i，初始化为零，当一个帧被标记为可疑时，该计数器将递增。每次系统接收到可以作为正常行为直接预测的帧时，相应ECU的计数器都会减少。如果计数器csuf，i超过阈值tsuf，则假定攻击。

4.3.3 Detecting additional ECUs.额外ECU的检测与未受监控设备的检测非常相似。然而，最大的区别在于连接一个额外的设备会导致拓扑结构的显著变化。由于总线结构对指纹特性的影响远大于ECU本身，如第2.2节所述，因此计算的概率不太可能超过阈值。由于所有ECU都受到影响，因此这些变化会导致所有计数器csuf，i的直接和大规模增加。

4.3.4 Detecting Scission-aware Attacker.如果 Scission-aware的远程攻击者可以影响所有ECU的电压水平，这将导致整体识别精度性能的可测量损失。如果准确度可能会受到快速而显著的影响，则系统可能无法识别入侵，直到模型被修改，这可能会被用来执行攻击。为了模拟特定的ECU，攻击者可以通过加热或冷却受损的ECU来影响其自身的电压水平。由于这两种变化不是直接出现的，而是稳定的，特别是在电池耗尽时，系统能够持续适应轻微变化的条件。此外，绝对电压电平的变化不会影响信号的一般形状，这使得识别更加困难。由于 Scission-aware使用多种特征，攻击者不太可能模拟特定的ECU。即使一般形状非常相似，由于缺乏关于特征的一般信息。总的来说，包括安全学习阶段，我们认为我们的系统甚至能够检测到有Scission-aware的攻击者。

5 EVALUATION

在本节中，我们将评估典型配置、菲亚特500和保时捷Panamera S E-Hybrid上的 Scission。首先，我们证明了我们的指纹识别方法能够以高概率识别接收到的CAN帧的发送者。之后，我们评估了我们的入侵检测系统基于指纹识别受损、未受监控和额外ECU的能力

为了记录信号，我们使用了数字存储示波器PicoScope 5204，采样率为500 MS\/s，分辨率为8位。每帧创建两个测量序列，一个用于CAN低电平，另一个用于高电平，然后将其组合以获得差分信号。由于采样率为500 MS\/s的合适硬件的使用非常复杂，因此价格昂贵，我们已将测量值降低到20 MS\/s的采样率。这使得该方法在汽车领域的适用性更加现实。

分析和评估软件完全用Python编写，并使用Scikit机器学习和SciPy库。这也使得在Python中直接使用记录的帧成为可能。对于下面的每个测试，我们都训练了 Scission，第一次测量的是每个ECU 200帧。根据验证集的学习曲线确定训练大小。

5.1 Fingerprinting ECUs

5.1.1 prototype.我们评估方法的第一个装置是由五个Arduino UNO组成的CAN原型。每个都配备了两个CAN屏蔽，上面安装了MCP2515[21]控制器和MCP2551[22]收发器。原型的接线如图7所示。

对于原型，我们使用了真实车辆中使用的双绞线。总线的每一端都以120Ω 电阻器和短截线处的2400Ω 电阻器，这通常是为了减少反射。在许多车辆中，总线并没有完全按照规范实现，因为短存根长度会导致更高的成本。较长的短截线会导致更多更强的反射，这会可以通过在短截线处的附加电阻器最小化。ECU都由相同的电源供电，这导致特性不太明显。示波器直接连接在ECU 3的前面。

我们已经记录了56560帧，具有正常和扩展标识符。对于原型，我们采用随机有效载荷来显示独立于传输数据生成指纹的可能性。

混淆矩阵如表4所示。每列显示了使用第4.2节所述的指纹可以正确识别接收帧的百分比。可以看出，检测到来自原型的消息时，平均识别率为99.9%，最小识别率为1999.58%。特别值得注意的是，ECU 0、ECU 2和ECU 4之间的结构对称性没有任何影响。

5.1.2 Fiat 500.我们评估方法的第一辆真正的汽车是菲亚特500，它的CAN总线有六个内部ECU，每个ECU最多有七个标识符。为了发送伪造信息以评估系统，我们将两个配备CAN屏蔽的复盆子Pi 3连接到总线。一个树莓Pi（称为ECU 6）已连接到OBD-II端口，第二个树莓Pi（称为ECU7）已直接连接到汽车后备箱中的CAN总线。示波器还连接到ODB-II端口，我们在该端口上记录了25979帧。对于菲亚特500，我们实现了99.6%的平均识别率和98.56%的最低识别率，如表5所示。

