DeepL
订阅DeepL Pro以翻译大型文件。
欲了解更多信息，请访问www.DeepL.com/pro。

基于红外传感器的自主汽车智能安全系统

Khattab M Ali Alheeti, *会员，IEEE*
英国科尔切斯特埃塞克斯大学计算机科学和电子工程学院，kmali@essex.ac.uk 安巴尔大学，计算机学院-安巴尔，伊拉克

Klaus McDonald-Maier，*IEEE高级会员*
英国科尔切斯特，埃塞克斯大学计算机科学和电子工程学院
kdm@essex.ac.uk

***摘要*--**
自驾车辆的外部通信系统中的安全和非安全应用需要对控制数据、合作意识信息和通知信息进行认证。传统的安全系统可以防止攻击者入侵或破坏自动驾驶汽车的重要系统功能。本文提出了一个新颖的安全系统，旨在保护自动驾驶和半自动驾驶车辆中的车辆特设网络，该系统是基于集成电路计量技术（ICMetrics）。ICMetrics有能力利用自主车辆系统本身的特征来保护自主车辆中的通信系统。这个安全系统是基于从车辆行为及其传感器中提取的独特特征。具体来说，从红外传感器的偏差值中提取的特征与从模拟车辆特设网络的跟踪文件中提取的语义信息一起使用。该系统的实际实验实施和评估表明，该系统在识别典型攻击的异常/恶意行为方面很有效。

***索引词*--安全系统，入侵检测，自主车辆，ICMetric技术。**

I. 简介

自动驾驶和半自动驾驶车辆有可能改善乘客的安全。它们通过减少交通堵塞和车祸来实现这一目标，而交通堵塞和车祸往往是人为错误的结果。自主车辆通过利用通信系统与路侧单元（RSU）交换合作意识信息（CAMs）、警告信息、警告信息、控制数据和敏感信息。车载特设网络（VANET）是自动驾驶和半自动驾驶车辆中采用的典型的外部通信系统[1]。

这项新技术的成功有赖于无人驾驶汽车中VANET的安全性。然而，VANET中的一些特点导致了整个通信层的漏洞[2]。由于高度动态的拓扑结构、车辆的速度、移动性、开放介质无线通信、没有固定的安全系统以及在某些情况下道路上有大量的车辆，外部通信系统本身就是一个复杂的系统[2]。在这些复杂的情况下，攻击者可以远程发动攻击。总的来说，VANET中的通信被置于两种类型中[3]。

- 车对车通信（V2V）--
  当自主车辆彼此建立直接无线通信，形成V2V。
- 车辆到RSU（V2R）--
  这代表了自动驾驶车辆和其固定设备之间的信息共享方式。

RSU。这种通信是通过形成V2R来实现的，并被用于监测交通和管理服务。

图1显示了自主车辆的VANETs的概况。其含义是，入侵检测系统（IDS）执行识别和防止这些系统的内部和外部攻击的功能。与其他类型的网络相比，自驾车辆的外部通信系统更容易受到攻击，例如有线局域网。这是由于缺乏固定的安全基础设施；开放的无线媒介，以及高度动态的网络拓扑结构，使这种脆弱性暴露在攻击面前[2]。

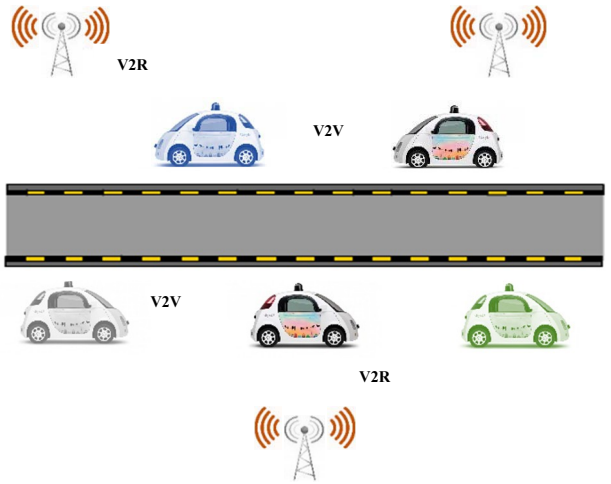

图1：自动驾驶汽车的外部通信系统。

一种被称为集成电路指标（ICMetrics）的新兴技术可以被用来为电子系统创建一个独特的标识符[4]。该技术利用设备的可测量特征来创建一个身份（基础编号）。本文研究了从无人驾驶车辆的红外传感器特征中获得的特征，以创建一个独特的标识。ICMetrics可以用于识别和安全的目的，类似于生物识别技术的电子等同物[5]。

