Application Brief

在车辆入侵监控系统中使用雷达

Ethan Cope, Tim Henderson

简介

随着机动车辆盗窃案件持续增加（根据刑事司法委员会的数据，2022 年至 2023 年的增幅达 105%），许多消费者正在寻求新的设计方案以确保车辆安全。车辆集成的视频行车记录仪作为一项新功能，有助于满足这一需求。尽管行车记录仪历来被用于记录道路事故，但越来越多的售后市场和集成行车记录仪系统开始提供一种新的保护形式：外部入侵监控。

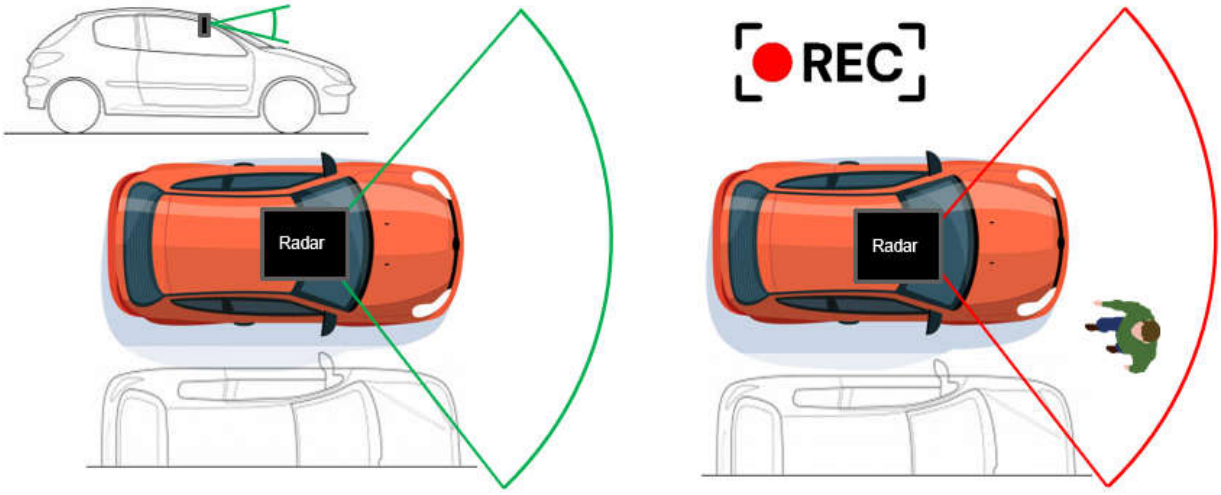

图 1. 外部入侵监控系统示例

基于摄像头的设计

许多现代车辆的高级驾驶辅助系统 (ADAS) 已经安装了面向外部的摄像头，车外入侵监控系统正是利用了这一点。当车辆停驻后，这些摄像头保持打开状态，旨在记录发生的任何入侵或破坏事件。在这些系统中，较先进的系统会利用机器学习算法来识别可疑活动，并警告潜在入侵者其活动正在被记录。此类系统还可以在检测到可能的入侵事件时实时通知车主。

但是，基于摄像头的外部入侵监控系统存在一些重大缺点，如功耗、非理想天气下的精度以及违反法规等问题。实时处理多个摄像头数据流会消耗大量电能，在某些情况下高达约 75W。在电动汽车中，寄生能耗会直接影响车辆的续航里程。基于摄像头的系统的精度也会根据情况有所不同。图像处理在理想天气条件下的表现良好，但精度通常受到弱光和恶劣天气条件的负面影响。例如，水滴可能会使摄像头图像失真，导致无法进行图像识别。最后，持续录像的系统可能不符合法规要求，例如欧盟 (EU) 的《通用数据保护条例》(GDPR)。

基于雷达的设计

雷达传感器可以解决基于摄像头的检测方案所固有的许多缺点。采用雷达的增强型外部入侵监控系统仍有一个面向外部的录像机，但摄像头传感器默认处于停用状态以节省电量。这种情况下改用了 AWRL6432 雷达片上系统 (SoC) 等器件来作为录像机的低功耗、高精度唤醒器件。凭借器件集成的处理能力，雷达 SoC 可以智能地区分路

English Document: SWRA829

人和潜在入侵者。如果雷达 SoC 确定即将发生入侵事件，SoC 可以触发车辆闪烁前照灯并开始录制视频以阻止入侵。图 2 展示了 EIM 一种可能的实现方式：雷达检测到潜在的入侵者，但只有当入侵者接近车辆或过于接近时才会唤醒摄像头。