5.1.3  Porsche Panamera S E-Hybrid.我们评估指纹识别方法的第二辆真车是保时捷Panamera S电子混合动力车。车辆有五条以上独立的CAN总线，并连接了多个ECU。在我们的评估中，我们观察了CAN总线，该总线用于动力传动系统，具有六个内部连接的ECU，每个ECU最多使用43个标识符。由于这辆车在混合动力系统和各种功能方面要复杂得多，因此这辆巴士的负载非常高。增加数据包大小或减少带宽的IDS可能难以在如此复杂的网络中部署。与菲亚特500一样，我们连接了两个树莓Pi 3（ECU 6、ECU 7），以增加ECU的数量。由于OBD-II端口未直接连接到CAN总线，我们必须直接连接Pis和示波器到汽车前部扶手附近的CAN总线。我们已经记录了6389帧，混淆矩阵如表6所示。与之前的测试一样，我们为保时捷实现了99.88%的概率和99.58%的最低识别率。

5.1.4 Summary.对这三种设置的评估表明，我们的指纹识别方法能够以高概率识别帧的发送者。所示结果是通过选择概率最高的ECU得出的。与Choi等人[6]的工作相比，我们的准确率为96.48%，平均成功率为99.85%。此外，通过使用更简单的机器学习算法，我们使用了125倍更低的采样率和更少的计算工作量。我们还表明，我们的指纹识别方法能够识别帧的发送者，而无需使用会减少可用带宽的特定CAN字段。

5.2 Detecting compromised ECUs

在上一节中，我们研究了指纹识别方法识别接收帧发送者的能力。当直接使用指纹时，达到99.85%的成功率意味着0.15%的假阳性率。如果长时间观察总线，这将导致大量假警报。

在下文中，我们评估了第4.3节中描述的拟议阈值方法减少误报的能力。使用相应的验证集确定参数tmax和tmin的配置。

5.2.1 Prototype. 对于原型设置，两个Arduinos已编程为使用10个普通标识符和10个扩展标识符发送伪造消息。通过这种方式，我们捕获了另外51个有效帧和467个伪造帧。如表7所示，对于tmax=0.6和tmin=0.2的原型设置，我们实现了98.5%的检测率。与简单指纹相比，阈值方法将误报降低到0。

5.2.2 Fiat 500.对于菲亚特500，我们从两个树莓Pis（ECU 6和7）发送了1230个伪造帧。不幸的是，我们无法操纵现有的一个ECU（0-5）从这些ECU发送伪造帧。Fiat 500的结果如表7所示。如前一次测试中所观察到的，Fiat的ECU具有高度的可区分性，这导致了假阳性率为0，tmax=0.7，tmin=0.2，从而提高了伪造消息的检测率。

5.2.3 Porsche Panamera S E-Hybrid.由于我们无法估计伪造动力总成CAN的高度关键信息的后果，我们决定只为ECU 6和7发送伪造信息。在这里，记录了157个伪造帧。由于这两个ECU的结构相同，并且在同一点连接到总线，因此它们的信号非常相似。这种情况表明，阈值方法可能导致假阴性率增加。另一方面，假阳性也可以减少到0。断开配置为tmax=0.6和tmin=0.2。

5.2.4 Summary.结果表明，所提出的入侵检测系统仍然能够检测到假帧，误报率为0%。即使我们在评估期间没有观察到假阳性，这并不意味着不会出现假阳性。车辆的寿命比我们测量的时间长得多。

对于标记为可疑的帧，我们认为通过根据实际车辆微调阈值，可以进一步提高检测率。我们还希望在实际条件下获得更好的结果，因为对专业连接器的干扰较少。通过设置和移除发送伪造帧的设备，我们无法确保测量点没有发生轻微变化，从而导致识别率降低。

5.3 Detecting Unmonitored ECUs

在本节中，我们评估了检测菲亚特500上未受监控的ECU的能力。为此，我们在不了解ECU 7的情况下对系统进行了培训。在监控了200个可信的帧后，我们插入了来自ECU 7的消息，伪造了来自ECU 1的消息。如果中断无法以高概率对帧进行分类，则计数器csuf，1将增加4，否则将减少1至最小值0。如果此计数器超过阈值tsuf 200，则中断将触发警报。

