(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2024 年 11 月 28 日 (28.11.2024)

WIPO | PCT

(10) 国际公布号
WO 2024/239605 A1

(51) 国际专利分类号:
G06V 10/80 (2022.01) *G06V 20/56* (2022.01)

(21) 国际申请号: PCT/CN2023/137634

(22) 国际申请日: 2023 年 12 月 8 日 (08.12.2023)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
202310584658.0 2023年5月23日 (23.05.2023) CN

(71) 申请人: 深 圳 先 进 技 术 研 究 院 (**SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY**) [CN/CN]; 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。

(72) 发明人:缪祖佳(**MIAO, Zujia**); 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。 邵翠萍(**SHAO, Cuiping**); 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。 李慧云(**LI, Huiyun**); 中国广东省深圳市南山区西丽大学城学苑大道1068号, Guangdong 518055 (CN)。

(74) 代理人: 北 京 中 巡 通 大 知 识 产 权 代 理 有 限 公 司 (**BEIJING ZHONG XUN TONG DA INTELLECTUAL PROPERTY AGENCY CO., LTD.**); 中国北京市西城区西直门外大街1号院2号楼7层7C1, Beijing 100044 (CN)。

(81) 指定国(除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ,

(54) **Title:** ATTACK DETECTION METHOD AND APPARATUS FOR AUTONOMOUS DRIVING SYSTEM, DEVICE, AND STORAGE MEDIUM

(54) 发明名称: 自动驾驶系统的攻击检测方法、装置、设备及存储介质

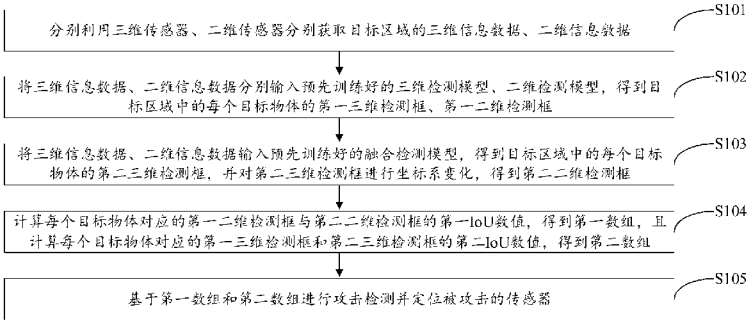


图 1

S101 Respectively acquire three-dimensional information data and two-dimensional information data of a target area by using a three-dimensional sensor and a two-dimensional sensor

S102 Respectively input the three-dimensional information data and the two-dimensional information data into a pre-trained three-dimensional detection model and two-dimensional detection model to obtain a first three-dimensional detection bounding box and a first two-dimensional detection bounding box of each target object in the target area

S103 Input the three-dimensional information data and the two-dimensional information data into a pre-trained fusion detection model to obtain a second three-dimensional detection bounding box of each target object in the target area, and perform coordinate system change on the second three-dimensional detection bounding box to obtain a second two-dimensional detection bounding box

S104 Calculate a first IoU value of the first two-dimensional detection bounding box and the second two-dimensional detection bounding box corresponding to each target object to obtain a first array, and calculate a second IoU value of the first three-dimensional detection bounding box and the second three-dimensional detection bounding box corresponding to each target object to obtain a second array

S105 Perform attack detection on the basis of the first array and the second array and locate an attacked sensor

(57) **Abstract:** Disclosed in the present invention are an attack detection method and apparatus for an autonomous driving system, a device, and a storage medium. The method comprises: respectively performing target detection on three-dimensional information data and two-dimensional information data acquired by a three-dimensional sensor and a two-dimensional sensor to obtain a first three-dimensional detection bounding box and a first two-dimensional detection bounding box; performing fusion target detection on the three-dimensional information data and the two-dimensional information data to obtain a second three-dimensional detection bounding box, and performing coordinate transformation on the second three-dimensional detection bounding box to obtain a second

WO 2024/239605 A1

[见续页]

LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW。

(84) 指定国(除另有指明，要求每一种可提供的地区保护): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

two-dimensional detection bounding box; then performing IoU value calculation on the first two-dimensional detection bounding box and the second two-dimensional detection bounding box corresponding to each object to obtain a first array, and performing IoU value calculation on the first three-dimensional detection bounding box and the second three-dimensional detection bounding box corresponding to each object to obtain a second array; and analyzing the first array and the second array to confirm whether a sensor is attacked. The present invention can perform attack detection on the basis of multi-modal data and can locate an attacked sensor.

(57) 摘要: 本发明公开了一种自动驾驶系统的攻击检测方法、装置、设备及存储介质，其中方法包括分别对三维传感器、二维传感器获取的三维信息数据、二维信息数据进行目标检测，得到第一三维检测框、第一二维检测框，且对三维信息数据、二维信息数据进行融合目标检测，得到第二三维检测框，并对第二三维检测框进行坐标变换，得到第二二维检测框，再对每个物体对应的第一二维检测框和第二二维检测框进行IoU数值计算，得到第一数组，对每个物体对应的第一三维检测框和第二三维检测框进行IoU数值计算，得到第二数组，分析第一数组和和第二数组确认是否传感器是否被攻击。本发明能够基于多模态的数据进行攻击检测并能够定位到被攻击的传感器。

自动驾驶系统的攻击检测方法、装置、设备及存储介质

技术领域

本申请涉及传感器检测技术领域，特别是涉及一种自动驾驶系统的攻击检测方法、装置、设备及存储介质。

背景技术

无人驾驶技术是一个涉及人工智能、传感技术、地图技术以及计算机等诸多前沿科技的综合技术。无人驾驶技术的功能实现依赖于车载定位传感器系统。定位传感器系统主要由激光雷达、视觉摄像头、毫米波雷达、全球定位系统(GPS)等设备组成。定位传感器系统为无人驾驶汽车的规划与决策模块提供丰富的定位数据，即车辆速度、姿态和位置等信息。自动驾驶汽车路线规划与决策控制的安全性以定位传感器系统的安全为前提，如果自动驾驶汽车的定位传感器系统出现异常，将会导致传感器获取到错误的定位信息，进而规划错误的驾驶控制策略，对其他车辆安全及驾驶员、行人生命造成威胁。

目前，无人驾驶技术的传感器攻击检测的方式主要是与具体的单传感器目标检测算法结合，并在此基础上进行攻击检测，但是，该种方式不具有普适性，例如，以激光雷达为主的目标检测算法搭配的攻击检测方法不能适用于以摄像头为主的目标检测算法的攻击检测场景，并且针对单一类型传感器的检测方式的攻击检测结果准确性不高。

发明内容

有鉴于此，本申请提供一种自动驾驶系统的攻击检测方法、装置、设备及存储介质，以解决现有自动驾驶系统攻击检测方式不具备普适性且准确性不高的问题。

为解决上述技术问题，本申请采用的一个技术方案是：提供一种自动驾驶系统的攻击检测方法，其包括：分别利用三维传感器、二维传感器分别获取目标区域的三维信息数据、二维信息数据；将三维信息数据、二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到目标区域中的每个目标物体的第一三维检测框、第一二维检测框；将三维信息数据、二维信息数据输入预先训练好的融合检测模型，得到目标区域中的每个目标物体的第二三维检测框，并对第二三维检测框进行坐标系变化，得到第二二维检测框；计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组；基于第一数组和第二数组进行攻击检测并定位被攻击的传感器。

