Anomaly recognition method of perception system for autonomous vehicles based on distance metric

Cuiping Shao, Zujia Miao, Beizhang Chen, Yunduan Cui, Huiyun Li

Shenzhen Institute of Advanced Technology, Chinese Academy of Sciences, 1068 Xueyuan Avenue, Shenzhen University Town, Shenzhen 518055, China

Email: cp.shao@siat.ac.cn.

Environmental perception system is the premise of the safety and stability of the autonomous vehicle system. However, studies have shown that the on-board sensors included in the perception system are extremely vulnerable to external attacks and interference, leading to incorrect driving strategies and bringing great security threats. Aiming at the problem, this paper divides the vehicle-mounted sensors into a positioning group and an identification group according to their role in the perception system. Then, based on the information correlation between sensors in the same group and the information correlation of a single sensor on adjacent time series, the distance metric model between sensors in a group and the distance metric model for each sensor of this group on time series is established. And the normal distance intervals corresponding to the confidence interval are calculated respectively. According to the distance metric model between sensors, we can detect anomalies in the perception system in real-time. Further, according to the distance metric model for each sensor on adjacent time series, we can identify anomaly sensors. Our experimental results quantitatively show that the method achieves real-time anomaly recognition, and demonstrate the effectiveness and robustness of the method on the open-source KITTI dataset.

Introduction: Onboard sensors play a crucial role in the decision-making and planning of autonomous vehicles [1], which are the cornerstone of the safety and stability of an autonomous vehicle system [2]. The vulnerability of autonomous vehicle sensors has been shown in many studies [3]. These sensors are prone to be affected by the external environment, such as an attack, interference, and so on, resulting in the distortion of sensor sensing data. The external attack is one of the most common, simple, and covert methods [4]. Y. Cao removes real obstacles and adds false obstacles in front of his vehicle to manipulate the point cloud. [5]. A. Xue demonstrates that GPS devices are vulnerable to GPS spoofing (GSA) anomalies. [6]. For the safety of autonomous vehicle systems, the perception system must be capable of anomalous detecting in real-time [7]. However, current environmental perception technology is mainly focused on environmental information acquisition under an ideal environment, the high-precision recognition of semantic information, multi-sensor fusion, etc [8]. A comprehensive anomaly recognition and defense system for autonomous vehicle systems are still not available [9].

A novel anomaly recognition method of perception system for autonomous vehicles based on distance metrics is proposed in this letter. This method utilizes the redundancy of sensing information between multiple sensors and the overlap of sensing information of the same sensor at adjacent moments to respectively establish the cross-correlation of multiple sensors at the same moment and the auto-correlation of the same sensor on adjacent time series with the distance metric models. Finally, based on the distance metric model, we monitor in real-time whether the distance values are within the corresponding normal confidence intervals, to judge and identify anomaly sensors. Figure 1 shows the core idea of this method. The hierarchical detection method of cross-correlation and auto-correlation is adopted, which makes that this method not only takes into account the detection efficiency but also ensures the detection accuracy.

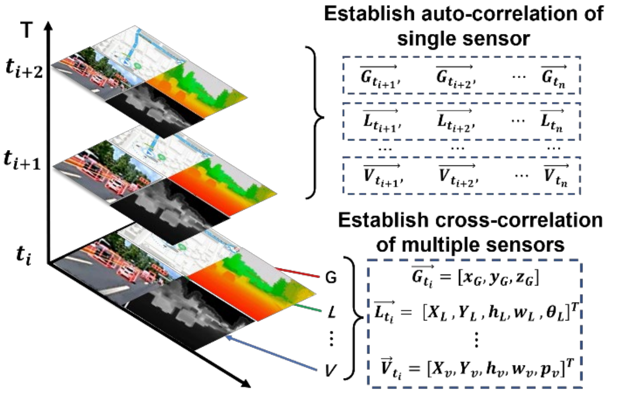

Establish auto-correlation of single sensor
T
t_{i+2}
t_{i+1}
t_i
$\overrightarrow{G_{t_{i+1}}},\ \overrightarrow{G_{t_{i+2}}},\ \cdots\ \overrightarrow{G_{t_n}}$
$\overrightarrow{L_{t_{i+1}}},\ \overrightarrow{L_{t_{i+2}}},\ \cdots\ \overrightarrow{L_{t_n}}$
$\cdots$
$\overrightarrow{V_{t_{i+1}}},\ \overrightarrow{V_{t_{i+2}}},\ \cdots\ \overrightarrow{V_{t_n}}$
Establish cross-correlation of multiple sensors
G
L
⋮
V
$\overrightarrow{G_{t_i}} = [x_G, y_G, z_G]$
$\overrightarrow{L_{t_i}} = [X_L, Y_L, h_L, w_L, \theta_L]^T$
⋮
$\vec{V}_{t_i} = [X_v, Y_v, h_v, w_v, p_v]^T$

