车辆网络入侵检测的滑动窗优化信息熵分析方法

引言

随着现代汽车网络安全风险的大幅增加，车载网络环境下的网络安全问题越来越受到人们的关注。 最近几年。在考虑计算资源和成本约束的同时，提高车载网络的网络安全能力成为一个迫切需要解决的问题。为了解决这个问题，一个新的Informa 本文提出了一种以固定数目的消息作为滑动窗口的方法。通过对滑动窗策略的改进，优化决策条件。提高了准确率，降低了假阳性率。实验结果表明，该方法能够对攻击进行实时响应，并有较大的改进。车载网络环境下入侵检测的精度。

背景

汽车电子系统是由各种电子设备组成的分布式系统，如电子控制单元(ECU)、行动者(例如发动机、马达、制动器和方向盘)，以及 传感器(例如，LIDAR、GPS、位置估计器、雷达和摄像机)，它们与车载网络(如控制器区域网络(CAN)、LIN和FlexRay)相关联。目前，这个数字 在现代高端汽车中部署的ECU中，有100多个可以实现各种功能[1]。随着现代车辆的复杂性和连通性的不断提高， 汽车的安全隐患日益突出。然而，车辆作为一个独立的系统已经存在了很长一段时间，而现有的车载网络并不存在。 在协议设计阶段提供消息加密和认证机制。

目前，车辆上的网络安全攻击有所增加，并在几篇论文[2]、[4]、[5]中作了报告。例如，Koscher等人。在[4]中成功地控制了广泛的自动驾驶 我的功能，如禁用刹车和停止发动机。这次袭击导致制造商召回了140万辆汽车。对车辆的攻击通常包括一系列行动，如 CAN总线的过滤和模糊化以及ECU固件的逆向工程。考虑到汽车电子系统的安全性是至关重要的，它的设计需要严格遵循所需的标准规范。 国际标准化组织26262[6]。网络安全对安全功能系统的威胁不仅是对信息安全和隐私的威胁，也是对用户生命财产安全的威胁。避免硒 由于黑客入侵造成的巨大破坏，车载网络的入侵检测能力有待提高。

提出了提高车载网络安全性能的对策[7]-[9]。但是，安全增强方法，如消息加密和认证受到成本和资源的限制[10]-[13]。不断发展的攻击技术很难用防火墙阻止[14]，因为网络攻击变得越来越多样化， 智能在汽车的生命周期(一般超过20年)。为了防止攻击者进行逆向工程，现有的保护技术无法处理这些攻击-Effe。 以牙还牙。因此，入侵检测以其成本效益高、兼容性好等优点被认为是提高车载网络安全的一种很好的选择。在本研究中， 针对车载网络的入侵检测问题，提出了Liding窗优化信息熵分析方法.这意味着一种策略，它使用最优的固定数目的消息作为滑块窗。

动机

最近，在[15]-[18]中提出了几项检测针对车辆的攻击的研究。最近发布的sae j 3061网络物理车辆系统指南侧重于设计赛博秒。 与汽车安全标准ISO 26262密切相关的安全意识系统。与当前工作有关的研究主要包括[19]和[20]。以前基于信息熵的研究 以下缺点。首先，在[19]和[20]中采用了以固定时间为滑动窗口的监测策略。因为CAN总线是一个事件触发的车载网络。信息 在这种监测策略下，n熵不能避免非周期can消息和不同传输速率(例如125 kbps和250 kbps)的巨大影响，从而导致高假偏置。 我们的费率。第二，采样窗口的大小对信息熵有很大的影响，但是如何确定采样窗口的大小在以往的研究中一直没有得到深入的研究。为了提高车载网络环境下入侵检测系统(IDS)的检测精度，需要一种高精度、低响应时间的入侵检测方法。