作为本申请的进一步改进，将三维信息数据、二维信息数据输入预先训练好的融合检测模型之前，还包括：将上一时刻的二维信息数据和当前时刻的二维信息数据进行卡方比较，得到卡方比较数值；判断卡方比较数值是否超过预设阈值；当卡方比较数值超过预设阈值时，将当前时刻的二维信息数据与上一时刻的二维信息数据进行直方图匹配，得到当前时刻的增强二维信息数据，并替换掉当前时刻的二维信息数据；当卡方比较数值未超过预设阈值时，维持当前时刻的二维信息数据。

作为本申请的进一步改进，对第二三维检测框进行坐标系变化，得到第二二维检测框，包括：获取第二三维检测框的三维中心点坐标；利用三维中心点坐标确认第二三维检测框上与三维中心点在同一平面的

四个点的齐次坐标；利用预先获取的相机投影矩阵、相机旋转矩阵、传感器到相机坐标系的旋转矩阵和齐次坐标计算得到四个二维坐标点；利用四个二维坐标点构建第二二维检测框。

作为本申请的进一步改进，计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，包括：确认每个目标物体对应的目标第一二维检测框和目标第二二维检测框；分别计算目标第一二维检测框、目标第二二维检测框的第一面积、第二面积，以及目标第一二维检测框与目标第二二维检测框的重叠区域的第三面积；利用第一面积、第二面积、第三面积计算得到每个目标物体对应的第一 IoU 数值；利用所有目标物体对应的第一 IoU 数值构建第一数组。

作为本申请的进一步改进，计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组，包括：确认每个目标物体对应的目标第一三维检测框和目标第二三维检测框；分别计算目标第一三维检测框、目标第二三维检测框的第一体积、第二体积；计算目标第一三维检测框与目标第二三维检测框的重叠区域的底面面积；确认目标第一三维检测框与目标第二三维检测框的重叠区域的高度；利用底面面积和高度计算得到重叠区域的第三体积；利用第一体积、第二体积、第三体积计算得到每个目标物体对应的第二 IoU 数值；利用所有目标物体对应的第二 IoU 数值构建第二数组。

作为本申请的进一步改进，基于第一数组和第二数组进行攻击检测并定位被攻击的传感器，包括：分别判断第一数组、第二数组是否存在离群值；当第一数组存在离群值、第二数组不存在离群值时，确认三维传感器被攻击；当第一数组不存在离群值、第二数组存在离群值时，确认二维传感器被攻击；当第一数组、第二数组均存在离群值时，确认三维传感器和/或二维传感器被攻击；当第一数组、第二数组均不存在离群

值时，确认三维传感器和二维传感器未受到攻击。

作为本申请的进一步改进，三维传感器包括激光雷达，二维传感器包括摄像头，三维检测模型基于 PointPillar 算法构建，二维检测模型基于 YOLOv3 算法构建，融合检测模型基于 AVOD 算法构建。

为解决上述技术问题，本申请采用的又一个技术方案是：提供一种自动驾驶系统的攻击检测装置，其包括：获取模块，用于分别利用三维传感器、二维传感器分别获取目标区域的三维信息数据、二维信息数据；第一检测模块，用于将三维信息数据、二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到目标区域中的每个目标物体的第一三维检测框、第一二维检测框；第二检测模块，用于将三维信息数据、二维信息数据输入预先训练好的融合检测模型，得到目标区域中的每个目标物体的第二三维检测框，并对第二三维检测框进行坐标系变化，得到第二二维检测框；计算模块，用于计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组；分析模块，用于基于第一数组和第二数组进行攻击检测并定位被攻击的传感器。

为解决上述技术问题，本申请采用的再一个技术方案是：提供一种计算机设备，所述计算机设备包括处理器、与所述处理器耦接的存储器，所述存储器中存储有程序指令，所述程序指令被所述处理器执行时，使得所述处理器执行如上述任一项的自动驾驶系统的攻击检测方法的步骤。

为解决上述技术问题，本申请采用的再一个技术方案是：提供一种存储介质，存储有能够实现上述任一项的自动驾驶系统的攻击检测方法的程序指令。

本申请的有益效果是：本申请的自动驾驶系统的攻击检测方法通过分别对三维传感器、二维传感器获取的三维信息数据、二维信息数据进行目标检测，得到第一三维检测框、第一二维检测框，且对三维信息数据、二维信息数据进行融合目标检测，得到第二三维检测框，并对第二三维检测框进行坐标变换，得到第二二维检测框，再对每个物体对应的第一二维检测框和第二二维检测框进行 IoU 数值计算，得到第一数组，对每个物体对应的第一三维检测框和第二三维检测框进行IoU数值计算，得到第二数组，分析第一数组和和第二数组确认是否传感器是否被攻击，其利用三维传感器和二维传感器在时间和空间上的相关性进行攻击检测，从而提高攻击检测的准确性，并且利用作为自动驾驶汽车的基本配置的三维传感器和二维传感器即能够实现攻击检测，不再局限于利用其中一种传感器为主的目标检测算法进行攻击检测，具有更高的普适性。

附图说明

图 1 是本发明实施例的自动驾驶系统的攻击检测方法的一流程示意图；

图 2 是本发明实施例的第二三维检测框的示意图；

图 3 是本发明实施例的二维检测框重叠区域的示意图；

图 4 是本发明实施例的自动驾驶系统的攻击检测装置的功能模块示意图；

图 5 是本发明实施例的计算机设备的结构示意图；

图 6 是本发明实施例的存储介质的结构示意图。

具体实施方式

下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例仅是本申请的一部分实

施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

本申请中的术语“第一”、“第二”、“第三”仅用于描述目的，而不能理解为指示或暗示相对重要性或者隐含指明所指示的技术特征的数量。由此，限定有“第一”、“第二”、“第三”的特征可以明示或者隐含地包括至少一个该特征。本申请的描述中，“多个”的含义是至少两个，例如两个，三个等，除非另有明确具体的限定。本申请实施例中所有方向性指示（诸如上、下、左、右、前、后……）仅用于解释在某一特定姿态（如附图所示）下各部件之间的相对位置关系、运动情况等，如果该特定姿态发生改变时，则该方向性指示也相应地随之改变。此外，术语“包括”和“具有”以及它们任何变形，意图在于覆盖不排他的包含。例如包含了一系列步骤或单元的过程、方法、系统、产品或设备没有限定于已列出的步骤或单元，而是可选地还包括没有列出的步骤或单元，或可选地还包括对于这些过程、方法、产品或设备固有的其它步骤或单元。

在本文中提及“实施例”意味着，结合实施例描述的特定特征、结构或特性可以包含在本申请的至少一个实施例中。在说明书中的各个位置出现该短语并不一定均是指相同的实施例，也不是与其它实施例互斥的独立的或备选的实施例。本领域技术人员显式地和隐式地理解的是，本文所描述的实施例可以与其它实施例相结合。

图 1 是本发明实施例的自动驾驶系统的攻击检测方法的流程示意图。需注意的是，若有实质上相同的结果，本发明的方法并不以图 1 所示的流程顺序为限。如图 1 所示，该自动驾驶系统的攻击检测方法包括步骤：

