2023 21st International Conference on Advanced Robotics (ICAR)
5-8 December 2023. Abu Dhabi, UAE

Anomaly Detection in LiDAR Data Using Virtual and Real Observations

Keiichiro Hattori
Tohoku University
Miyagi, Japan
hattori.keiichiro@rm.is.tohoku.ac.jp

Ranulfo Bezerra
Tohoku University
Miyagi, Japan
bezerra.ranulfo@rm.is.tohoku.ac.jp

Shotaro Kojima
Tohoku University
Miyagi, Japan
kojima@rm.is.tohoku.ac.jp

Yoshito Okada
Tohoku University
Miyagi, Japan
okada@rm.is.tohoku.ac.jp

Kazunori Ohno
Tohoku University
Miyagi, Japan
kazunori@rm.is.tohoku.ac.jp

Shintaro Ishihara
Kyoto Sangyo University
Kyoto, Japan
shintaro.stonefield@gmail.com

Kenji Sawada
The University of Electro-Communications
Tokyo, Japan
knj.sawada@uec.ac.jp

Satoshi Tadokoro
Tohoku University
Miyagi, Japan
tadokoro@tohoku.ac.jp

2023 21st International Conference on Advanced Robotics (ICAR) | 979-8-3503-4229-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAR58858.2023.10406443

***Abstract*—With the constant progress of robot integration within society, security remains a paramount concern, particularly due to the increasing potential for damage arising from malicious attacks. However, the inherent challenges of preventing every potential attack vector require innovative security measures. This study presents a unified anomaly detection method employing a virtual environment mirroring real-world observations. By focusing on the discrepancies between real and virtual observational data, anomalies can be effectively detected, the types of which are further identified through a time-series analysis of these discrepancies. Results demonstrated the capacity of our method to successfully detect and categorize anomalies arising from various sources including environmental noise, robotic malfunctions, and communication-based attacks. Furthermore, our anomaly detection method consistently achieved precision, recall, and F1 scores higher than 90%, underscoring its effectiveness.**

I. Introduction

As robotics becomes increasingly integrated into our society, security has emerged as a paramount concern. Traditional robotics, which primarily operates within closed networks and controlled environments, is giving way to advanced contemporary robotics in which there is frequent interaction through networks and clouds, which enables the exchange of a myriad of data. This evolution in robotics has opened up new avenues for malicious actors to launch attacks from both cyber and physical domains, employing a diverse range of routes and methods [1]. The potential for harm from such malevolent attacks is escalating, underscoring the urgent need for robust security measures in robotics.

This paper focuses on the security issues related to inspection robots deployed in industrial plants. These robots autonomously navigate using pre-existing maps, conducting tasks such as visual gauge inspections and abnormal sound detection. The environmental elements these robots interact with are generally stationary, and the environment's overall shape is known beforehand. Key sensors incorporated in these robots include Lidar, cameras, and infrared thermal imaging. Of these, securing Lidar data is particularly crucial as it is utilized for core functions in autonomous movement, such as location estimation [2] and obstacle detection [3]. An attack on the Lidar system can cause malfunctioning, disrupting the robot's normal operation and potentially damaging surrounding equipment, causing harm to the plant. Therefore, detecting such attacks and preventing damage to the plant is fundamental.

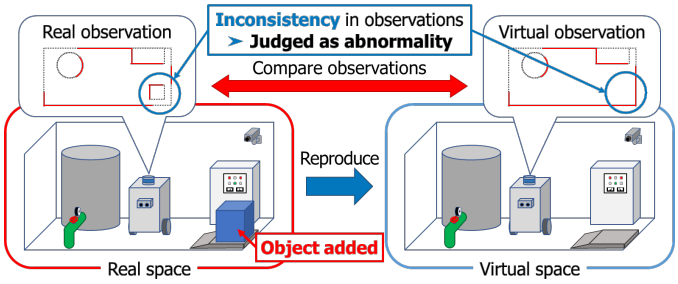


Fig. 1: Anomaly Detection through Real and Virtual Observations: We build a replica of the real environment in a virtual space, enabling analogous sensor observations. Anomalies, such as the introduction of an object solely in the real world, are detected through differences in the real and virtual observations.