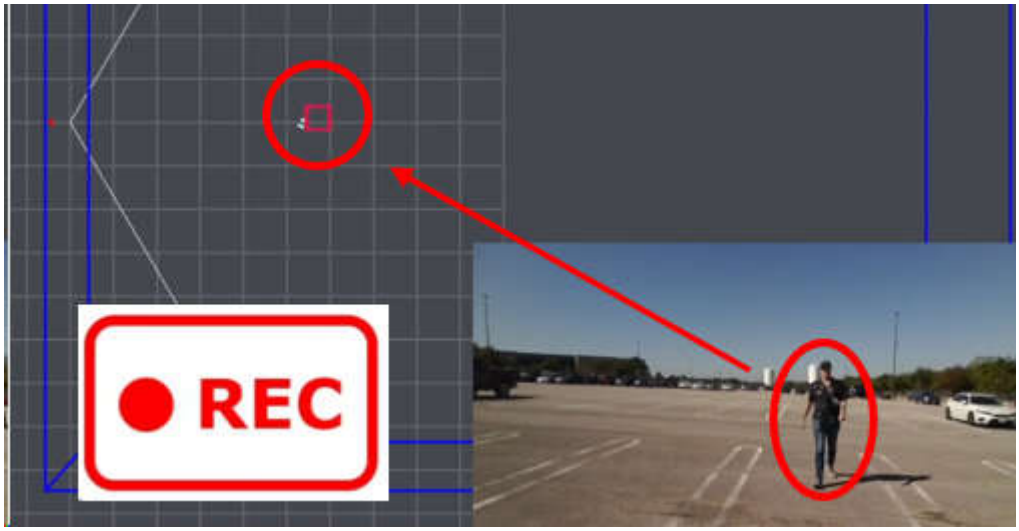

图 2. 接近检测 EIM 实现方案

节能

使用雷达可以显著降低这些检测系统的被动功耗。当作为这些系统的唤醒器件进行调优时，AWRL6432 的功耗仅为 22mW，比同类图像处理系统的 75W 平均功耗低三个数量级。假设在一个用例中，这两个系统都安装在电动汽车上，车辆的平均效率为 2.9 英里/kWh。经过 24 小时的监控后，基于摄像头的系统可能导致电动汽车的续航里程缩短 5 英里。使用雷达作为唤醒触发器时，同一车辆损失的续航里程只有 8 英尺。

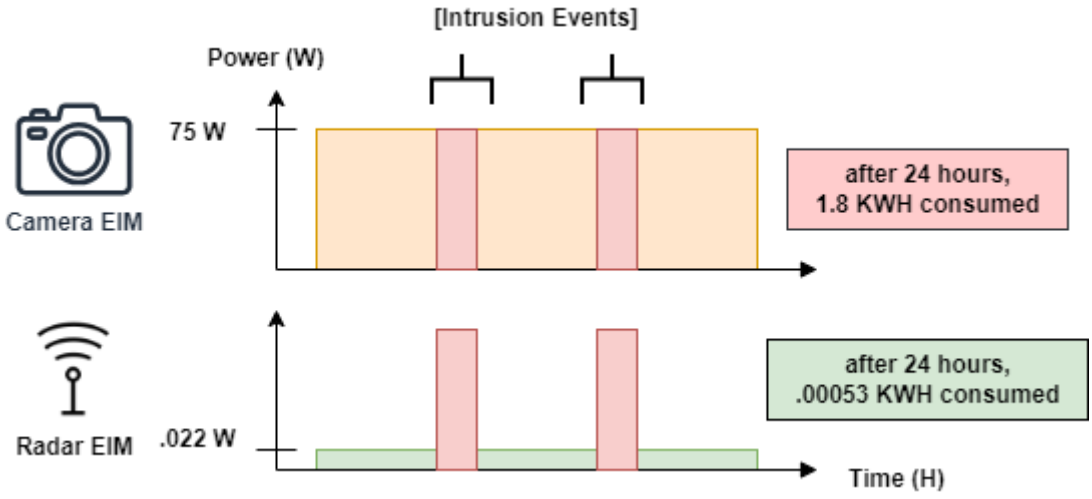

图 3. 雷达与摄像头 EIM 的功耗对比

减少误报

在检测到入侵的情况下打开摄像头或闪烁车灯仍然会耗电，但基于雷达的设计可通过独特的方式减少误报，从而保持低功耗。雷达增加了根据物体的实时位置、速度和加速度来定义摄像头唤醒逻辑的灵活性。AWRL6432 雷达 SoC 甚至可以通过轻量级机器学习算法处理微多普勒特征，以便将这些物体分类为人类或非人类。借助这种深度的信息，板载处理器可以确定一个人更有可能是入侵者还是路人，并相应采取行动。

雷达用作唤醒传感器

为了尽可能提高入侵监控系统的精度，可以使用雷达作为对现有机器学习摄像头的补充。此架构仍然利用雷达的位置精度以及对弱光或天气条件的无感特性。但是，雷达不会直接触发入侵威慑，而是会激活机器学习摄像头来收集其他数据。因此，机器学习模型可以利用图像和雷达数据对下一步的行动做出最明智的决定。由于车辆仅在满足一组特定入侵条件后才会开始录像，因此无需持续调查周围环境，从而更容易符合当地隐私法规。