步骤 S101：分别利用三维传感器、二维传感器分别获取目标区域的三维信息数据、二维信息数据。

本实施例中，三维传感器优选为激光雷达，需要说明的是，本发明实施例的三维传感器不局限于激光雷达，其他可用于获取三维信息数据的传感器设备同样包括在本发明的保护范围之内。二维传感器优选为摄像头，需要说明的是，本发明实施例的二维传感器不局限于摄像头，其他可用于获取二维信息数据的传感器设备同样包括在本发明的保护范围之内。

具体地，本实施例在使用自动驾驶系统驾驶车辆时，利用车辆上配备的三维传感器和二维传感器同时采集目标区域的三维信息数据和二维信息数据。需要说明的是，在进行攻击检测时，其检测范围局限在一个目标区域内，该目标区域为三维传感器和二维传感器视野交叠的部分，例如，对于激光雷达和摄像头而言，该交叠区域为激光雷达的FOV（Field of view, FOV）视域，通过将摄像头拍摄的图像尺寸投影到激光雷达的视觉区域之内，从而获取激光雷达采集的三维信息数据和摄像头采集的二维信息数据。

步骤S102：将三维信息数据、二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到目标区域中的每个目标物体的第一三维检测框、第一二维检测框。

其中，该三维检测模型基于PointPillar算法构建。具体地，三维传感器使用PointPillars（3D Object Proposal Generation and Detection from Point Cloud）算法进行三维目标检测得到第一三维目标检测框，输入数据为三维传感器的原始数据点云数据即三维信息数据，格式为$[x, y, z, intensity]$。三维传感器的原始特征为点云集合，可表示为矢量$Lidar = [X,\ Y,\ Z,\ intensity] \epsilon \mathbb{R}^{64\times1800}$，（64线激光雷达，每线扫描一周1800个点云）其中X表示点云在水平面的横坐标，Y表示点云在水平面的纵坐标，Z表示点云的高度，$intensity$表示点云的反射强度。使用

two-stage 方式，利用 PointNet++作为主干网络，先完成 segmentation 任务，判断每个三维点的 label，对分为前景的每个点，使用 feature 生成框。然后对框进行优化。目标物体检测结果用向量$\vec{V}_{lidar}=[X_{lidar},Y_{lidar},Z_{lidar},L,W,H]^T$表示。其中$x_{lidar}=[X_vY_vZ_v]^T$表示目标物体在三维传感器坐标系上的中心点值，$[L,W,H]^T$表示第一三维检测框的长宽高。

其中，该二维检测模型基于 YOLOv3 算法构建。具体地，使用 YOLOv3 算法对二维传感器获取的二维信息数据进行二维目标检测得到目标中心点。例如，以摄像头为例，将采集到的图片以 RGB 格式输入二维检测模型，二维检测模型调用深度卷积神经网络算法对 RGB 图像进行特征提取，神经网络算法中常见的结构有卷积层，池化层，激活层，dropout 层，BN(batch normalization)层，全连接层等，最终从图片中提取的特征能有效描述目标物体的信息。输入的数据格式为摄像头的 RGB 图像，输出的为图像坐标系上的中心点坐标及检测框宽（width）和高(height)，格式为$\vec{V}_{camera}=[X_{camera},Y_{camera},w,h]^T$，其中$X_{camera}$表示图像坐标系上 x 方向的数值，$Y_{camera}$表示 y 方向数值，w 表示第一二维检测框的宽度，h 表示第一二维检测框的高度。得到第一二维检测框后可以进一步得到第一二维检测框四个点的坐标分别如下所示：

$$\vec{V}_{camera,\ 1}=\left[X_{camera,\ 1'},Y_{camera,\ 1'}\right]^T;$$

$$\vec{V}_{camera,\ 2}=\left[X_{camera,\ 2'},Y_{camera,\ 2'}\right]^T;$$

$$\vec{V}_{camera,\ 3}=\left[X_{camera,\ 3'},Y_{camera,\ 3'}\right]^T;$$

$$\vec{V}_{camera,\ 4}=\left[X_{camera,\ 4'},Y_{camera,\ 4'}\right]^T;$$

$$X_{camera,\ 1'}=X_{camera,\ 3'}=X_{camera}-w/2;$$

$$X_{camera,\ 2'} = X_{camera,\ 4'} = X_{camera} + w/2;$$

$$Y_{camera,\ 1'} = Y_{camera,\ 2'} = Y_{camera} + h/2;$$

$$Y_{camera,\ 3'} = Y_{camera,\ 4'} = Y_{camera} - h/2;$$

其中$X_{camera,\ i'}, i = 1, 2, 3, 4$分别表示第一二维检测框左上角，右上角，左下角，右下角的图片坐标系的 x 方向的坐标值。$Y_{camera,\ i'}, i = 1, 2, 3, 4$分别表示第一二维检测框左上角，右上角，左下角，右下角的图片坐标系的 y 方向的坐标值。

步骤 S103：将三维信息数据、二维信息数据输入预先训练好的融合检测模型，得到目标区域中的每个目标物体的第二三维检测框，并对第二三维检测框进行坐标系变化，得到第二二维检测框。

具体地，该融合检测模型基于 AVOD 算法（Joint 3D Proposal Generation and Object Detection from ViewAggregation）构建，在得到三维信息数据和二维信息数据后，将三维信息数据和二维信息数据输入至 AVOD 算法进行目标检测，得到第二三维检测框。AVOD 算法融合了三维信息数据和二维信息数据，当三维信息数据为激光雷达获取的点云数据信息时，AVOD 算法只使用了点云的俯视图和前视图，这样既能减少计算量，又不至于丧失过多的信息。随后生成三维候选区域，把特征和候选区域融合后输出最终的第二三维检测框。

进一步的，为了提高二维传感器的防御能力，在一些实施例中，步骤 S103 之前还包括：

1、将上一时刻的二维信息数据和当前时刻的二维信息数据进行卡方比较，得到卡方比较数值。

2、判断卡方比较数值是否超过预设阈值。

3、当卡方比较数值超过预设阈值时，将当前时刻的二维信息数据

与上一时刻的二维信息数据进行直方图匹配，得到当前时刻的增强二维信息数据，并替换掉当前时刻的二维信息数据。

4、当卡方比较数值未超过预设阈值时，维持当前时刻的二维信息数据。

本实施例中，图像增强的目的是为了提高融合检测模型对二维传感器攻击的防御能力。通过将上一时刻的二维信息数据和当前时刻的二维信息数据进行卡方比较，得到卡方比较数值，再判断卡方比较数值是否超过预设阈值。当卡方比较数值超过预设阈值时，将当前时刻的二维信息数据与上一时刻的二维信息数据进行直方图匹配，得到当前时刻的增强二维信息数据，并替换掉当前时刻的二维信息数据。当卡方比较数值未超过预设阈值时，维持当前时刻的二维信息数据。