Despite the critical importance of securing Lidar data, limited research has been conducted on the detection of

attacks against this kind of sensor. While numerous studies exist on environmental noise affecting Lidar data, addressing challenges such as removing interference from snow [4] or fog [5], there are currently no detection methods for deliberate alterations of Lidar data or physical obstructions to measurements.

To address this gap, this study introduces a novel approach to Lidar attack detection by leveraging observational data from a meticulously constructed virtual environment that emulates real-world conditions, as depicted in Fig. 1. The proposed method hinges on the comparison of observational data from both the actual and virtual environments, with the aim of pinpointing Lidar data anomalies from the discrepancies evident between these two datasets. Upon detecting an anomaly, the method facilitates the classification of the anomaly type by conducting a temporal analysis of these discrepancies.

The effectiveness of this approach is further validated through the examination of various types of anomalies, specifically 'Block', 'Spoof', and 'Mirror'. The results highlight the capacity of this method to accurately detect and categorize a wide range of attacks. An impressive precision rate and recall rate of over 80% were consistently achieved across an array of anomaly detection classifiers, with the Random Forest classifier performing notably well, recording rates of 0.93, 0.91, and 0.92 for precision, recall, and F1 score, respectively, even without meticulous fine-tuning.

The primary contributions of this paper are threefold:

- The proposal of an anomaly detection method based on the comparison of temporal observations in virtual and real environments. This method allows for the identification of anomalies and their origins by focusing on the temporal changes in the difference between virtual and real observations.
- The implementation of the proposed method on an actual system. A 2D LiDAR sensor was used for observations, assuming an inspection robot in a plant as the application. A method to detect anomalies from the difference in time series data obtained from both a Unity-based simulator and the actual system was implemented.
- The replication of various types of anomalies at different locations and verification of anomaly detection through experimental tests. Verification was conducted for anomalies occurring in the environment, on the robot, and in the network. Results suggest that it is possible to detect anomalies from data differences and categorize various types of anomalies based on differences in temporal change patterns.

The remainder of this paper is organized as follows. Chapter 2 describes robot cybersecurity, anomaly detection methods that use machine learning, and anomaly detection methods that use simulations. Chapter 3 introduces the system configuration used in this paper, describes the method to detect anomalies using the differences between real and virtual time-series observations, and discusses the identification of anomalies based on the trend of differences. Chapter 4 explains the experimental methods and verification items using an actual machine regarding the trend of differences discussed in Chapter 3. Chapter 5 shows the difference in trends for each anomaly obtained from the evaluation experiment, and Chapter 6 discusses these trends. Chapter 7 summarizes the paper and outlines future work.

II. Related works

In the realm of cybersecurity research, the focus is generally on communication components and the development of secure protocols. In the field of robotics, issues concerning the security of the Robot Operating System (ROS) middleware have been pointed out [6]. ROS2, the successor to ROS, has been developed with improvements in protocol security [7]. Research on intrusion detection systems to protect against abnormal communication and firewall studies is also ongoing [8] [9].

However, in robot security, not only cyber attacks but also physical attacks must be considered. Lawson et al. [10] proposed an anomaly detection system for a patrol robot using Generative Adversarial Networks (GANs), focusing on the detection of anomalies when the robot is attacked. This approach, while effective, does not consider physical attacks. Tarapore et al. [11] developed a robust fault-detection approach in which robots in a swarm learn to distinguish between normal and faulty behaviors online. This approach was tested on a swarm of seven physical mobile robots and showed promising results. However, it does not consider cyber attacks.

Therefore, there are many attack routes to consider compared to general cybersecurity [12]. This study is motivated by the development of a security system that can handle attacks from both cyber and physical perspectives. Specifically, this paper focuses on minimizing the damage when the robot is attacked, and is dedicated to the detection of anomalies when attacked. Unlike the aforementioned studies, our work aims to detect both cyber and physical attacks on robots, providing a more comprehensive security solution.

Regarding the detection of errors in LiDAR data, there are many studies on filtering methods for environmental noise such as fog removal [5] and snow removal [4]. However, there is little research on specific detection methods for intentional attacks on the LiDAR data that we target in this paper, although there are reports on the threats [13]. This paper aims to realize the detection of attacks and clustering of attack methods using digital twin and learning-based clustering against attacks from both cyber and physical sides to the Lidar.