主要思路

据我们所知，与现有的基于信息熵的入侵检测系统设计相比，本研究首次采用了一种利用固定nu的观测策略。 作为滑动窗口的信息。本文提出的入侵检测方法不需要改变现有的CAN协议。因此，它可以与市场上现有的车辆兼容。T型 本研究的主要贡献可归纳如下。1)提出了一种基于固定数目消息的滑动窗口策略，以避免因不同的b而引起的信息熵干扰。 AUD率和非周期CAN消息。2)提出了一种基于模拟退火的启发式算法。根据该算法和实际的网络通信数据集[21]，我们实现了 为这类车辆的入侵检测系统设计提供了最佳的滑动窗口参数。

1. 进行了基于真实车辆数据集的评价实验，结果表明，与现有的基于熵的方法相比，该方法具有较好的鲁棒性。 低响应时间和假阳性率的入侵检测系统。论文的其余部分组织如下。在第二节中，我们介绍了背景知识和攻击模型以及SCE。 纳里奥斯。第三节介绍了我们提出的检测机制。在第四节中，我们详细描述了所提出的算法。在第五节中，我们展示了实验和评估结果。科蒂奥 NVI介绍了相关的工作。最后，我们在第七节中详细阐述了结论。

准备工作

CAN概述

CAN协议是罗伯特·博世公司(RobertBoschGmbH)为满足车载环境中实时性、鲁棒性强、成本效益高等具体要求而发明的。罐头是一种常见的 在当前车载环境下使用的通信网络，是一种基于优先级的非抢占通信网络，最大数据速率为1Mbit/s。在数据链路层，CAN协议。 使用广播通信来传输消息。图1显示了CAN 2.0的基本数据框架结构。图中的蓝线表示CAN物理总线上的传输波形。当N OD3获得总线传输权限，其他节点将停止发送并等待网络再次空闲。一旦can网络被非法访问，此仲裁机制将受高优先级拒绝服务(DoS)攻击的。

CAN协议是一个事实上的标准通信网络协议，在汽车和工业设备上使用了30年，它通常由多个安全关键系统连接。然而，这个COM Ponent由于缺乏安全机制设计而容易受到攻击。因此，本文研究的重点是适合CAN环境的入侵检测技术。

CAN漏洞

根据CAN协议的特点，可以将CAN的脆弱性描述为接下来的四点[22]。

广播传输：在数据链路层上，CAN协议使用广播通信传输消息，从而表明总线上的所有节点都可以同时接收消息。

无认证：CAN总线上的消息传输缺乏设计认证机制。攻击者可以破坏一个或多个ECU，并限制它们发送少量或全部消息。

无加密：can消息缺乏加密机制，而为can添加加密技术会导致额外的延迟，并会降低网络的有效利用率。 带宽和有效负载资源的约束。

基于ID的优先级方案：CAN的仲裁机制是：高优先级的消息可以在不影响总线碰撞决策时间的情况下继续传输数据，而低优先级的优先级则是较低的PRIO。 rity消息必须等待下一个空闲状态。因此，黑客可以很容易地使用高优先级的ID来发起DoS攻击.

图2显示了车载网络的脆弱性、研究人员采取的攻击以及相应的对策[7]-[9]、[15]-[18]。如图2所示，有效的对策 针对帧注入和DoS攻击，本文提出了一种基于异常检测的入侵检测系统。应该指出的是安全ENH 增强系统对DoS攻击的对策是有限的，特别是对于高优先级DoS攻击.这意味着检测DoS攻击很容易，但要防止DoS攻击是非常困难的。

攻击假设

1. 威胁模型中，我们假设攻击者可以访问CAN总线。接入点包括但不限于蓝牙、OBD\_II、Wi-Fi、物理访问和USB端口。一次 拦截器可以访问CAN，攻击者可以进行嗅探、欺骗和DoS攻击。在本研究中，在车载网络中检测到两种攻击类型.一个是DoS攻击，另一个是注射攻击。
2. 攻击场景-基于威胁模型给出了两类攻击场景。在图3和图4中，白色框是说明来自合法ECU的合法消息。红色方框显示为攻击者发出的欺骗消息。然后，x轴是消息传输的时间。