进一步的，步骤 S103 中对第二三维检测框进行坐标系变化，得到第二二维检测框的步骤，具体包括：

1、获取第二三维检测框的三维中心点坐标。

2、利用三维中心点坐标确认第二三维检测框上与三维中心点在同一平面的四个点的齐次坐标。

3、利用预先获取的相机投影矩阵、相机旋转矩阵、传感器到相机坐标系的旋转矩阵和齐次坐标计算得到四个二维坐标点。

4、利用四个二维坐标点构建第二二维检测框。

具体地，本实施例中，使用 4 个角点（只包含 x 坐标,y 坐标）和 2 个高度来描述一个第二三维检测框，如图 2 所示，第二三维检测框以向量 $\vec{V}_{3d融合检测} = [c_1, c_2, c_3, c_4, h_1, h_2]^T$ 表示，其中 $c_i = [x_{ci} y_{ci}]^T$，$i = 1, 2, 3, 4$表示第二三维检测框 4 个顶点的 x、y 方向的坐标，h_1表示第二三维检测框底面距离三维坐标系中 x 轴与 y 轴构成的平面的高度，h_2表示第二三维检测框顶面距离三维坐标系中 x 轴与 y 轴构成的平

面的高度。

具体地，在得到第二三维检测框后，将第二三维检测框投影至图像坐标系，得到第二二维检测框。请一并参阅图 2，首先将第二三维检测框的向量形式转换为常规的三维检测框格式$Y_{3D融合检测} = [X_v Y_v Z_v]^T$，其中：

$$Z_v = (h_2 - h_1)/2;$$

$$X_v = x_{c1} - x_{c2};$$

$$Y_v = y_{c1} - y_{c2};$$

其中，x_{ci}表示c_i点的 x 轴坐标，y_{ci}表示c_i点的 y 轴坐标，$i = 1, 2, 3, 4$，$[X_v Y_v Z_v]^T$表示第二三维检测框中心点的坐标。

然后，对第二三维检测框中心点附近的四个点（图 2 中 A、B、C、D 四个点）依次进行坐标系的转换，得到四个在图像坐标系的点，具体转换过程如下：

$$Y_{点A齐次坐标} = [X_{v,\ 1}, Y_{v,\ 1}, Z_{v,1}]^T = [X_v - (x_{c2} - x_{c1})/2, Y_v, h2];$$

$$Y_{点B齐次坐标} = [X_{v,\ 2}, Y_{v,\ 2}, Z_{v,2}]^T = [X_v + (x_{c2} - x_{c1})/2, Y_v, h2];$$

$$Y_{点C齐次坐标} = [X_{v,\ 3}, Y_{v,\ 3}, Z_{v,3}]^T = [X_v - (x_{c2} - x_{c1})/2, Y_v, h1];$$

$$Y_{点D齐次坐标} = [X_{v,\ 4}, Y_{v,\ 4}, Z_{v,4}]^T = [X_v + (x_{c2} - x_{c1})/2, Y_v, h1];$$

$$Y = P * R * Tr_v elo_t o_c am * Y_{点n齐次坐标},\ n = \text{A},\ \text{B},\ \text{C},\ \text{D};$$

其中，Y表示第二二维检测框的坐标，$Y_{点n齐次坐标}$表示目标物体的齐次向量，P为相机投影矩阵，R为相机旋转矩阵，$Tr_v elo_t o_c am$为 3x4 的三维坐标系到相机坐标系的旋转矩阵。

步骤 S104: 计算每个目标物体对应的第一二维检测框与第二二维检

测框的第一 IoU 数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组。

具体地，IoU 数值可以用于表征两组检测框之间的不一致性。利用第一二维检测框和第二二维检测框进行 IoU 数值计算，得到表征第一二维检测框和第二二维检测框不一致性的第一 IoU 数值，多个目标物体则对应有多个第一 IoU 数值，将其构建为第一数组。利用第一三维检测框和第二三维检测框进行 IoU 数值计算，得到表征第一三维检测框和第二三维检测框不一致性的第二 IoU 数值，多个目标物体则对应有多个第二 IoU 数值，将其构建为第二数组。需要说明的是，两组检测框均对应的同一目标区域，该目标区域的目标物体是恒定的，因此，第一数组和第二数组中元素个数相等，每个目标物体在第一数组或第二数组中均存在对应的元素。

进一步的，步骤 S104 中计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组的步骤，具体包括：

1、确认每个目标物体对应的目标第一二维检测框和目标第二二维检测框。

具体地，由于场景中往往存在多个目标物体，会有多个检测框，因此，在确认每个目标物体对应的目标第一二维检测框和目标第二二维检测框时，先选取一个第一二维检测框作为目标第一二维检测框，再计算该目标第一二维检测框的中心点与每个第二二维检测框的中心点的欧式距离，选取欧式距离最小的第二二维检测框作为目标第二二维检测框。

2、分别计算目标第一二维检测框、目标第二二维检测框的第一面积、第二面积，以及目标第一二维检测框与目标第二二维检测框的重叠区域的第三面积。

具体地，通过获取二维检测框四个顶点的坐标，通过四个顶点的坐标计算得到目标第一二维检测框和目标第二二维检测框的第一面积和第二面积。计算公式如下：

$$S_A = |x_{a2} - x_{a1}| \times |y_{a2} - y_{a1}|;$$

$$S_B = |x_{b2} - x_{b1}| \times |y_{b2} - y_{b1}|;$$

其中，S_A表示第一面积，A1(x_{a1}, y_{a1})、B1(x_{a1}, y_{a2})、C1(x_{a2}, y_{a1})、D1(x_{a2}, y_{a2})表示目标第一二维检测框四个顶点的坐标。S_B表示第二面积，A2（x_{b1}, y_{b1}）、B2（x_{b1}, y_{b2}）、C2（x_{b2}, y_{b1}）、D2（x_{b2}, y_{b2}）表示目标第二二维检测框四个顶点的坐标。

以图 3 所示为例进行说明，两个检测框存在重叠区域时，该重叠区域同样为一个矩形框，该矩形框的四个顶点可根据重叠的目标第一二维检测框和目标第二二维检测框的四个顶点坐标得到，其左上角坐标为A2(x_{b1}, y_{b1})，左下角坐标为 E(x_{b1}, y_{a2})，右上角坐标为 F(x_{a2}, y_{b1})，右下角坐标为 D1（x_{a2}, y_{a2}）。再利用重叠区域的四个顶点坐标计算得到重叠区域的第三面积。

3、利用第一面积、第二面积、第三面积计算得到每个目标物体对应的第一 IoU 数值。

具体地，第一IoU数值=第三面积/(第一面积+第二面积−第三面积)。

4、利用所有目标物体对应的第一 IoU 数值构建第一数组。

具体地，第一数组表示为：$I = [i_1, i_2, \ldots, i_n]$，$n$为第一 IoU 数值的个数。

进一步的，步骤 S104 中计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组的步骤，具体包括：

1、确认每个目标物体对应的目标第一三维检测框和目标第二三维检测框。

具体地，目标第一三维检测框和目标第二三维检测框同样利用第一三维检测框和第二三维检测框的中心点坐标之间的欧式距离确认。

2、分别计算目标第一三维检测框、目标第二三维检测框的第一体积、第二体积。

具体地，根据三维检测框的 8 个顶点的坐标即可确认三维检测框的长宽高，利用长宽高计算得到三维检测框的体积。

3、计算目标第一三维检测框与目标第二三维检测框的重叠区域的底面面积。

4、确认目标第一三维检测框与目标第二三维检测框的重叠区域的高度。

5、利用底面面积和高度计算得到重叠区域的第三体积。

需要理解的是，第一三维检测框和第二三维检测框的重叠区域同样为一方体结构，其体积可由底面积乘以高求得，而第一三维检测框和第二三维检测框对应的目标物体均处于地面上，即第一三维检测框和第二三维检测框的底面处于同一平面，因此第一三维检测框和第二三维检测框的重叠区域的底面的顶点坐标可根据第一三维检测框的底面的四个顶点坐标和第二三维检测框的四个顶点坐标确认，再根据重叠区域的底面的顶点坐标可求得重叠区域的底面积，该方式与二维检测框中求取重叠面积的方式相同，此处不再赘述。而对于重叠区域的高，因第一三维检测框和第二三维检测框对应的目标物体均处于地面上，即第一三维检测框和第二三维检测框的底面处于同一平面，因此，第一三维检测框和第二三维检测框重叠区域的高为第一三维检测框和第二三维检测框中较小的高度值。在得到第一三维检测框和第二三维检测框的重叠区域的底面积和高之后，即可计算得到该重叠区域的第三体积。