Fig 1. *Schematic diagram of cross-correlation and auto-correlation of sensors*

The proposed method for recognizing anomaly sensors: In this section, we formulate a new method based on the distance metric to recognize the anomaly sensor. As shown in Figure 2, we establish the distance model and distance distribution between sensors to judge whether the group of sensors is abnormal. The overall algorithm is briefly described as follows.

Firstly, it is necessary to unify the data characteristics of sensors within a group according to the functional requirements since different sensor data provide various data vectors for different functions. Then, the cross-correlation distance of the sensor is calculated to judge whether the function is abnormal. If the distance exceeds the confident interval, the sensor of this function calculates the auto-correlation distance to recognize the anomaly sensor.

Secondly, according to the information correlation between sensors in the same group, we can establish a cross-correlation distance metric method and use the norm to describe the distance metric. We calculate the cross-correlation distance between different sensor feature data and the cross-correlation distance formula is presented as follows.

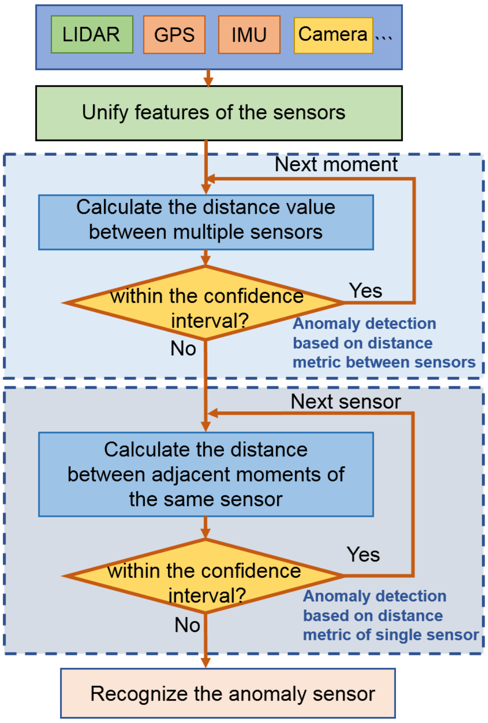

LIDAR
GPS
IMU
Camera
…
Unify features of the sensors
Next moment
Calculate the distance value between multiple sensors
within the confidence interval?
Yes
No
Anomaly detection based on distance metric between sensors
Next sensor
Calculate the distance between adjacent moments of the same sensor
within the confidence interval?
Yes
No
Anomaly detection based on distance metric of single sensor
Recognize the anomaly sensor

Fig 2. *The proposed method for detecting and locating anomaly sensor*

$$Distance_{i+1}\,(\mathrm{s1},\mathrm{s2}) = L_n\left(\overrightarrow{s1}_{i+1} - \overrightarrow{s2}_{i+1}\right) \qquad (1)$$

Where n is a non-negative integer, which can be taken as 0,1,2,3. $\overrightarrow{s1}_{i+1}$ and $\overrightarrow{s2}_{i+1}$ represent the sensing data of the sensor jointly realizing a certain function at $i + 1$ time respectively. The metric of the distance between multiple sensors, as well as the distance model, allows us to detect whether there is a problem between the sensors. Assuming that we judge whether the same groups of sensors are abnormal with a 99% confidence interval, the confidence intervals formula is present in the following.

$$Distance_{\ i+1}(S1,S2) \in \left[\varepsilon - 2.58\frac{\sigma}{\sqrt{m}}, \varepsilon + 2.58\frac{\sigma}{\sqrt{m}}\right] \qquad (2)$$

Where ε and σ^2 is the expectation and the variance of historical normal data, respectively. If the distance of the group of sensors is not within the above confidence interval, it indicates that the abnormalities in the group of sensors are detected, but the anomaly sensors cannot be recognized.

