2021-8-BCTF自动驾驶-WriteUp

demo

Lane Detection: targeted attack

> 题目说明
> Lane detection is an essential component in low-autonomy autonomous driving systems such as OpenPilot and Tesla Autopilot, which steers the vehicle to keep at the center of the lane based on the detected lane line shapes. Such lane detectors predominantly use DNNs, which are naturally vulnerable to adversarial perturbations to the road surface. In this challenge, a group of armed drug dealers is currently driving an AV with automated lane centering system engaged to deliver drugs. As a drug enforcement agent, your task is to sabotage their mission by causing instability in their driving. However, since they are heavily armed, you need to do that in a stealthy way by placing a malicious road patch to affect the automated lane centering system. More concretely, in this challenge, your road patch needs to cause the AV to deviate laterally and hit the cardboard boxes. Before evaluation, the system will check the patch content and reject the patch if its perturbations are over certain level.Team task: Generate and submit a road patch that can steer the vehicle to crash into the cardboard boxes on the road.

题目附件


task_data_4.zip
27.4MB

解题思路

ADC Programming: interception

> 题目说明
> The planning module is to plan a trajectory that the vehicle can travel based on the result of perception prediction, current vehicle information and road conditions. It is an important part of all levels of automated driving systems. By designing intelligent planning modules, unmanned vehicles can complete some dangerous tasks that do

> not require a driver. In this challenge, we simulated a dangerous interception scene in which a vehicle carrying dangerous goods was driving on the road. Your goal is to submit a planning program to identify the dangerous vehicle on the road and eliminate the threat by hitting it. If it fails to hit the target vehicle or hits the wrong obstacle within the specified time, it will be regarded as a challenge failure. Please note that the escape route (green line in the following image) of the target vehicle will not be provided, and it may not be the same in different executions.Team task: Design and submit a planning program that can automatically plan the path of travel according to the location of the target vehicle to prevent the vehicle from escaping.

题目附件

task_data_0.zip
2.3KB

解题思路

planning.py
5.8KB

Adversarial NPC: single box

> 题目说明
> Autonomous Vehicles (AVs) react to obstacles on the road and choose different planned trajectories using planning algorithms. However, such planning algorithms may contain vulnerabilities that can be leveraged by attackers who’s in control of the trajectories of other vehicles on the road. In this challenge, some AV developers suspect that their current planning algorithm may only consider dynamic obstacles (e.g., cars and pedestrians) when checking for road blocking conditions. Thus, they want you to help them demonstrate if this vulnerability could lead to any real world consequences in order to under its severity. Particularly, we simulate a scenario where the AV drives on a 4-lane road (2 lanes each direction) and it is following the current lane with 20 m/s towards its destination at 400 meters away. Due to the road structure, the AV regards both lanes in the current direction as its candidate lanes in the planning algorithm in case one of them is blocked by any obstacles. Your goal is to manipulate the driving trajectory of another vehicle (let’s call it the “NPC”), who’s originally driving on a lane in the opposite direction, such that the AV will yield and crash into a cardboard box on the road.Team task: Design and submit an NPC trajectory file that can make the AV yield to crash into the cardboard box.

题目附件

task_data_0 (1).zip
20.1KB

解题思路

gps.py
1.5KB

gps_new.json
0.1MB

GPS Spoofing: GPS is all you got

> 题目说明
> For Autonomous Vehicles (AVs), GPS is the de facto sensor for localization. However, GPS has been widely demonstrated to be vulnerable to spoofing attacks, where the attacker sends fake satellite signals to the victim GPS receiver to cause it to output a falsified position. In this challenge, the AV runs in a simulator and its steering wheel is controlled by a lateral controller, which constantly corrects the lateral deviation between the AD localization output (i.e., the GPS positions) and a predefined planned trajectory. You will be helping us test the robustness of the AV design against GPS spoofing. Particularly, you goal is to spoof the GPS positions such that the AV can be deviated by at least 1 meter in the lateral direction.Team task: Design and submit a spoofed GPS position trace that can deviate the AV by 1 meter laterally.

题目附件

task_data_0 (2).zip
4.9KB

解题思路

gps.py
1KB

gps_new.json
28.4KB

Adventure

Basic

> 赛题描述
> According to the following description by NHTSA, this is the level _____ of automation. 'An automated driving system (ADS) on the vehicle can do all the driving in all circumstances. The human occupants are just passengers and need never be involved in driving.'