DoS攻击：如图3所示，攻击者可以在总线上的短周期内注入高优先级消息。针对CAN总线的DoS攻击可分为两类。一是腐败合法化 通过从攻击者发送的错误帧(如干扰)对消息进行分组.CAN控制器可以过滤出没有被ecu接收到的消息，因为它有一个过滤器和一个子网掩码寄存器。 。因此，向特定的ECU发送特定的ID攻击可以禁用特定的功能。另一种方法是较高优先级的消息，如can-id等于零。CAN是一种基于广播的总线n。 基于优先权仲裁的网络。因此，上述类型DoS的推出将直接导致can bus的损坏。

注入攻击：如图4所示，注入攻击表示攻击者重新发送来自节点的最新接收消息。这种攻击会导致异常的高利用率。 CAN总线通过注入攻击降低目标信号内容的速率。数据段内容的更改可以使先前发送的消息无效。注射类型 CAN网络的套路分为两种情况。一种是重放攻击，这意味着攻击者预先保存合法消息并注入这些消息。另一个是布料 运行时系统中消息的转换

方法

为了提高入侵检测系统的检测性能和有效性，设计了入侵检测系统。在本研究中，我们主要是重点研究了滑动窗的优化设计。我们为我们的检测模型定义了以下几个特征。定义1：使用窗口来监视网络信息熵，并且它可以监视网络信息熵。 消息的固定时间或固定数量。消息的时间和数量用作窗口参数。我们把它定义为滑动窗口。定义2：从攻击开始到攻击发生之间的时间 入侵检测系统可以定义为攻击检测的响应时间RT=at−dt，其中at表示攻击的起始时间，DT表示检测攻击的时间。在本研究中，t 攻击起始时间是通过插入带有时间标记的攻击块来获得的。

问题描述

汽车电子系统是一个安全关键系统，其正确性不仅需要正确的动作，而且需要在正确的时间做出反应。因此，对入侵的响应时间 CKS也是入侵检测系统的一个重要的评价指标。本文研究的重点是如何在车辆网络环境下实现低响应时间的入侵检测。 新台币。研究问题可以说是如何在车载网络环境下实现高精度、低延迟的入侵检测设计。车载网络环境具有 以下特征：资源约束(包括计算、存储和网络带宽资源)、成本敏感和安全关键。

拟议方法的框架

如图5所示，我们提出的方法的框架主要分为两个阶段。一是离线训练阶段。采用模拟退火滑动算法得到最优解。 Liding窗口参数第二阶段是在线检测阶段.根据参数在训练阶段，我们建立了一个入侵检测系统来检测异常入侵。

1. 离线训练阶段方法的训练阶段主要包括以下步骤.

步骤1：向测试数据集添加攻击块(携带用于评估的标记)。关于通用电气的更多细节 在培训阶段使用的数据集的神经化在下面的V.·

步骤2部分中描述：从测试数据集中提取CAN消息ID以获得一个新的ID集。

第三步：使用滑动 窗口作为信息熵采样窗口，分析在滑动窗口中捕获的消息ID的信息熵。

步骤4：比较步骤3中获得的信息熵 用正常信息熵范围来判断是否存在攻击块。·

步骤5：将步骤4中获得的攻击结果与添加的攻击块的标记进行比较，并获得th e初始检测精度数据。

步骤6：为下一次迭代选择新的滑动窗口大小和正常范围。整个训练过程采用模拟退火算法，并重复了a。

第一步到第六步，以获得最佳的滑动窗口大小和决策条件，具有最高的检测精度。

1. 在线检测阶段这一阶段主要包括以下几个重复步骤。·

步骤1：在线读取CAN网络消息并存储在缓存中。当数达到设定的滑动风后 现在，进行信息熵计算。

步骤2：将步骤1中获得的信息熵与正常信息熵范围进行比较，得到入侵检测结果。

步骤3：更新系统入侵检测日志和t 如果检测到攻击，将发出警报

需要强调的是，每种入侵检测方法只能针对特定的攻击模型。本文提出的方法主要针对无法用ot处理的攻击模型。 她的安全增强方法，也是车载网络中常见的攻击模型.未来的研究可以考虑增加第三阶段，即运行时监控/采用阶段。在t 在此阶段，入侵检测系统的灵敏度可以在假阳性确认的基础上自动调整。