ECU 1的计数器如图8所示，表明系统能够检测到攻击。如果要更快地检测到攻击，可以降低阈值或以更高的值增加计数器。

5.4 Detecting Additional ECUs

在下文中，我们展示了断开检测其他连接设备的能力。为此，我们首先让系统监控未更改的总线，这意味着参与者很有可能被检测到。几帧后，系统切换到修改后的总线上记录的帧。因此，标记为可疑的帧数增加，表明CAN总线发生了重大变化

每当中断无法分配高概率的帧（这意味着该帧被视为可疑帧）时，计数器csuf，i将增加4。如果一个帧可以分配给高概率的ECU，计数器将减少1，最小值为0。一旦概率急剧下降，许多帧被错误地归类为可疑帧，计数器将快速增加。为了提高可读性，我们将所有csuf，i值一起计数到计数器csuf。如果此计数器超过阈值tsuf 200，则中断将触发警报。

5.4.1 Prototype.为了评估原型设置，我们在没有将ECU 9连接到总线的情况下记录了正常帧。与前面的场景一样，示波器直接连接在ECU 3的CAN控制器前面。对于恶意测试集，我们使用了先前评估中记录的帧，将所有ECU连接到总线。首先，我们使用正常帧训练ID。为了模拟额外连接的设备，我们在IDS分析了420个正常帧后切换到恶意测试集。计数器csuf的过程如图9a所示。一旦数据从正常测试量更改为恶意测试量，曲线将增加尖锐地。从IDS中观察到53帧恶意总线配置后，已达到阈值，这导致报警

5.4.2 Fiat 500.对于菲亚特500，我们记录了正常帧，而ECU 6和7未连接到总线。只有示波器通过OBD-II端口连接到总线。以前连接所有ECU的测试中记录的数据被用作恶意测试集。在正常测试集的390帧之后，我们切换到恶意帧。菲亚特500的计数器csuf的过程如图9b所示。在系统处理了77帧后，检测到了附加设备ECU 6和7。

5.4.3 Porsche Panamera S E-Hybrid.对于保时捷Panamera，我们使用了与菲亚特500类似的设置。为了评估保时捷上的系统，我们拍摄了几个没有树莓Pis（ECU 6，ECU 7）连接到总线的帧。这些框架已被用作正常测试集，用于学习阶段和评估的第一步。在处理370个正常帧后，我们切换到恶意帧集。在检测到攻击之前，IDS处理了79帧，如图9c所示。

5.4.4 Summary.评估结果显示了我们的系统检测额外连接设备的能力。计数器csuf在切换到恶意测试集后直接增加，并且在平均处理了70帧后超过阈值。

6 DISCUSSION

6.1 Stability

Murvay和Groza[33]已经表明，这些特征在几个月内保持不变。这一说法与我们的观察一致。我们建立了另一个原型，并在半年多的时间里观察了其特性，在实验室条件下，该特性在这段时间内保持稳定。硬件和总线结构与第5.1.1节评估中使用的原型设置相当，由5个ECU组成。在这里，使用了位镜Micro BS051记录信号，并使用Raspberry Pi 3进行计算。

然而，由于实验室设置没有真实车辆复杂，因此没有相同的表现力，我们还分析了我们的方法在菲亚特不断变化的条件下的行为。为此，我们通过OBD-II端口记录了菲亚特在其原始状态下的额外信号，如第5.1.2节所述。第一个数据集记录在环境温度约为25℃的大厅中◦C（77◦F） ，而车辆因至少一天未移动而被关闭和冷却。从这个集合中，6个内部ECU中的每一个的前200帧用于分类器的训练。在同一状态下，又记录了3369帧，并毫无例外地正确分类。第二个数据集的记录在车辆冷启动后开始，并包含在平均环境温度32℃下约30分钟的行程◦C（89.6◦F） 。车辆完全加热后，记录完成，车辆停驻在大约23号的地下车库里◦C（73.4◦F） 。此外，该数据集由6672帧组成，由已训练的分类器正确分类，无需重新学习。冷却3小时后，在车辆发动机仍然关闭的情况下，开始记录第三组数据。在短时间后，车辆启动，并在大约36时驶出车库◦C（96.8◦F） 再持续20分钟。第三个数据集由4863帧组成，分类完全正确，无需重新学习。

在特性方面观察到的最大变化是电压水平，该电压水平从关闭和冷却的发动机下降到预热的发动机约0.012 V至0.026 V。我们的观察还证实了第3节中的假设，即在变化的条件下，ECU可能发生不同的电压变化。