题目附件：

解题思路
5

Expensive Sensor

> 题目说明
> _____ sensor is common on level-4 autonomous vehicles but is generallly not available on today's level 2 autonomous vehicles.

题目附件：

解题思路
LIDAR

Google it

> 题目说明
> As of July 16, 2021, the California DMV has received ____ Autonomous Vehicle Collision Reports.

题目附件

解题思路
具体忘记了，330-320直接的某个数字，都尝试一下

Try it

> 题目说明
> In order to run challenge evaluation environments locally (please refer to "Evaluation Environments for Players" in https://autodrivingctf.org/#resource), you need to setup ____ simulation environment.

题目附件

解题思路

GPS Spoofing

GPS Spoofing: GPS is all you got

> 题目说明
> For Autonomous Vehicles (AVs), GPS is the de facto sensor for localization. However, GPS has been widely demonstrated to be vulnerable to spoofing attacks, where the attacker sends fake satellite signals to the victim GPS receiver to cause it to output a falsified position. In this challenge, the AV runs in a simulator and its steering wheel is controlled by a lateral controller, which constantly corrects the lateral deviation between the AD localization output (i.e., the GPS positions) and a predefined planned trajectory. You will be helping us test the robustness of the AV design against GPS spoofing. Particularly, you goal is to spoof the GPS positions such that the AV can be deviated by at least 1 meter in the lateral direction.Team task: Design and submit a spoofed GPS position trace that can deviate the AV by 1 meter laterally.

题目附件

task_data_0 (2).zip
4.9KB

解题思路

gps.py
1KB

gps_new.json
28.4KB

Lane Detection

Lane Detection: free drawing

> 题目说明
> Lane detection is an essential component in low-autonomy autonomous driving systems, which steer the vehicle to keep at the center of the lane based on the detected lane line shapes. Such lane detectors predominantly use DNNs, which are naturally vulnerable to adversarial perturbations to the road surface. In this challenge, a group of armed drug dealers is currently driving an AV with automated lane centering system engaged to deliver drugs. As a drug enforcement agent, your task is to sabotage their mission by causing instability in their driving. However, since they are heavily armed, you need to do that in a stealthy way by placing a malicious road patch to affect the automated lane centering system. More concretely, in this challenge, your road patch needs to cause the AV to deviate laterally by at least 2

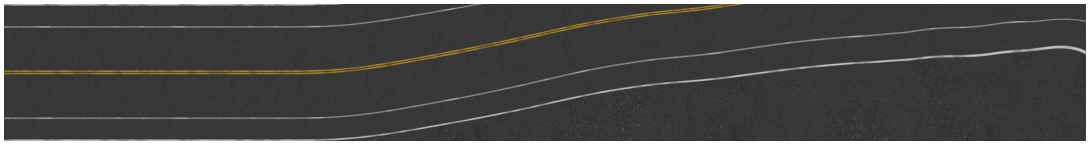
> meters.Team task: Generate and submit a road patch that can steer the vehicle to deviate by 2 meters laterally.

题目附件：

> To get started, you will be provided with a benign road patch without any perturbations as well as the benign camera video when driving on the road. In addition, a Keras lane detection model used in the AV will be provided.

附件太大https://anquan.baidu.com/bctf/games/lanedet-001/task_data_0.zip

解题思路



Lane Detection: dirty road patch

题目说明Lane detection is an essential component in low-autonomy autonomous driving systems, which steer the vehicle to keep at the center of the lane based on the detected lane line shapes. Such lane detectors predominantly use DNNs, which are naturally vulnerable to adversarial perturbations to the road surface. In this challenge, a group of armed drug dealers is currently driving an AV with automated lane centering system engaged to deliver drugs. As a drug enforcement agent, your task is to sabotage their mission by causing instability in their driving. However, since they are heavily armed, you need to do that in a stealthy way by placing a malicious road patch to affect the automated lane centering system. More concretely, in this challenge, your road patch needs to cause the AV to deviate laterally by at least 1 meter. Before evaluation, the system will check the patch content and reject the patch if its perturbations are over certain level.
Team task: Generate and submit a road patch that can steer the vehicle to deviate by 1 meters laterally.