熵评价模型

为了检测车载网络的信息熵，有必要根据CAN总线的特点建立信息熵模型。CAN消息具有较低的诱捕能力。 Y，平均11.436位[23]。根据Shannon熵的定义计算消息ID的熵。假设系统X，其有限的可能状态集是{x1，x2，…，xN}，那么infor 系统X的熵为H(X)=−XNi=0p(Xi)log p(Xi)，其中p(Xi)是系统X在状态xi中的概率。

1. CAN IDS的熵用于评价CAN ID的信息熵，CAN系统模型可以表示为8=(i，W)，其中i={Id1，id2，id3.，idn}是一组不同的ID。 在滑动窗口大小W的情况下，滑动窗口W中的CAN ID的信息熵值可以表示为H(I)=−X id∈i PID日志PID。(2)由于本文确定了 通过检测和监控车载网络的网络状态，确定了样本窗口中的消息总数，从而确定了样例窗口W中消息的总数。 由方程(3)确定：nTotal=xni=1 Countidi。(3)通过计数得到W中出现的Idi数。那么，Idi出现在W中的概率可以表示为P(Idi)=CountidiNTotalPnI=1P(Idi)=1，P(Idi)>0(i=1，2，.，n)。定义Idi的不确定性在于它的自我信息。Idi的自信息为Uidi=log 1P(Idi)=log NTotal Countidi.(5)在采样窗口W中，车辆网络上ID的熵为H(I)=E[u(Idi)]=xn i=1 hidi，(6)wh。 Ere Hidi=P(Idi)U(Idi)=Countidi NTotal×log NTotal Countidi。(7)

入侵判断

为了判断网络是否处于攻击状态，我们设置了以下参数：UE平均信息熵，σe是对应的标准差。代表e 每一个滑动窗口大小W，检测算法根据方程(6)计算H(I)。如果H(I)不在正常范围[ue−kσe，ue kσe]，则被认为受到攻击，其中使用k。 设置偏差σe，0.001≤k≤2的灵敏度.滑动窗口设置的变化对信息熵有重要的影响。本文的研究重点是如何获得b。 EST滑动窗口参数，滑动窗口尺寸W，偏差σe。采用一种基于模拟退火的算法来获得最优参数。更多细节将在其本身中介绍IV-B节。

算法描述

我们的目标是为车载网络获得一种高精度的实时入侵检测方法，该方法可以较低的工作量部署在当前的车载网关节点上。为了这个 提出的入侵检测方法可以作为车载网关平台的软件插件，也可以作为硬件节点加载到现有的CAN总线上。首先，我们设计了一个 形成熵-基于固定数目的消息作为滑动窗口的监测算法。其次，采用模拟退火算法优化滑模赢的参数设置。

基于信息熵的入侵检测算法

简单地说，熵测量算法可以表示为在单个采样周期内对CAN总线交通流的信息熵进行监测。本文的完整设计流程 在算法1中描述了粘滞测量算法。假阴性和假阳性率是入侵检测系统的主要指标，本文在[24]中对这些指标进行了测量。r a表示攻击数据包的检测率(检测精度)，如

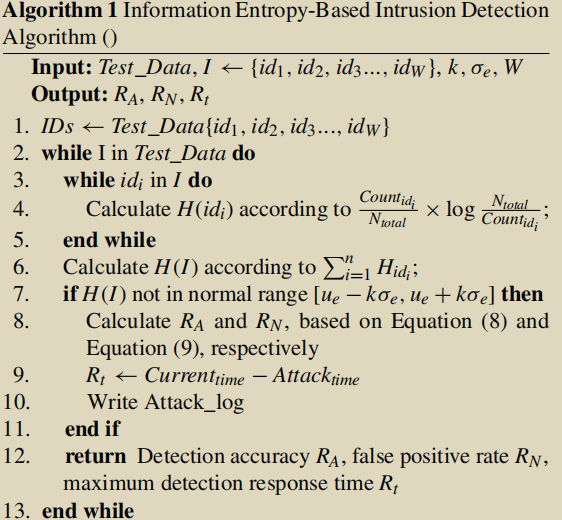
(8)