6、利用第一体积、第二体积、第三体积计算得到每个目标物体对

应的第二 IoU 数值。

具体地，第二 IoU 数值=第三体积/（第一体积+第二体积－第三体积）

7、利用所有目标物体对应的第二 IoU 数值构建第二数组。

具体地，第一数组表示为：$U=[u_1,u_2,\ldots,u_n]$，n为第二 IoU 数值的个数。

步骤 S105: 基于第一数组和第二数组进行攻击检测并定位被攻击的传感器。

具体地，在得到第一数组和第二数组后，对两个数组进行不一致性检测，从而确认是否传感器是否被攻击，并定位被攻击的三维传感器还是二维传感器。

进一步的，步骤 S105 具体包括：

1、分别判断第一数组、第二数组是否存在离群值。

2、当第一数组存在离群值、第二数组不存在离群值时，确认三维传感器被攻击。

3、当第一数组不存在离群值、第二数组存在离群值时，确认二维传感器被攻击。

4、当第一数组、第二数组均存在离群值时，确认三维传感器和/或二维传感器被攻击。

5、当第一数组、第二数组均不存在离群值时，确认三维传感器和二维传感器未受到攻击。

本发明实施例的自动驾驶系统的攻击检测方法通过分别对三维传感器、二维传感器获取的三维信息数据、二维信息数据进行目标检测，得到第一三维检测框、第一二维检测框，且对三维信息数据、二维信息数据进行融合目标检测，得到第二三维检测框，并对第二三维检测框进行坐标变换，得到第二二维检测框，再对每个物体对应的第一二维检测

框和第二二维检测框进行 IoU 数值计算，得到第一数组，对每个物体对应的第一三维检测框和第二三维检测框进行 IoU 数值计算，得到第二数组，分析第一数组和和第二数组确认是否传感器是否被攻击，其利用三维传感器和二维传感器在时间和空间上的相关性进行攻击检测，从而提高攻击检测的准确性，并且利用作为自动驾驶汽车的基本配置的三维传感器和二维传感器即能够实现攻击检测，不再局限于利用其中一种传感器为主的目标检测算法进行攻击检测，具有更高的普适性。

图 4 是本发明实施例的自动驾驶系统的攻击检测装置的功能模块示意图。如图 4 所示，该自动驾驶系统的攻击检测装置 20 包括获取模块 21、第一检测模块 22、第二检测模块 23、计算模块 24 和分析模块 25。

获取模块 21，用于分别利用三维传感器、二维传感器分别获取目标区域的三维信息数据、二维信息数据；

第一检测模块 22，用于将三维信息数据、二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到目标区域中的每个目标物体的第一三维检测框、第一二维检测框；

第二检测模块 23，用于将三维信息数据、二维信息数据输入预先训练好的融合检测模型，得到目标区域中的每个目标物体的第二三维检测框，并对第二三维检测框进行坐标系变化，得到第二二维检测框；

计算模块 24，用于计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组；

分析模块 25，用于基于第一数组和第二数组进行攻击检测并定位被攻击的传感器。

可选地，第二检测模块 23 执行将三维信息数据、二维信息数据输入预先训练好的融合检测模型的操作之前，还用于：将上一时刻的二维

信息数据和当前时刻的二维信息数据进行卡方比较，得到卡方比较数值；判断卡方比较数值是否超过预设阈值；当卡方比较数值超过预设阈值时，将当前时刻的二维信息数据与上一时刻的二维信息数据进行直方图匹配，得到当前时刻的增强二维信息数据，并替换掉当前时刻的二维信息数据；当卡方比较数值未超过预设阈值时，维持当前时刻的二维信息数据。

可选地，第二检测模块 23 执行对第二三维检测框进行坐标系变化，得到第二二维检测框的操作，具体包括：获取第二三维检测框的三维中心点坐标；利用三维中心点坐标确认第二三维检测框上与三维中心点在同一平面的四个点的齐次坐标；利用预先获取的相机投影矩阵、相机旋转矩阵、传感器到相机坐标系的旋转矩阵和齐次坐标计算得到四个二维坐标点；利用四个二维坐标点构建第二二维检测框。

可选地，计算模块 24 执行计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组的操作，具体包括：确认每个目标物体对应的目标第一二维检测框和目标第二二维检测框；分别计算目标第一二维检测框、目标第二二维检测框的第一面积、第二面积，以及目标第一二维检测框与目标第二二维检测框的重叠区域的第三面积；利用第一面积、第二面积、第三面积计算得到每个目标物体对应的第一 IoU 数值；利用所有目标物体对应的第一 IoU 数值构建第一数组。

可选地，计算模块 24 执行计算每个目标物体对应的第一三维检测框和第二三维检测框的第二 IoU 数值，得到第二数组的操作，具体包括：确认每个目标物体对应的目标第一三维检测框和目标第二三维检测框；分别计算目标第一三维检测框、目标第二三维检测框的第一体积、第二体积；计算目标第一三维检测框与目标第二三维检测框的重叠区域的底

面面积；确认目标第一三维检测框与目标第二三维检测框的重叠区域的高度；利用底面面积和高度计算得到重叠区域的第三体积；利用第一体积、第二体积、第三体积计算得到每个目标物体对应的第二 IoU 数值；利用所有目标物体对应的第二 IoU 数值构建第二数组。

可选地，分析模块 25 执行基于第一数组和第二数组进行攻击检测并定位被攻击的传感器的操作，具体包括：分别判断第一数组、第二数组是否存在离群值；当第一数组存在离群值、第二数组不存在离群值时，确认三维传感器被攻击；当第一数组不存在离群值、第二数组存在离群值时，确认二维传感器被攻击；当第一数组、第二数组均存在离群值时，确认三维传感器和/或二维传感器被攻击；当第一数组、第二数组均不存在离群值时，确认三维传感器和二维传感器未受到攻击。

可选地，三维传感器包括激光雷达，二维传感器包括摄像头，三维检测模型基于 PointPillar 算法构建，二维检测模型基于 YOLOv3 算法构建，融合检测模型基于 AVOD 算法构建。

关于上述实施例自动驾驶系统的攻击检测装置中各模块实现技术方案的其他细节，可参见上述实施例中的自动驾驶系统的攻击检测方法中的描述，此处不再赘述。

需要说明的是，本说明书中的各个实施例均采用递进的方式描述，每个实施例重点说明的都是与其他实施例的不同之处，各个实施例之间相同相似的部分互相参见即可。对于装置类实施例而言，由于其与方法实施例基本相似，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