>

题目附件：
https://anquan.baidu.com/bctf/games/lanedet-002/task_data_2.zip
解题思路

Lane Detection: targeted attack

题目说明Lane detection is an essential component in low-autonomy autonomous driving systems, which steer the vehicle to keep at the center of the lane based on the detected lane line shapes. Such lane detectors predominantly use DNNs, which are naturally vulnerable to adversarial perturbations to the road surface. In this challenge, a group of armed drug dealers is currently driving an AV with automated lane centering system engaged to deliver drugs. As a drug enforcement agent, your task is to sabotage their

mission by causing instability in their driving. However, since they are heavily armed, you need to do that in a stealthy way by placing a malicious road patch to affect the automated lane centering system. More concretely, in this challenge, your road patch needs to cause the AV to deviate laterally and hit the cardboard boxes. Before evaluation, the system will check the patch content and reject the patch if its perturbations are over certain level.
Team task: Generate and submit a road patch that can steer the vehicle to crash into the cardboard boxes on the road.

To get started, you will be provided with a benign road patch without any perturbations as well as the benign camera video when driving on the road. In addition, a Keras lane detection model used in the AV will be provided.

题目附件https://anquan.baidu.com/bctf/games/lanedet-003/task_data_4.zip

解题思路
答案和上一题一样

对抗性 NPC

Adversarial NPC: single box

> 题目说明
> 自动驾驶车辆 （AV） 对道路上的障碍物做出反应，并使用规划算法选择不同的规划轨迹。 但是，此类规划算法可能包含漏洞，这些漏洞可能由控制道路上其他车辆轨迹的攻击者利用。 在这项挑战中，一些AV开发人员怀疑，他们目前的规划算法在检查道路堵塞状况时可能只考虑动态障碍（例如汽车和行人）。 因此，他们希望您帮助他们证明此漏洞是否会导致任何现实世界的后果，以降低其严重程度。 特别是，我们模拟了一个场景，即AV在4车道道路上行驶（每个方向2车道），并且它正以20米/s的速度跟随当前车道，向400米外的目的地行驶。 由于道路结构，AV 将当前方向的两条车道视为规划算法中的候选车道，以防其中一条车道被任何障碍物阻塞。 你的目标是操纵另一辆车的行驶轨迹（让我们称之为”NPC”），他最初是在相反方向的车道上行驶，这样AV就会屈服并撞上路上的纸板箱。 团队任务：设计并提交 NPC 轨迹文件，使 AV 屈服于纸板箱。

题目附件

task_data_0 (1).zip
20.1KB

解题思路

gps.py
1.5KB

gps_new.json
0.1MB

Adversarial NPC: single box with constraints

> 题目说明
> Autonomous Vehicles (AVs) react to obstacles on the road and choose different planned trajectories using planning algorithms. However, such planning algorithms may contain vulnerabilities that can be leveraged by attackers who's in control of the trajectories of other vehicles on the road. In this challenge, some AV developers suspect that their current planning algorithm may only consider dynamic obstacles (e.g., cars and pedestrians) when checking for road blocking conditions. Thus, they want you to help them demonstrate if this vulnerability could lead to any real world consequences in order to under its severity. Particularly, we simulate a scenario where the AV drives on a 4-lane road (2 lanes each direction) and it is following the current lane with 20 m/s towards its destination at 400 meters away. Due to the road structure, the AV regards both lanes in the current direction as its candidate lanes in the planning algorithm in case one of them is blocked by any obstacles. Your goal is to manipulate the driving trajectory of another vehicle (let's call it the "NPC"), who's originally driving on a lane in the opposite direction, such that the AV will yield and crash into a cardboard box on the road.
> Team task: Design and submit an NPC trajectory file that can make the AV yield to crash into the cardboard box.

题目附件

解题思路
解答同上一道

ADC Programming

ADC Programming: interception

> 题目说明
> The planning module is to plan a trajectory that the vehicle can travel based on the result of perception prediction, current vehicle information and road conditions. It is an important part of all levels of automated driving systems. By designing intelligent planning modules, unmanned vehicles can complete some dangerous tasks that do not require a driver. In this challenge, we simulated a dangerous interception scene in which a vehicle carrying dangerous goods was driving on the road. Your goal is to submit a planning program to identify the dangerous vehicle on the road and eliminate the threat by hitting it. If it fails to hit the target vehicle or hits the wrong obstacle within the specified time, it will be regarded as a challenge failure. Please note that the escape route (green line in the following image) of the target vehicle will not be provided, and it may not be the same in different executions.Team task: Design and submit a planning program that can automatically plan the path of travel according to the location of the target vehicle to prevent the vehicle from escaping.

题目附件

task_data_0.zip
2.3KB

解题思路

planning.py
5.8KB