RN表示正常块的检出率(假阳性率)，

(9)

其中TA是攻击块的总数，DA是IDS检测到的攻击块数，TN是正常块的总数，dn是检测到的正常数据包数。 D由IDS。攻击块由来自攻击节点的连续CAN消息组成。

算法1基于信息熵的入侵检测算法()



算法1的主要思想是计算出现在滑动窗口中的所有消息ID的信息熵，其中test\_data由具有以下内容的can消息集组成。 攻击块，RT是指攻击检测的响应时间。然后，对网络进行实时监控，防止滑动窗口单元的入侵。使用固定数量的消息W。 作为本研究的滑动窗口。对熵测量算法的详细说明如下：1)在第1行中，给出了算法的输入和输出参数。输入测试D ATA是来自CAN总线的真实消息数据，由示例窗口内的监视器节点接收[21]。输出是该参数下的检测精度和响应时间。2)在第2-6行中，我们计算 计算滑动窗口中每个ID的信息熵。然后得到整个滑动窗口的信息熵。3)在第7-10行中，我们判断熵是否在正常范围内。 ，并得到检测结果。第4行给出了主要的时间复杂度。算法1的时间复杂度为O(x=0)。

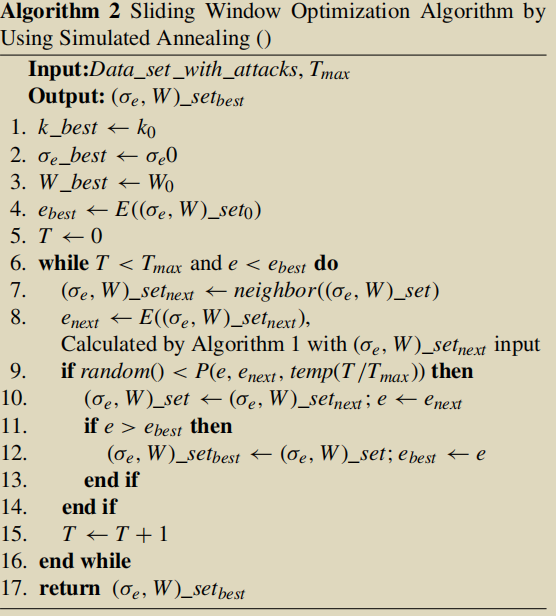
改进熵测量算法

在针对车载网络环境设计入侵检测系统时，应尽可能提高检测正确率，而错误阳性率(Rn)应尽可能低。 尽可能。我们采用模拟退火(SA)算法(即算法2)来优化算法1中使用的参数，并给出了算法1的能量函数。

（10）

其中E()是代表模型检测精度和效率的能量函数。该函数基于算法1，符合方程(8)和方程(9)。 )使用三个加权参数C1、C2和C3来评估所提出的入侵检测系统的特性，其中这些参数固定在训练阶段。这些参数 可以对入侵检测系统进行调整，以获得不同的入侵检测特性。考虑到车辆的安全性，我们分别设定C1=1，C2=0.5，C3=1。

主要思想 算法2是通过模拟退火快速确定最佳滑动窗口尺寸W和偏差σe，实现高精度、快速的入侵检测。(σe，W)\_SET\_0是一个初始解 随机产生的离子，其中σe是偏差，k是偏差的敏感性，ue是平均信息熵。算法2的目标是获取参数设置。 (σe，W)\_SET\_BEST在最大化E()的情况下。



滑动窗口优化算法在算法2中得到描述，邻居()是一个随机生成(σe，W)集候选的邻域函数。算法2的主要时间复杂度 出现在第7行。由于算法1的时间复杂度为O(x=0)，算法2的时间复杂度为O(x=0)，所以算法2的时间复杂度为O(x=0)。