请参阅图 5，图 5 为本发明实施例的计算机设备的结构示意图。如图 5 所示，该计算机设备 30 包括处理器 31 及和处理器 31 耦接的存储器 32，存储器 32 中存储有程序指令，程序指令被处理器 31 执行时，使

得处理器 31 执行上述任一实施例所述的自动驾驶系统的攻击检测方法步骤。

其中，处理器 31 还可以称为 CPU（Central Processing Unit，中央处理单元）。处理器 31 可能是一种集成电路芯片，具有信号的处理能力。处理器 31 还可以是通用处理器、数字信号处理器（DSP）、专用集成电路（ASIC）、现场可编程门阵列（FPGA）或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件。通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

参阅图 6，图 6 为本发明实施例的存储介质的结构示意图。本发明实施例的存储介质存储有能够实现上述自动驾驶系统的攻击检测方法的程序指令 41，其中，该程序指令 41 可以以软件产品的形式存储在上述存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）或处理器（processor）执行本申请各个实施方式所述方法的全部或部分步骤。而前述的存储介质包括:U 盘、移动硬盘、只读存储器（ROM，Read-Only Memory）、随机存取存储器（RAM，Random Access Memory）、磁碟或者光盘等各种可以存储程序代码的介质，或者是计算机、服务器、手机、平板等计算机设备。

在本申请所提供的几个实施例中，应该理解到，所揭露的计算机设备，装置和方法，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

另外，在本发明各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理存在，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用软件功能单元的形式实现。以上仅为本申请的实施方式，并非因此限制本申请的专利范围，凡是利用本申请说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本申请的专利保护范围内。

权利要求书

1、一种自动驾驶系统的攻击检测方法，其特征在于，其包括：

分别利用三维传感器、二维传感器分别获取所述目标区域的三维信息数据、二维信息数据；

将所述三维信息数据、所述二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到所述目标区域中的每个目标物体的第一三维检测框、第一二维检测框；

将所述三维信息数据、所述二维信息数据输入预先训练好的融合检测模型，得到所述目标区域中的每个目标物体的第二三维检测框，并对所述第二三维检测框进行坐标系变化，得到第二二维检测框；

计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和所述第二三维检测框的第二 IoU 数值，得到第二数组；

基于所述第一数组和所述第二数组进行攻击检测并定位被攻击的传感器。

2、根据权利要求 1 所述的自动驾驶系统的攻击检测方法，其特征在于，所述将所述三维信息数据、所述二维信息数据输入预先训练好的融合检测模型之前，还包括：

将上一时刻的二维信息数据和当前时刻的二维信息数据进行卡方比较，得到卡方比较数值；

判断所述卡方比较数值是否超过预设阈值；

当所述卡方比较数值超过预设阈值时，将当前时刻的二维信息数据与上一时刻的二维信息数据进行直方图匹配，得到当前时刻的增强二维信息数据，并替换掉当前时刻的二维信息数据；

当所述卡方比较数值未超过预设阈值时，维持当前时刻的二维信息数据。

3、根据权利要求 1 所述的自动驾驶系统的攻击检测方法，其特征在于，所述对所述第二三维检测框进行坐标系变化，得到第二二维检测框，包括：

获取所述第二三维检测框的三维中心点坐标；

利用所述三维中心点坐标确认所述第二三维检测框上与所述三维中心点在同一平面的四个点的齐次坐标；

利用预先获取的相机投影矩阵、相机旋转矩阵、传感器到相机坐标系的旋转矩阵和所述齐次坐标计算得到四个二维坐标点；

利用所述四个二维坐标点构建所述第二二维检测框。

4、根据权利要求 1 所述的自动驾驶系统的攻击检测方法，其特征在于，所述计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，包括：

确认每个目标物体对应的目标第一二维检测框和目标第二二维检测框；

分别计算所述目标第一二维检测框、所述目标第二二维检测框的第一面积、第二面积，以及所述目标第一二维检测框与所述目标第二二维检测框的重叠区域的第三面积；

利用所述第一面积、所述第二面积、所述第三面积计算得到每个目标物体对应的第一 IoU 数值；

利用所有目标物体对应的第一 IoU 数值构建所述第一数组。

5、根据权利要求 1 所述的自动驾驶系统的攻击检测方法，其特征在于，所述计算每个目标物体对应的第一三维检测框和所述第二三维检测框的第二 IoU 数值，得到第二数组，包括：

确认每个目标物体对应的目标第一三维检测框和目标第二三维检测框；

分别计算所述目标第一三维检测框、所述目标第二三维检测框的第一体积、第二体积；

计算所述目标第一三维检测框与所述目标第二三维检测框的重叠区域的底面面积；

确认所述目标第一三维检测框与所述目标第二三维检测框的重叠区域的高度；

利用所述底面面积和所述高度计算得到重叠区域的第三体积；

利用所述第一体积、所述第二体积、所述第三体积计算得到每个目标物体对应的第二 IoU 数值；

利用所有目标物体对应的第二 IoU 数值构建所述第二数组。

6、根据权利要求 1 所述的自动驾驶系统的攻击检测方法，其特征在于，所述基于所述第一数组和所述第二数组进行攻击检测并定位被攻击的传感器，包括：

分别判断所述第一数组、所述第二数组是否存在离群值；

当所述第一数组存在离群值、所述第二数组不存在离群值时，确认所述三维传感器被攻击；

当所述第一数组不存在离群值、所述第二数组存在离群值时，确认所述二维传感器被攻击；

当所述第一数组、所述第二数组均存在离群值时，确认所述三维传感器和/或所述二维传感器被攻击；

当所述第一数组、所述第二数组均不存在离群值时，确认所述三维传感器和所述二维传感器未受到攻击。

7、根据权利要求 1 所述的自动驾驶系统的攻击检测方法，其特征

在于，所述三维传感器包括激光雷达，所述二维传感器包括摄像头，所述三维检测模型基于 PointPillar 算法构建，所述二维检测模型基于 YOLOv3 算法构建，所述融合检测模型基于 AVOD 算法构建。

8、一种自动驾驶系统的攻击检测装置，其特征在于，其包括：

获取模块，用于分别利用三维传感器、二维传感器分别获取所述目标区域的三维信息数据、二维信息数据；

第一检测模块，用于将所述三维信息数据、所述二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到所述目标区域中的每个目标物体的第一三维检测框、第一二维检测框；

第二检测模块，用于将所述三维信息数据、所述二维信息数据输入预先训练好的融合检测模型，得到所述目标区域中的每个目标物体的第二三维检测框，并对所述第二三维检测框进行坐标系变化，得到第二二维检测框；

计算模块，用于计算每个目标物体对应的第一二维检测框与第二二维检测框的第一 IoU 数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和所述第二三维检测框的第二 IoU 数值，得到第二数组；

分析模块，用于基于所述第一数组和所述第二数组进行攻击检测并定位被攻击的传感器。

9、一种计算机设备，其特征在于，所述计算机设备包括处理器、与所述处理器耦接的存储器，所述存储器中存储有程序指令，所述程序指令被所述处理器执行时，使得所述处理器执行如权利要求 1-7 中任一项权利要求所述的自动驾驶系统的攻击检测方法的步骤。