在这项研究中，ICMetric与IDS结合在一起，结果显示，它为当前的安全系统增加了一个新的维度。由红外传感器确定的ICMetric基数与传统的IDS相结合，创建了一个新的、强大的检测系统，可用于保护无人驾驶和半自动汽车的外部通信。

这个ICMetric-
IDS被提出来为自动驾驶汽车的外部通信系统建立安全系统，并利用ICMetric技术来识别外来者和内部者的攻击，有两个优点。

- 它通过建立一个由红外传感器的偏差读数产生的ICMetric，加强了自主车辆的认证方面。
- 创建智能ICMetric-
  IDS，这取决于自驾车辆的特征。显示正常或恶意行为的特征是从利用第二版网络模拟器（ns-
  2）生成的跟踪文件中提取的。

本文的其余部分组织如下：第二节讨论了相关的工作，第三节讨论了VANET的概况。第四节研究了拟议的ICMetric智能入侵检测系统，而第五节重点讨论了拟议安全系统的方法。第六节讨论了模拟的结果。第七节介绍了关于拟议的ICMetric-IDS的讨论，最后一节介绍了结论和未来工作。

II. 相关作品

由于VANETs对社会的直接和积极影响，人们对无人驾驶和半自动汽车的出现产生了极大兴趣。为了在车辆和RSU之间移动和交换重要信息，这些车辆广泛地依赖于对周围环境的感知。在这些车辆中使用的外部通信系统具有一些特点，使其容易受到不同的攻击[2]。

Chaudhary等人在[6]中提出了一种新型的入侵检测，它利用模糊逻辑来为移动广告网络（MANET）提供安全。该安全系统可以检测掉落的攻击，并从他们的互联网协议（IP）交换中阻止恶意车辆。

最近由[3]提出了一种智能安全，以保护自驾车辆的外部通信免受内部或外部攻击。它有能力检测和防止可能对乘客安全产生负面影响的灰洞和冲撞攻击。IDS是基于从ns-
2的跟踪文件中提取的特征生成的。

在[7]中，研究人员介绍了当前车辆互联网的保护和隐私系统的各个方面，该系统在弥补所有安全漏洞方面发挥了重要作用。

在[8]中，提出了一个IDS，为自驾车辆的路由协议提供足够的安全性。该系统被设计在网络层，用于部署在RSU和车辆上。它有能力提供足够的安全性，以保护数据和信息免受黑洞攻击。

这项研究的目的是为车辆的外部网络设计一个智能IDS，以防止诸如Sybil和两种类型的拒绝服务（DoS）的攻击。1）灰洞和2）黑洞。

III. VANET的概述

安全和隐私是VANET的严重问题。这些问题
车辆负责发送警告信息和CAMs
通过开放的无线信道，在无线电覆盖区域内通知其他节点它们的状态。发送这些信息的目的是为了确定车辆的状态，从而。

自驾车辆的通信配置在很大程度上取决于对车辆和周围环境的控制数据和信息的正确获取。更详细地说，它们需要最新的通信协议、运动学数据和定位系统的帮助，以便在它们之间进行可靠和有效的信息交流。传感器、通信系统和车载单元（OBU）共同作用于自驾车辆，以提供车辆和基础设施所需的广泛服务[9]。

该通信系统允许支持OBU的车辆与同一通信区内的其他车辆或RSU之间发送和接收信息。这些设备在提供短程无线ad hoc网络以向车辆网络传输所需的运动数据和控制数据方面发挥着重要作用。这些功能有助于促进上述道路上的交通效率和安全[10]。此外，全球定位系统（GPS）或差分全球定位系统（DGPS）接收器被安装在自动驾驶车辆上，以处理其位置[11]。

其他固定的基础设施，如路侧单元被连接到网络主干，它们被安装在道路的重要位置，以提高车辆特设网络的可靠性和效率。最后，网络设备被连接到RSU，以利用IEEE 802.11p无线电技术为专用短程通信（DSRC）提供支持。