实验与评价

利用所描述的攻击场景和检测算法，我们进行了以下三个实验来评估和验证该方法的有效性。在实验1中，我们分析了 不同滑动窗口策略对信息熵分析的影响。在实验2中，滑动窗口大小对入侵检测性能的影响，包括响应时间和检测。 在精度方面，进行了测试和分析。在实验3中，根据最佳滑动窗参数，确定了真实汽车网络交通测试数据中攻击检测的效果到算法2。

测试数据集

汽车攻击的多样性和不确定性给车载网络安全研究带来了获取数据集的困难。在本研究中，我们使用了真实的汽车环境。 [21]提供的总线网络数据集。表1显示了数据集特性。表中的DoS攻击数据集是通过将id=0x000的can消息块插入到实际正常状态中生成的。 车辆数据集其中一个攻击块是指一个连续的攻击消息。攻击块大小设置范围为5-70。为了生成包含注入攻击的数据集以进行模拟，我们 将消息块从合法ECU发送的CAN消息复制到普通车辆数据集，然后将其注入测试数据集。考虑到汽车攻击的不确定性，1000多个DoS 攻击和1000注入攻击出现在整个测试数据集的高斯分布中。

实验1：不同滑动窗口策略的分析

为了评价不同滑动窗口策略下的信息熵分析效果，我们在不同策略下进行了两个信息熵观测实验。图6显示了TH e两个监测结果。图中的X轴表示时间(X轴一致转换为时间进行比较分析)，Y轴表示SING中的信息熵值。 滑动窗。在实验1中，利用两个数据集分析了不同滑动窗口策略对信息熵的影响。数据集1是真实的车载网络通信。 关联数据集[21]。基于数据集1，在添加DoS攻击块后生成数据集2。

在以往的研究中，总线信息熵的观测与固定时间窗[19]、[20]是一致的。图6(A)显示了示例窗口设置为100 ms时的熵分析。 。CAN总线是一个事件触发的网络.因此，本研究以固定数量的信息作为观察窗口。测试数据集中100 ms示例窗口中的平均消息数。 是50条信息。因此，在比较中使用50条消息的滑动窗口大小，如图6(B)所示。图6(A)和图6(B)显示了消息ID的熵分析结果。 在正常网络条件下，图6(C)和图6(D)显示了攻击下的熵分析结果，其中基于算法得到了一个滑动窗口的信息熵值。

观察：通过比较不同滑动窗口策略(固定时间和固定消息号)下的信息熵分析实验，可以得出以下结论： 结论：1)当以固定时间作为滑动窗口时，即使对正常数据进行信息熵评估，整个信息熵也会发生很大的波动。 这种固定时间滑动窗口策略不利于车载网络的入侵检测。2)当将固定数量的消息设置为滑动窗口时， 当对正常数据进行分析时，整个测试数据集的熵略有波动。当分析包含攻击的数据集时，信息熵开始波动。如所述 d在表2中，平均信息熵为2.987，最大偏差为2.637。3)由于最后一次滑动的信息量不足，信息熵急剧下降。 indow(图6(B)结尾)。实验一的结果表明，不同的滑动窗口策略对入侵检测效果有很大的影响。我们发现用固定数目的混乱 年龄作为滑动窗口，有利于基于信息熵分析的入侵检测分析设计。与以前使用固定时间作为滑块的方法相比 G窗口，利用固定数目的消息，可以有效地减少非周期消息引起的信息熵扰动。因此，滑动窗口使用固定数目的 为了减少检测干扰，提高检测精度，本研究采用消息。

实验2：滑动窗口尺寸比较分析

分析了不同滑动窗口大小对信息熵的影响。我们使用一个真实的信息熵网络MES来测量不同滑动窗口大小下的信息熵。 SAGE数据集[21]。最大的入侵检测响应时间是最大时间被夸大的窗口。图7显示了不同滑动窗口大小对信息的影响。 熵。观察：通过测量不同滑动窗口大小的真实车辆数据集的信息熵，得出以下结论：

1. 滑动窗口的大小对减少数据资源和提高精度起着重要作用。大的观测滑动窗口对应于所获得的信息的平滑变化。 所获得的信息熵具有很大的平均值。
2. 大的滑动窗口大小对应于较小的信息熵值。同时，对入侵检测的最大响应时间 N会很大。如表3所述，用于入侵检测的最大响应时间从0.054 ms逐渐增加到0.189 ms。

