# Article information:

[1907.06826] Adversarial Sensor Attack on LiDAR-based Perception in Autonomous Driving
<https://arxiv.org/abs/1907.06826>

# Article summary:

1. 本文是对自动驾驶中基于激光雷达的感知系统进行安全研究的首次尝试。

2. 文章探讨了利用机器学习模型来欺骗攻击目标车辆的可能性，并设计了相应的优化算法。

3. 作者构建并评估了两种攻击场景，同时也提出了在自动驾驶系统、传感器和机器学习模型层面上的防御方向。

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

本文是一篇关于自动驾驶中基于激光雷达感知系统的安全性研究。文章提出了针对激光雷达欺骗攻击的威胁模型，并将攻击目标设定为在受害者车辆前方伪造障碍物。作者通过优化问题设计建模方法，探索了通过欺骗机器学习模型来实现攻击目标的可能性，并构建和评估了两种可能危及道路安全和流动性的攻击场景。

然而，本文存在一些潜在偏见和不足之处。首先，文章只关注了激光雷达感知系统的安全性问题，而忽略了其他传感器如相机等的安全性问题。其次，文章没有考虑到攻击者需要具备高度专业技能才能进行此类攻击，这使得该研究结果可能被误解为普通人可以轻易地进行此类攻击。此外，在防御方面，文章只简单地提到了AV系统、传感器和机器学习模型三个层面上的防御方向，并未深入探讨如何实现这些防御措施。

总之，本文提供了有价值的研究成果，但需要更全面地考虑相关问题，避免偏见和不足之处。

# Topics for further research:

* Other sensor security issues
* Attacker expertise requirements
* Limitations of the study
* Defense strategies
* Comprehensive consideration of related issues
* Avoiding biases and shortcomings

# Report location:

<https://www.fullpicture.app/item/142b723990c797696b7887a8646c1b05>