10、一种存储介质，其特征在于，存储有能够实现如权利要求 1-7 中任一项所述的自动驾驶系统的攻击检测方法的程序指令。

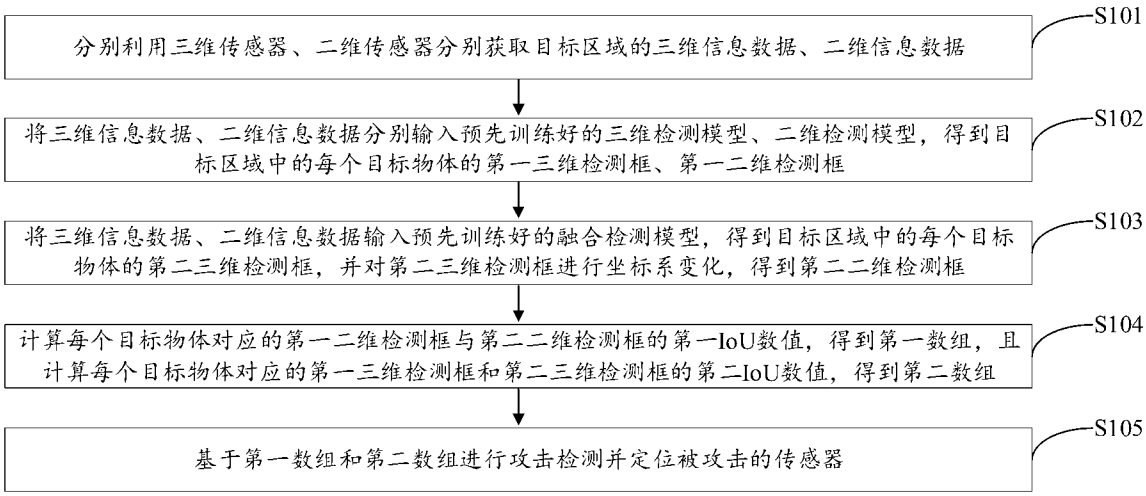

分别利用三维传感器、二维传感器分别获取目标区域的三维信息数据、二维信息数据
S101
将三维信息数据、二维信息数据分别输入预先训练好的三维检测模型、二维检测模型，得到目标区域中的每个目标物体的第一三维检测框、第一二维检测框
S102
将三维信息数据、二维信息数据输入预先训练好的融合检测模型，得到目标区域中的每个目标物体的第二三维检测框，并对第二三维检测框进行坐标系变化，得到第二二维检测框
S103
计算每个目标物体对应的第一二维检测框与第二二维检测框的第一IoU数值，得到第一数组，且计算每个目标物体对应的第一三维检测框和第二三维检测框的第二IoU数值，得到第二数组
S104
基于第一数组和第二数组进行攻击检测并定位被攻击的传感器
S105