IV. 入侵检测系统

入侵检测系统被看作是任何安全系统中必不可少的第二层，旨在识别恶意行为[12]。这些系统在识别对自主系统的各种攻击方面起着非常重要的作用。在传统的安全系统中，例如，主要的担忧是加密/解密不具备识别内部/内部攻击的能力[12]。

IDS通过访问控制和认证方法，利用预防机制来保护敏感数据的安全。根据收集到的来源日期集，这可以被分为基于网络的入侵检测（NID）和基于主机的入侵检测（HID）。HID集成在计算机上，以便能够监测审计跟踪。而NID则是基于从网络流量中收集的数据。
检测方法，包括异常和滥用检测系统，在IDS的分类中被采用[13]。异常或行为方法的检测过程是基于识别VANETs中无人驾驶车辆的正常交通行为。因此，它具有检测主动攻击的能力。这是通过确定系统已经明显偏离其正常行为来实现的。当这种情况发生时，这种行为被认为是不正常的。

另一种检测系统，被称为滥用或签名检测系统，是基于预先定义的数据或系统漏洞。这种检测系统只是将流量

用异常行为的签名来检测VANETs中的恶意行为。这些系统的唯一问题是，它们没有能力检测新的攻击类型。

相反，通过基于异常的检测系统，可以检测到以前没有遇到过的新型攻击。这意味着滥用检测是基于规则而不是模式，因此可以检测到自主车辆外部通信中的任何类型的异常行为。通过这种方法，不仅可以检测到恶意行为，而且还能够检测到未知/新的恶意行为。此外，利用异常检测系统，可以通过合法用户的错误应用来识别入侵行为，而不会破坏安全政策[14], [15]。

异常检测系统的局限性是高假阳性检测错误，加上昂贵的计算负载和难以处理渐进式不当行为[16]。滥用检测方法有很多局限性，如不灵活和难以更新入侵签名规则[15]。两种系统固有的优点和局限性意味着一个有效的IDS应该同时使用签名和行为检测[16]。

这里提出的保护系统是一个异常检测系统，以确保自动驾驶和半自动驾驶车辆的外部通信。

V. ICMETRIC INTELLIGENT INTRUSION DETECTION SYSTEM

目前的防御机制的一个问题是，它们缺乏在VANET中有效防止内部攻击所需的特征。在拟议系统的设计中采用ICMetric技术的目的是，它有能力使用从特定嵌入式系统的特征中提取的可测量的特征[17]。这些特征可以为一个特定的系统产生一个独特的标识符。这些特征被提取出来，然后被规范化，以验证它们的唯一性和确定性特征。在本文中，重点是利用现代自主系统中通常存在的红外传感器作为设备识别的基础。在设计拟议的IDS时利用了红外传感器的偏差读数。这些读数被用于创建一个ICMetric基础编号。

拟议的ICMetric-IDS由六个阶段组成；图3显示了拟议的ICMetric-IDS的整体架构。

- 1st 阶段（生成ICMetric号码）--在这个阶段，从自主车辆的红外传感器中提取偏移读数。采用统计函数从传感器提取的读数中计算出ICMetric的基础数字。除此之外，还从ICMetric号码中生成哈希值，该值将用于ICMetric-IDS。下面的图2显示了设置的硬件，它由红外线（IR）传感器红外模块Arduino raspberry PI传感器组成，它被嵌入了红外线传感器。