6.2 Limitations

Scission可以通过监测can通信来检测受损的ECU。它检查是否已从允许使用相应标识符的ECU发送帧。当恶意ECU使用另一ECU的标识符时，检测到攻击。但是，如果攻击者使用ECU在正常情况下允许使用的标识符，则Scission无法检测到它们。

如评估所示，断开可以检测到其他ECU的连接。由于系统使用主要受总线结构影响的CAN信号的特性，因此系统只能检测导致总线变化的修改。如果在不影响特性的情况下修改总线，系统将不再能够可靠地识别变化。

6.3 On the sample rate

如第4.2.3节所述，发送器可区分性的最重要特征出现在上升沿。因此，我们推断G10上的采样率。在上升沿，超调是最明显的特征，在图5c中可以清楚地识别。同时，该特性表示信号的最短部分，因此对于采样率的选择非常重要。在我们分析的数据中，超调的最小持续时间约为200 ns，对应于5 MHz的频率。根据奈奎斯特-香农采样定理，至少10 MHz的采样是可靠记录超调的必要条件。由于采用20 MHz的故意过采样，可以更详细地记录曲线过程，从而提供更精确的特征计算。此外，这在超调持续时间较短的情况下提供了裕度。表8显示了不同样本率的平均识别率和假阳性率。使用菲亚特数据集的每个ECU 1000帧来确定这些值

6.4 Masking unmonitored ECUs

如果未受监控的ECU可以在不触发基于其指纹的报警的情况下向总线发送消息，则使用可疑计数器进行检测。在这种情况下，攻击者可以通过不定期渗透伪造消息来绕过系统，使计数器低于阈值。然而，这种危险主要存在于非周期性消息中。对于定期发送的消息，攻击者必须停用实际发件人，然后接管消息的发送。必须保持消息的频率，因为可以用较少的努力识别额外或丢失的消息[4,34]。

6.5 Preventing attacks

Scission可以自定义，以不仅检测攻击，而且主动防止攻击。如果只有一定数量的第一比特用于分析而不是整个帧，则这是可能的。通过这种方式，可以以适当的计算速度做出决策，并且传输可能会受到干扰，例如，通过使CRC校验和无效或发送错误帧。必须极其谨慎地考虑自主作用系统，因为错误的决策可能导致高风险[16，17]。对于安全关键信息，必须进行广泛调查，以满足安全要求。

6.6 Field of application

如果实现Scission的成本可以相应降低，则可以在多个ECU中设置中断。这允许ECU可以更快速和独立地确定接收到的帧是否可信以及如何处理它们。此外，多个系统的使用提供了在不同测量点相互验证的可能性，这可以进一步提高可靠性。由于CAN总线不仅用于车辆，而且还用于许多其他应用领域，因此，在这些领域中也可以使用中断。例如，其中包括航空航天、自动化、医学和铁路系统。此外，许多高级协议（如CANopen或SafetyBUS）都基于CAN。

由于CAN不能为许多未来的应用提供足够的带宽，2012年推出了具有灵活数据速率的CAN（CAN-FD）[11]。这使得用户数据长度从8字节增加到64字节，并提高了数据传输速率。在汽车行业，可以假设平均传输速率为2.5 Mbit\/s[13]。由于CAN-FD的功能方法基本保持不变，因此在即将进行的改进中，断开也可用于未来的公共汽车。

7 CONCLUSION

智能决策支持系统在车载网络中的应用是提高其安全性的一项很有前途的技术。由于CAN不能提供可靠的方法来识别接收到的消息的发送者，我们提出了一种从CAN信号中提取指纹的方法。评估表明，Scission能够以99.85%的概率识别正确的发送者

除了显著提高识别率外，与Choi等人[6]的方法相比，我们还能够通过使用逻辑回归和低125倍的采样率来降低要求。我们的采样方法进一步使我们能够在不影响可用带宽的情况下部署中断。此外，我们还引入了一种基于上述采样方法得出的指纹的入侵检测系统，该系统使我们能够在评估过程中检测从受损ECU发送的伪造消息，且无误报。

我们已经证明，所提出的入侵检测系统还能够检测来自未受监控和其他设备的攻击。通过评估原型菲亚特500和保时捷Panamera的Scission，我们评估并建立了生产车辆的能力。

考虑到大多数针对汽车的攻击都是成功的，因为不可能确定接收到的帧是否来自有效的发送者，我们的系统可以提高安全性，从而提高系统安全性。指纹技术可以增强传统的入侵检测方法，它可以进一步用作独立系统的基础，或者提高连接不同总线的网关的安全性。