3)得到了试验d的最佳滑动窗参数。 ATA集使用算法2。在该入侵检测系统中，滑动窗口的大小为60 can消息，以实现响应时间和指令准确性之间的权衡。

实验2的结果表明，滑动窗口参数对入侵检测系统的性能有着重要的影响，这将影响入侵检测系统的准确性和响应时间。如所述 在表3中，滑动窗口大小不仅影响检测精度，而且还影响最大的入侵检测响应时间。最大响应时间是指在滑动窗口中攻击的开始，直到检测到为止。

实验3：入侵检测实验

利用算法2推导出了用于检验滑动窗实际效果的最佳设计参数。考虑到汽车攻击的多样性和不确定性，我们在算法2中使用了数据集。 是真实的车载网络通信数据集[21].该入侵检测系统的滑动窗口大小为60 CAN消息，σe为0.52，ue为4.186。按照 在第二-C节中提到的攻击场景中，我们设计了两种攻击测试，即DoS攻击和CAN总线注入攻击。在V-A部分所提到的测试数据集的基础上，我们开发了fo发光实验。本研究给出的滑动窗最优参数为本研究所用的试验数据集。

首先，对DoS攻击数据进行分析说明。图8显示，当发生对CAN网络的攻击时，攻击数据将导致网络状态发生变化。这个变化 e反映在信息熵中。如图8所示，当检测到滑动窗口中的信息熵值超出正常范围时，系统将进行入侵。 阿宁。然后，对两种攻击场景下的数据采集进行了仿真，验证了该方法的有效性。生成两种类型的攻击数据(DoS和注入攻击)。

整个数据集中的攻击数据呈高斯分布。为了模拟DoS攻击场景，我们考虑了DoS攻击的不确定性。我们将高优先级的DoS攻击添加到真正的-l中。 给定高斯分布的IFE车辆网络数据集。为了生成注入攻击场景，我们采用了重放攻击的方法，生成先前发送的CAN消息。分 接着，我们对这两种攻击场景进行入侵检测。实验结果如图9所示。图中的X轴表示偏差k的灵敏度，Y- 轴表示单个滑动窗口中的信息熵值。在实验中，我们发现偏差k的灵敏度设置对检测精度有很大的影响。 我们可以得出以下结论：

图9显示，当偏差k为0.5时，所提出的方法对DoS攻击的影响迅速增加，而对于注入攻击，则发生同样的情况。 n偏差k的灵敏度为0.8。另外，当偏差k的灵敏度增加到一定程度时，在达到一定值后，检测精度不会提高。 。在图9中，我们还可以看到，注入攻击的检测精度达到最大值要求k的值为1.1，但是k的值必须较小 n1用于DoS攻击检测。因此，考虑到未知的攻击类型，如何确定合适的k值是本研究尚未解决的问题，也是一个重要的问题。 我们未来的研究课题。该方法的最佳入侵检测结果如表4所示，该方法对DoS和注入攻击的检测准确率为100%a。 Nd分别为92.3%。两种情况下的假检出率均为0%。

最后，对于相同的实验条件，偏差k的灵敏度为0.6，σe为0.5 2，ue 4.186.我们实现了[20]中提出的基于熵的入侵检测方法。 h使用固定时间作为滑动窗口。假设数据集中60 CAN消息的平均间隔为0.11s。因此，在对比实验中，我们采用0.11s作为滑动窗口的大小。我们 生成不同攻击块大小的测试数据，两种方法的入侵检测效果如图所示。