Finally, if the cross-correlation distance of the sensor group is not within the confidence interval, it is necessary to further computer the distance of a single sensor in the time domain to recognize the anomaly sensor. The information sensed by a sensor in two adjacent times will, under normal circumstances, have overlapping areas, meaning that the sensor data have a time correlation in the time series. Therefore, the auto-correlation distance of the single sensor at the adjacent time is within a certain range. The auto-correlation distance formula is given as follows.

$$\mathrm{Difference_{sensor}}(\mathrm{t_i}, \mathrm{t_{i-1}}) = \mathrm{L_n}(\mathrm{t_i}, \mathrm{t_{i-1}}) \qquad (3)$$

Assuming that we judge whether the single sensors are abnormal with a 99% confidence interval, the confidence intervals formula is present in the following.

$$\mathrm{Difference}_{sensor}(t_i, \mathrm{t}_{i-1}) \in [\tau - 2.58\frac{\sigma}{\sqrt{\mathrm{m}}}, \tau + 2.58\frac{\sigma}{\sqrt{\mathrm{m}}}] \quad (4)$$

If the auto-correlation distance of the sensor at two adjacent times is not within the above confidence interval, it indicates that this sensor successfully is recognized as an anomaly sensor.

Experiment result: In this section, we demonstrate the proposed method on the KITTI dataset under the LIDAR tampered attack. According to the positioning group of the autonomous vehicle, we group the sensors in the sensor system and unify the data characteristics of relevant sensors (such as LIDAR, GPS, and IMU). Considering the data correlation and computational efficiency, we choose the sliding window represent a time index and set to 10 seconds. A selection of anomaly points is used to simulate the sensor anomaly test and the wrong point cloud data of LIDAR location features is injected at the moment when the time series index is 100, then we implement our proposed method.

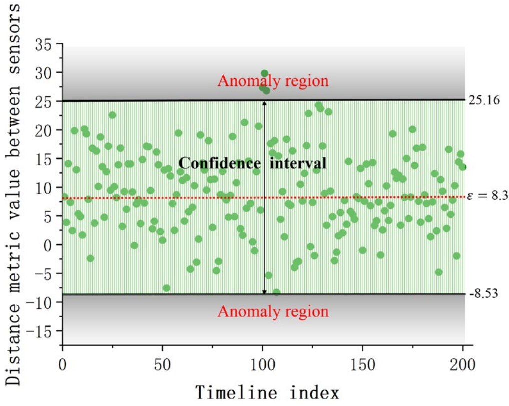
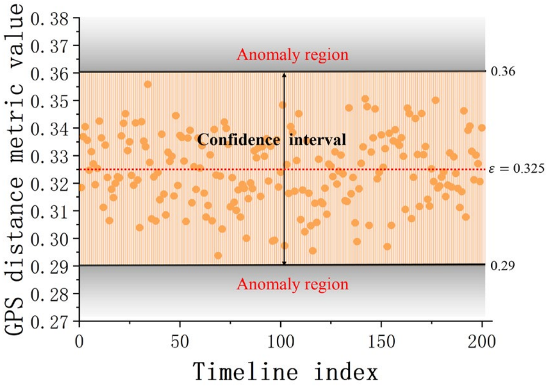


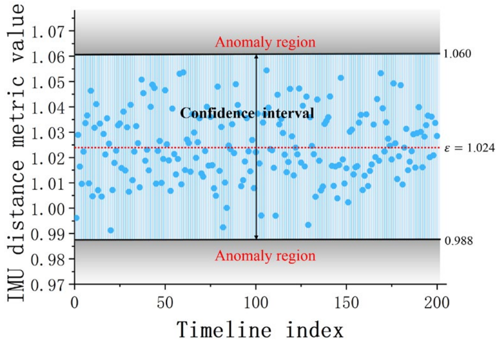
Fig 3. *Distribution of distance metric values for sensors in the positioning group at 99% confidence* ($\varepsilon = 8.32$ $\sigma = 6.53$ ）

To detect anomaly sensors in real-time, We calculate the cross-correlation distance between different sensors data. As shown in Figure 3, it can be observed that there is the distribution of distance metric values for sensors in the positioning group and most distance values are in the 99% confidence interval (green region), while there are significant outliers appearing in the anomaly region (grey region) under the LIDAR tampering attack. This means that there are anomaly sensors in the positioning group and it is necessary to calculate the auto-correlation of the sensor to recognize the anomaly sensor. In Figure 4, there is the distribution of the distance measure of the auto-correlation of each sensor in the positioning group at 99% confidence.