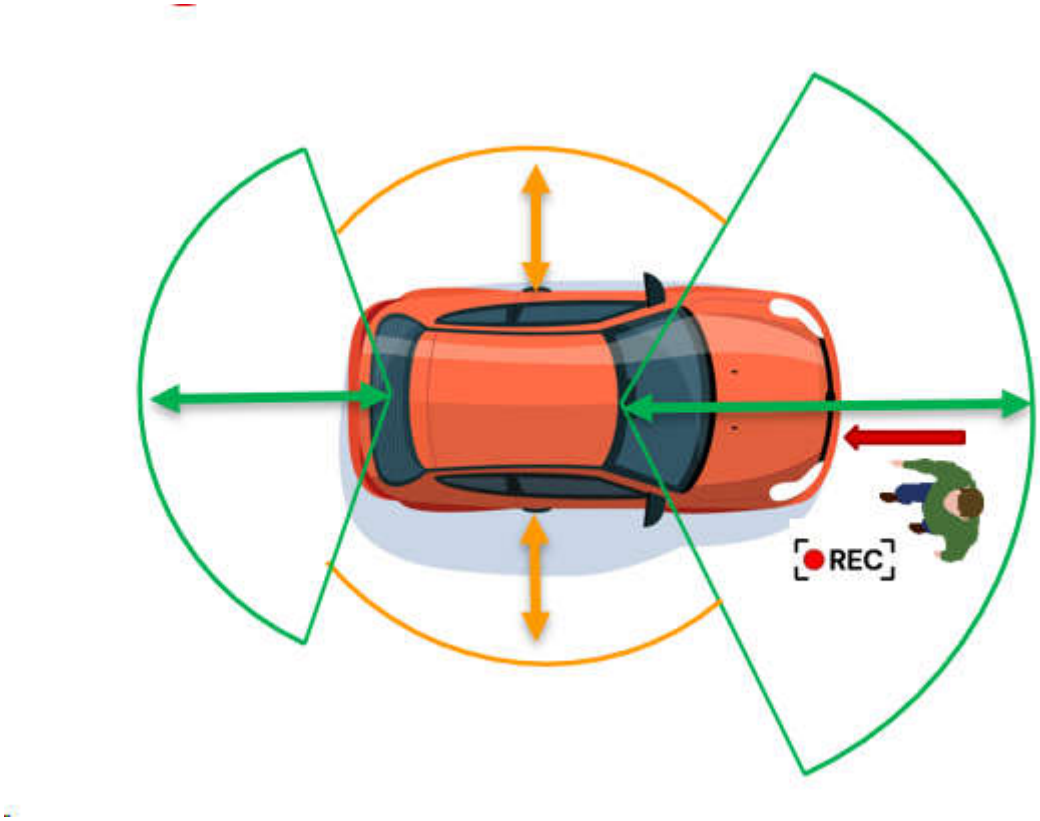

图 4. 多用途雷达实现 360 度覆盖

结语

外部入侵监控领域可能相对较新，但并不是一成不变的。市场仍然需要比现有第一代系统更低的功耗和更高的精度。TI 低功耗雷达设计可以超越这些期望，同时增加新功能。例如，用于儿童存在检测的车内检测雷 (达根据欧洲 NCAP 标准) 可以兼作短距离外部入侵监控传感器。77GHz 电动后备箱门脚踢开启模块可以提供关键的后视功能，从而在车辆周围实现 360 度雷达覆盖。TI 毫米波设计不仅能降低外部入侵监控功耗，还能在不产生额外成本的情况下带来额外的安全性和便利性。

其他资源

评估存在检测行车记录仪演示

- 在 TI.com 上订购 AWRL6432BOOST EVM
- 从 Radar Toolbox 运行外部入侵监控演示
- 在 TI.com 上观看外部入侵监控演示

商标

所有商标均为其各自所有者的财产。

重要声明和免责声明

TI“按原样”提供技术和可靠性数据（包括数据表）、设计资源（包括参考设计）、应用或其他设计建议、网络工具、安全信息和其他资源，不保证没有瑕疵且不做出任何明示或暗示的担保，包括但不限于对适销性、某特定用途方面的适用性或不侵犯任何第三方知识产权的暗示担保。

这些资源可供使用 TI 产品进行设计的熟练开发人员使用。您将自行承担以下全部责任：(1) 针对您的应用选择合适的 TI 产品，(2) 设计、验证并测试您的应用，(3) 确保您的应用满足相应标准以及任何其他功能安全、信息安全、监管或其他要求。

这些资源如有变更，恕不另行通知。TI 授权您仅可将这些资源用于研发本资源所述的 TI 产品的应用。严禁对这些资源进行其他复制或展示。您无权使用任何其他 TI 知识产权或任何第三方知识产权。您应全额赔偿因在这些资源的使用中对 TI 及其代表造成的任何索赔、损害、成本、损失和债务，TI 对此概不负责。

TI 提供的产品受 TI 的销售条款或 ti.com 上其他适用条款/TI 产品随附的其他适用条款的约束。TI 提供这些资源并不会扩展或以其他方式更改 TI 针对 TI 产品发布的适用的担保或担保免责声明。

TI 反对并拒绝您可能提出的任何其他或不同的条款。

邮寄地址：Texas Instruments, Post Office Box 655303, Dallas, Texas 75265