观察：通过在不同的滑动窗口策略(固定时间[20]和基于固定消息计数)下的检测精度比较实验，我们得出如下结论：

1. 如图10(A)所述，对于DoS攻击，当攻击块大于60 CAN消息时，我们的方法和[20]方法具有更高的检测精度。
2. 如图10所述 (B)对于注入攻击，当攻击块的大小大于30时，该方法的检测准确率达到92.3%。文[20]方法检测精度达到91.0%。 n攻击块大于50。
3. 实验结果表明，当攻击块较大时，[20]方法具有明显的效果，对于较小的攻击块，检测结果并不理想。 攻击封锁。
4. 在算法计算复杂度方面，由于它们都是基于信息熵的，所以两种滑动窗口策略的算法复杂度是相同的。然而，在 在实际运行过程中，认为CAN网络是一个事件触发的网络，即网络中的消息在时间域内的分布并不均匀。因此，固定 基于时间的滑动窗口策略将包含一些无效的周期计算，并且我们的滑动窗口策略可以更有效地利用计算资源来分析消息信息绳状的.

总结：通过对两种攻击场景的入侵检测实验，我们发现优化的滑动窗口策略提高了基于入侵检测系统的检测精度。 关于信息熵与现有的车辆网络入侵检测方法[20]相比，该方法对不同攻击块大小的攻击具有较高的入侵检测精度。该方法对DoS和注入的入侵检测准确率分别为100%和92.3%。我们还强调，我们的入侵检测方法在我们的扩展程序中不需要很长的响应时间。食物评价因此，一种低成本、高兼容性、低响应时间的入侵检测方法特别适用于汽车网络环境中的异常入侵检测。

相关作品

车载网络的安全增强方法主要包括消息加密和认证、防火墙和入侵检测.与其他方法相比，入侵检测方法 D可以有效地节省宝贵的带宽，并且与市场上大量的现有车辆兼容。[25]和[26]中的研究人员表明，当攻击者注入合法信息时 若要执行欺骗攻击或DoS攻击，频率将增加。这种检测方法具有精度高、假阳性率低等优点，但只适用于周期性业务。奥 汽车网络异常检测的流行设计是基于指纹信息的[18]、[27]、[28]。

基于机器学习的方法也被应用于车载网络的入侵研究[24]，[29].然而，由于对它们的计算性能要求很高，导致了它们的不适用性。 当前的车内环境。基于信息熵的方法具有成本低、兼容性强的特点。因此，这种方法被认为适用于异常情况。 车辆网络环境下的入侵检测。以前与本研究有关的更相关的研究是[19]和[20]。

在[19]中，Muter和Asaj首次提出了基于内隐式攻击检测的概念。他们专注于具有相同ID的消息，而不是考虑所有的cantr。 情感数据。这种方法的优点是可以精确地攻击ID以确定特定的攻击类型。缺点是它很容易影响信息熵。 由于汽车运行状态的变化而具有相同ID的消息；因此，它被错误地检测到。CAN是一个事件触发的网络.因此，消息通常有不同的p。 路径(从0.01 ms到几秒)，这可能导致观察窗口中的一些消息消失。在[20]中，Marchetti等人。评估信息的有效性 应用于现代车辆网络中的异常检测算法。他们通过实验发现，直接利用信息熵对所有CA进行异常入侵检测。 n消息只有在大量伪造CAN消息的情况下才有效。

该方法考虑了CAN总线的特点和汽车电子系统环境的特点，适用于周期和非周期的CAN环境，解决了系统的安全问题。 现有解决方案的评述。有效地提高了入侵检测的准确性，并设置了最优的滑动窗口，减少了响应时间。

结论

基于信息熵的入侵检测方法，它考虑了汽车成本和计算性能的限制，以及汽车网络攻击的多样性和不确定性。 RKS具有成本低、兼容性强的特点。本文通过分析CAN网络的特点，改进了分析了以往基于信息熵的入侵检测方法，提高了对低响应时间的车载网络攻击的检测精度。参数，如最佳滑动Windo 采用基于固定消息数的滑动窗设计模拟退火方法，得到W尺寸、标准差和相应的灵敏度。检测性能 通过实验对所提出的方法进行了评价，并根据实际CAN流量数据集进行了验证。实验结果表明，所提出的方法能够有效地实现。 提高了车辆网络DoS和注入攻击入侵检测的准确性和有效性.未来可考虑的研究主要是考虑其影响。 车辆运行状态对信息熵的影响。