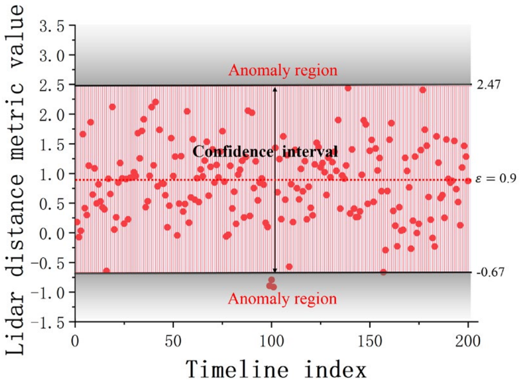
In Figure 4 (a) and Figure 4 (b), it can be observed that the auto-correlation distance of IMU and GPS are always within the 99% confidence interval (colored region), while some outliers of LIDAR appear in the anomaly region (grey region), as shown in Figure 4 (c), which means that the data of LIDAR violates the time correlation and the anomaly occurs on the LIDAR sensor. Therefore, our proposed method successfully detects and recognizes the anomaly data of LIDAR.



(a) *Distribution of GPS distance metric value on adjacent time series*（$\varepsilon = 0.325\ \sigma = 0.0136$）



(b) *Distribution of IMU distance metric value on adjacent time series (* $\varepsilon = 0.9\ \sigma = 0.61$*)*



(c) *Distribution of LIDAR distance metric value on adjacent time series (* $\varepsilon = 1.024\ \sigma = 0.014$*)*

Fig 4. *The distribution of the distance measure of the auto-correlation of each sensor in the positioning group at 99% confidence*

Conclusion: In this letter, we propose an anomaly recognition method based on distance metrics in the spatial domain and time domain for autonomous vehicle perception systems. This method can not only detect abnormalities but also recognize anomaly sensors, which will greatly ensure the safety of the autonomous vehicle. In the experiment, a tampered anomaly is implanted into the LIDAR, and experiments on the real KITTI dataset demonstrate the feasibility of the method. The proposed method in this paper is not only applicable to autonomous vehicles but also applicable to other unmanned systems, such as UAVs and unmanned ships.

Acknowledgments: This work has been funded by NSFC 62004212, 62103403, Shenzhen Basic Research Project (Grant Nos. JCYJ20210324101210027, JCYJ20200109115414354, JCYJ20200109115403807), Shenzhen Key Laboratory of Electric Vehicle Powertrain Platform and Safety Technology， CAS Key Laboratory of Human-Machine Intelligence-Synergy Systems, Shenzhen Institute of Advanced Technology, Guangdong-Hong Kong-Macao Joint Laboratory of Human-Machine Intelligence-Synergy Systems (NO. 2019B121205007).

References

1. Woodward, B., and Tomas, K.. Intelligent Transportation Applications, Autonomous Vehicle Perception Sensor Data, and Decision-Making Self-Driving Car Control Algorithms in Smart Sustainable Urban Mobility Systems, Contemporary Readings in Law and Social Justice 13.2 (2021): pp. 51-64.
2. Khan, F. et al.. Autonomous vehicles: A study of implementation and security, International Journal of Electrical & Computer Engineering (2088-8708) 11, no. 4 2021.
3. Vargas, J., Alsweiss, S., Toker O., Razdan, R and Santos, J.. An overview of autonomous vehicles sensors and their vulnerability to weather conditions., Sensors 21, no. 16, 2021.
4. Kim, K., et al., Cybersecurity for autonomous vehicles: Review of attacks and defense, Computers & Security, no. 103, 2021, p. 102150.
5. Sun, J., Cao, Y., Choy, C. B., Yu, Z., Anandkumar, A., Mao, Z. M., and Xiao, C.. Adversarially Robust 3D Point Cloud Recognition Using Self-Supervisions, Advances in Neural Information Processing Systems, no. 34, 2021.
6. Xue, A., Xu, F., Chow, J.H., Leng, S., Kong, H., Xu, J. and Bi, T.. Data-driven detection for GPS spoofing anomaly using phasor measurements in smart grid, International Journal of Electrical Power & Energy Systems, no. 129, 2021,p.106883.
7. You, C., Hau, Z. and Demetriou, S.. Temporal Consistency Checks to Detect LiDAR Spoofing Anomalys on Autonomous Vehicle Perception, In Proceedings of the 1st Workshop on Security and Privacy for Mobile AI , June, 2021, pp. 13-18.
8. Chen, Q., Xie, Y., Guo, S., Bai, J. and Shu, Q.. Sensing system of environmental perception technologies for autonomous vehicles: A review of state of the art and challenges. Sensors and Actuators A: Physical, 319, 2021, p.112566.
9. Deng, Y., Zhang, T., Lou, G., Zheng, X., Jin, J., and Han, Q. L.. Deep learning-based autonomous driving systems: a survey of anomalys and defenses, IEEE Transactions on Industrial Informatics, 17, no. 17, 2021, pp. 7897-7912.