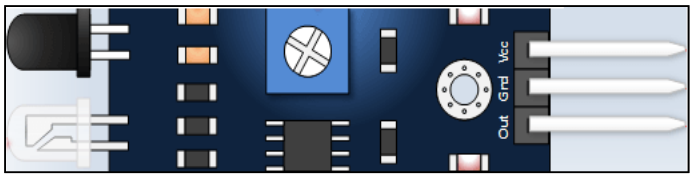

图2: 红外线传感器。

- 2nd 阶段（现实世界）--在创建现实世界的模拟时，利用了两个软件工具。这些工具是模拟城市移动性（SUMO）和移动性车辆（MOVE），反映车辆的移动性。
- 3rd 阶段（特征提取）--建议的ICMetric-IDS只利用整个提取的特征空间中的16个重要特征[8]。我们还发现，减少特征的数量对提高检测率、降低错误率和误报有重要作用。
- 4th 阶段（预处理）。这个阶段的重要特征是进行预处理，如：a）将一些符号和字母转为数字，b）做均匀分布以平衡正常和异常记录，以提高IDS的效率，c）从跟踪文件中产生的特征值在这个阶段被规范化，使ICMetric-IDS的性能在检测和阻止恶意行为方面更加有效。
- 5th 阶段（训练阶段-k-近邻（k-NN））。在设计ICMetric-IDS时采用了k-NN。在第三阶段提取的数据集被用于拟议的IDS的训练阶段。
- 6th 阶段（测试阶段-k-NN）。这一阶段涉及用提取的特征对ICMetric-IDS进行测试。检测准确率和四种警报也在测试阶段进行计算。一些标准被用来衡量k-NN的效率。这些标准包括检测率、数据包交付率（PDR）、错误警报的数量和端到端延迟。

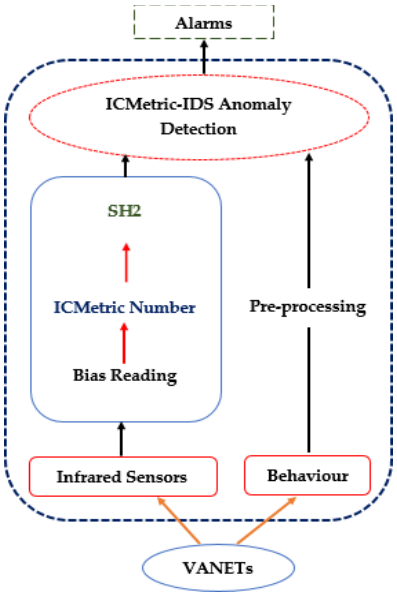

图3：ICMetric-IDS的整体架构。

安全系统最初评估来自红外传感器的ICMetric基础编号。ICMetric基数与CAMs相结合，CAMs在无线电覆盖区域内从源车到目的车发出信号。提取的正常/异常行为的特征需要一个预处理阶段，以使拟议系统易于适应。然后，它们被认为是ICMetric-IDS的输入。最后，IDS的输出被分类为正常或恶意的。

VI. 仿真结果

本实验中从红外传感器获得的偏差读数被用于创建一个新颖的ICMetric-IDS，以检测内部/外部攻击。为了生成ICMetric数字，从三个相同的传感器中提取了偏置读数，并为三个不同的轴记录了1000个读数。在测试阶段，生成的读数被用来评估自主车辆的外部通信系统的异常检测。

为了评估ICMetric-IDS的性能，使用了检测准确率和四种警报。用于评估拟议的IDS的警报是：1）假阳性，2）真阳性，3）假阴性和4）真阴性。表1显示了ICMetric-IDS与传统IDS的检测率和误报情况。

表1.检测率和误报。

性能指标	吞吐量	PDR	延迟
无IDS的VANETs	1.02%	0.05%	23.*33ms*
带有普通IDS的VANETs	78.57%	97.86%	1.*47ms*
使用ICMetric-IDS的VANETs	79.23%	99.54%	30.*56ms*

表1显示了ICMetric-IDS在自主车辆的VANETs中在不同类型的攻击下的明显改进，其平均错误率为6.01%。在下面的表2中，我们显示了ICMetric-IDS的性能指标。

表2.性能指标。

性能指标	检测率		虚假警报
	正常	不正常	
带有普通IDS的VANETs	98.45%	85.02%	12.24%
使用ICMetric-IDS的VANETs	95.23%	92.74%	3.69%

提出的ICMetric-IDS和传统的IDS在异常条件下进行评估，以评价其性能指标。

VII. 讨论

自动驾驶汽车的成功部署在很大程度上取决于适当的安全系统。

仿真结果显示，6.01%是使用ICMetric的IDS的平均错误率，而检测率在95.23%和92.74%之间变化，精确度很高。此外，结果显示，平均错误报警率约为3.69%，非常低，这也是结果有希望的另一个指标。

另一方面，普通IDS的检测率在85.02%和98.45%之间，而误报率保持在12.24%。通过使用ICMetric技术和k-NN，检测率得到了提高。通过计算性能指标、PDR、吞吐量和端到端延迟，ICMetric-IDS的重要性已在表2中列出。