图 1

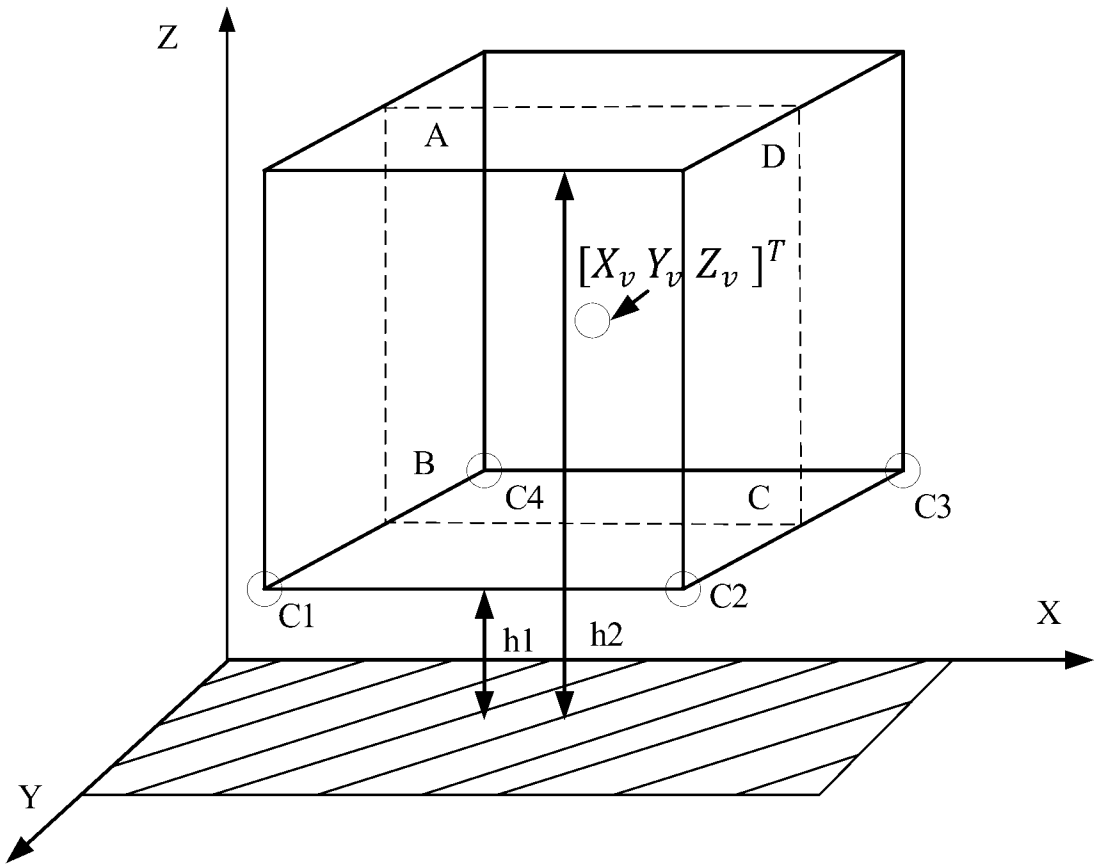

Z
A
D
$[X_v\ Y_v\ Z_v\ ]^T$
B
C4
C
C3
C1
C2
h1
h2
X
Y

图 2

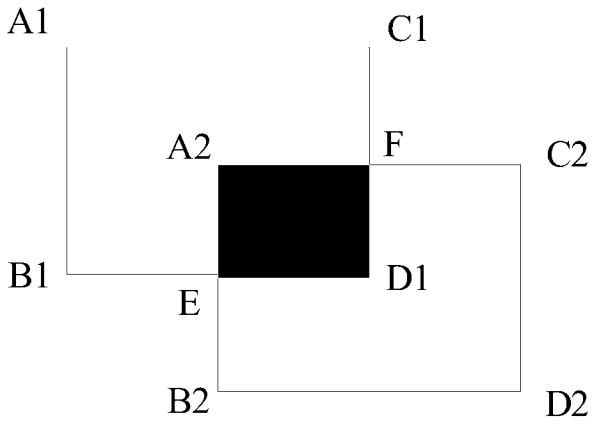

A1
C1
A2
F
C2
B1
D1
E
B2
D2

图 3

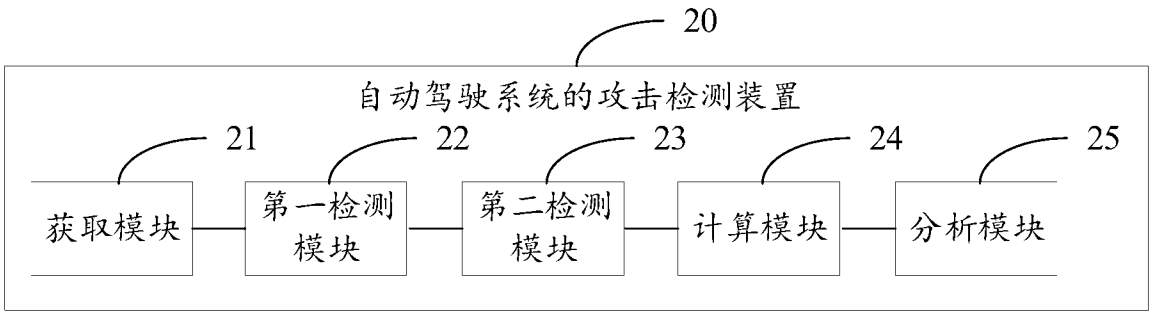

20
自动驾驶系统的攻击检测装置
21
22
23
24
25
获取模块
第一检测模块
第二检测模块
计算模块
分析模块

图 4

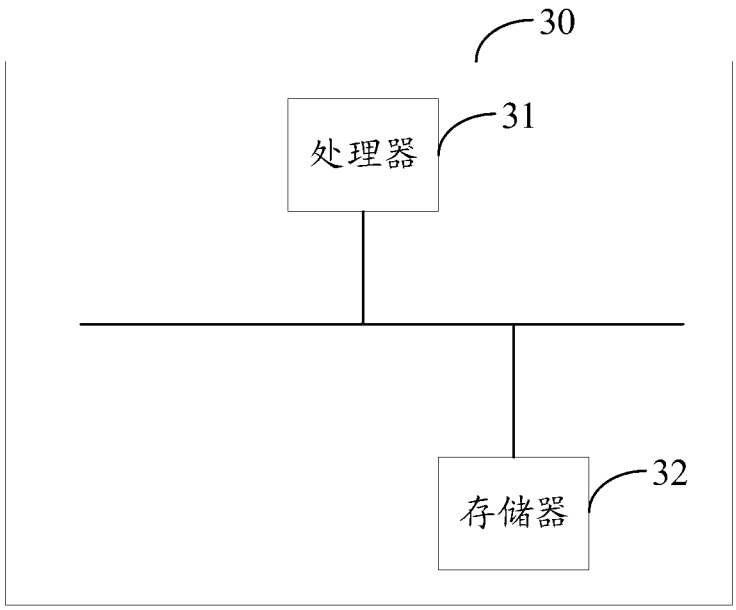


图 5

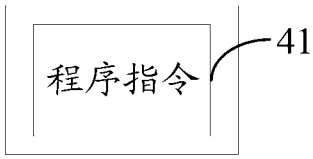


图 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/137634

A. CLASSIFICATION OF SUBJECT MATTER

G06V10/80(2022.01)i; G06V20/56(2022.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC:G06V

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNTXT; ENTXTC; ENTXT; DWPI; CNKI; IEEE: 二维, 三维, 目标, 检测, 可见光, 点云, 自动驾驶, 融合, 数组, 传感器, 攻击, automatic, driving, three, dimensional, two, sensor, fusion, array, IoU, attack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 116912788 A (SHENZHEN INSTITUTE OF ADVANCED TECHNOLOGY) 20 October 2023 (2023-10-20) claims 1-10	1-10
A	CN 114596358 A (SHENZHEN YIQING INNOVATION TECH CO., LTD.) 07 June 2022 (2022-06-07) description, pages 4-7,9	1-10
A	CN 111626217 A (NINGBO BODENG INTELLIGENT TECHNOLOGY CO., LTD.) 04 September 2020 (2020-09-04) entire document	1-10
A	CN 113111978 A (ZHEJIANG LAB) 13 July 2021 (2021-07-13) entire document	1-10
A	CN 114187579 A (ZHIDAO NETWORK TECHNOLOGY (BEIJING) CO., LTD.) 15 March 2022 (2022-03-15) entire document	1-10

☑ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 February 2024	**04 March 2024**

Name and mailing address of the ISA/CN	Authorized officer
China National Intellectual Property Administration (ISA/CN) **China No. 6, Xitucheng Road, Jimenqiao, Haidian District, Beijing 100088**	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2023/137634

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 115453589 A (SHENZHEN INSTITUTES OF ADVANCED TECHNOLOGY, CHINESE ACADEMY OF SCIENCES et al.) 09 December 2022 (2022-12-09) entire document	1-10
A	WO 2023277998 A2 (NEURAL PROPULSION SYSTEMS, INC.) 05 January 2023 (2023-01-05) entire document	1-10

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2023/137634

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
CN 116912788 A	20 October 2023	None	
CN 114596358 A	07 June 2022	None	
CN 111626217 A	04 September 2020	None	
CN 113111978 A	13 July 2021	None	
CN 114187579 A	15 March 2022	None	
CN 115453589 A	09 December 2022	None	
WO 2023277998 A2	05 January 2023	WO 2023277998 A3	13 April 2023

国际检索报告

国际申请号
PCT/CN2023/137634

A. 主题的分类

G06V10/80(2022.01)i；G06V20/56(2022.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

IPC:G06V

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用））

CNTXT;ENTXTC;ENTXT;DWPI;CNKI;IEEE:二维、三维、目标、检测、可见光、点云、自动驾驶、融合、数组、传感器、攻击、automatic、driving、three、dimensional、two、sensor、fusion、array、IoU、attack

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 116912788 A (深圳先进技术研究院) 2023年10月20日 (2023 - 10 - 20) 权利要求1−10	1−10
A	CN 114596358 A (深圳一清创新科技有限公司) 2022年6月7日 (2022 - 06 - 07) 说明书第4−7,9页	1−10
A	CN 111626217 A (宁波博登智能科技有限责任公司) 2020年9月4日 (2020 - 09 - 04) 全文	1−10
A	CN 113111978 A (之江实验室) 2021年7月13日 (2021 - 07 - 13) 全文	1−10
A	CN 114187579 A (智道网联科技（北京）有限公司) 2022年3月15日 (2022 - 03 - 15) 全文	1−10
A	CN 115453589 A (中国科学院深圳先进技术研究院等) 2022年12月9日 (2022 - 12 - 09) 全文	1−10
A	WO 2023277998 A2 (NEURAL PROPULSION SYSTEMS， INC.) 2023年1月5日 (2023 - 01 - 05) 全文	1−10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

“A” 认为不特别相关的表示了现有技术一般状态的文件

“D” 申请人在国际申请中引证的文件

“E” 在国际申请日的当天或之后公布的在先申请或专利

“L” 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

“O” 涉及口头公开、使用、展览或其他方式公开的文件

“P” 公布日先于国际申请日但迟于所要求的优先权日的文件

“T” 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

“X” 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

“Y” 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

“&” 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2024年2月22日	2024年3月4日
ISA/CN的名称和邮寄地址 中国国家知识产权局 中国北京市海淀区蓟门桥西土城路6号 100088	受权官员 吴倩 电话号码 (+86) 010−53961822

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2023/137634

检索报告引用的专利文件	公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN 116912788 A	2023年10月20日	无	
CN 114596358 A	2022年6月7日	无	
CN 111626217 A	2020年9月4日	无	
CN 113111978 A	2021年7月13日	无	
CN 114187579 A	2022年3月15日	无	
CN 115453589 A	2022年12月9日	无	
WO 2023277998 A2	2023年1月5日	WO 2023277998 A3	2023年4月13日