仿真结果与以前的工作[2]进行了比较。拟议的ICMetric-IDS的结果显示了较高的检测准确率，在检测自主车辆的恶意行为时，误报率较低，也有一些错误。

VIII. 结论和未来工作

提出了一种基于ICMetric的车辆传感方法，该方法利用红外传感器的特定偏置特性，为自动驾驶车辆的外部通信提供保护。在本文中，采用了一种新的车辆识别方法，即从红外传感器得出的车辆ICMetric基数来识别自动驾驶车辆。ICMetric-IDS是为训练和测试异常和正常行为而设计的，它建立在ns-2上。它有能力识别外部和内部攻击。

这个ICMetric-IDS是一个新颖的入侵检测系统，它为VANETs提供保护，首次将ICMetrics用于保护自主车辆的外部通信。异常ICMetric-IDS在识别自动驾驶和半自动驾驶车辆的外部通信的恶意车辆方面显示出一些令人满意的性能。ICMetric-IDS是一个智能IDS，它将有能力检测甚至阻止其他类型的攻击，如Sybil和虫洞攻击。

参考文献

[1] K.Ali Alheeti, A. Gruebler, and K. McDonald-Maier, "Intrusion Detection of Grey Hole and Rushing Attacks in Self-Driving Vehicular Networks, " *Computers*, vol. 5, no.3, p. 16, Jul. 2016.

[2] K.M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," in *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCN)*, 2015, pp.

[3] K.M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "On detection of gray hole and rushing attacks in self-driving vehicular networks," in *2015 7th Computer Science and Electronic Engineering Conference (CEEC)*, 2015, pp.231-236.

[4] X.Zhai等人，"ICmetrics在嵌入式系统安全中的应用"，*2013年第四届新兴安全技术国际会议*，2013年，pp.89-92。

[5] R.Tahir, H. Tahir, and K. McDonald-Maier, "Securing Health Sensing Using Integrated Circuit Metric," *Sensors*, vol. 15, no. 10, pp. 26621-26642, Oct. 2015.

[6] A.Chaudhary, V. N. Tiwari, and A. Kumar, "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks, " *Souvenir 2014 IEEE Int.Adv.Comput.Conf.IACC 2014*，第256-261页，2014。

[7] K.Zaidi, M. Rajarajan, S. Furnell, and A. Hudson-Smith, "Vehicular Internet:安全和隐私的挑战和机会，"*Futur.互联网*，第7卷，第257-275页，2015年。

[8] K.M. A. Alheeti, A. Gruebler, and K. D. McDonald-Maier, "An Intrusion Detection System against Black Hole Attacks on the Communication Network of Self-Driving Cars, " in *2015 Sixth*

新兴安全技术国际会议（EST），2015，第86-91页。

[9] E.C. Eze, S. Zhang, and E. Liu, "Vehicular ad hoc networks（VANETs）:现状、挑战、潜力和发展方向"，载于*2014年第20届国际自动化和计算会议*，2014年，第176-181页。

[10] S.Zeadally, R. Hunt, Y. -S.Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommun.系统。*, vol. 50, no.4, pp. 217- 241, Aug. 2012.

[11] J.Jakubiak和Y. Koucheryavy，"VANETs的技术现状和研究挑战"，*2008年第五届IEEE消费者通信和网络会议*，2008年，第912-916页。

[12] D.Tian, Y. Wang, G. Lu, and G. Yu, "A vehicular ad hoc networks intrusion detection system based on BUSNet," *2010 2nd Int.Conf.Futur.计算。通信。*, pp. V1-225-V1-229, 2010.

[13] K.M. Ali, W. Venus, and M. S. Al Rababaa, "The affect of fuzzification on neural networks intrusion detection system, " *2009 4th IEEE Conf.Ind.Electron.Appl. ICIEA 2009*，第1236-1241页，2009年。

[14] D.E. Denning, "An Intrusion-Detection Model," *IEEE Trans.Softw.Eng.*，第SE-13卷，第2期，第222-232页，1987年2月。

[15] P.Porras，"STAT--入侵检测的状态转换分析工具"。加州大学圣巴巴拉分校，1993年。

[16] B.Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection, " *IEEE Netw.*, vol. 8, no.3, pp. 26-41, May 1994.

[17] X.Zhai等人，"ICmetrics在嵌入式系统安全中的应用"，*2013年第四届新兴安全技术国际会议*，2013年，pp.89-92。