There are several studies on anomaly detection in robots using simulations and digital twins. For instance, Castellani et al. conducted accurate simulations using digital twins that can faithfully reproduce the characteristics of real space [14]. In this method, even with a small number of abnormal data samples in real space, high-precision detection is possible by using data from the digital twin simulation in a normal operating state. In this method, the digital twin is used only during learning. Unlike existing research that uses a digital twin to increase learning data, this paper generates real and virtual observations in real time using a digital twin and

detects attacks by focusing on the differences between them. Therefore, the proposed method uses the digital twin not only at the time of learning but also in the phase of actual attack detection.

Choi et al. [15] proposed a method for anomaly detection based on the deviation between predicted and actual sensor values, suggesting a replacement strategy for anomalous sensors. Similarly, Guo et al. [16] introduced a model-based anomaly detection system that leverages the physical dynamics of mobile robots and the correlation between sensor readings and control commands. Unlike these works, our approach not only considers the robot and its sensors but also simulates the surrounding environment, enabling the detection of a broader range of attacks, including those that alter the environment.

III. Condition Settings

A. Target Environment

In this paper, we address the security of LiDAR applied to plant inspection robots. Plant inspection robots generally operate according to pre-given environmental maps, and usually have a model of their operating environment. Furthermore, there are few changes in the arrangement of objects in the environment.

B. Threat Model

The hardware configuration of the robot is shown in Fig.2. The robot receives control inputs from the control PC via the router and transmits sensor data. The attacks on the robot that are anticipated in this context are described in Table I. Traditional security research has been focused on issues related to the network of the control PC and router. However, security related to the robot has been less explored. Therefore, in this paper, we will test against attacks on the environment, the robot itself, and robot communication, focusing on conditions 2, 3, 4 from Table I. Please note that our proposed method utilizes the difference between physical and virtual observation spaces, thus attacks that do not directly affect the observation, such as data theft and ransomware, are not considered for detection.

IV. Anomaly Detection Method Based on Virtual and Real Observation

A. Overview

In this paper, we apply and verify the effectiveness of anomaly detection based on the comparison of real and virtual spatiotemporal observation data to 2D LiDAR. LiDAR is a primary observation sensor for robots to perceive the outside world and is used for various functions such as mapping the surrounding environment and detecting obstacles. Here, we construct a robot with a similar structure in the virtual space to the real space and detect anomalies from the differences in the temporal data of LiDAR in both spaces.

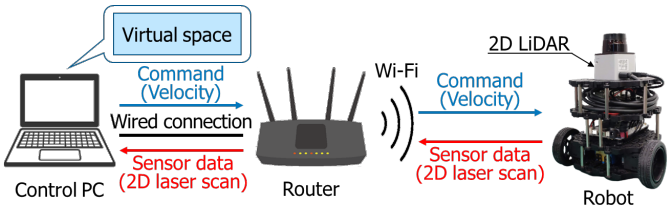


Fig. 2: Hardware configuration: The control PC and mobile robot communicate over a local network via a router. A virtual environment is operating on the control PC. Sensor data from the virtual robot and the real robot is aggregated on the control PC.

B. System Configuration of the Robot

Fig. 2 shows the hardware configuration in the proposed system. The control PC is wired to the router, and the robot communicates wirelessly through the router. The robot uses the Turtlebot3, a mobile robot platform equipped with a computer and 2D LiDAR. The robot's sensor data is transmitted to the control PC through communication in real-time. A virtual space is constructed within the simulator running on the control PC, which enables the comparison of the transmitted data from the real robot with the data of the robot in the virtual space.

Fig. 3 shows the software configuration. The control PC and robot operate via the Robot Operating System (ROS) 1, a middleware for robot development, and the robot's data is transmitted to the control PC by ROS1's communication. The physical simulator Unity is used to construct the virtual space. By replicating the robot's structure and the shape of the operating environment on Unity, we can obtain sensor data observed by the robot in the virtual space. We sequentially compare the temporal data of 2D LiDAR obtained in the real and virtual spaces and detect anomalies from the data

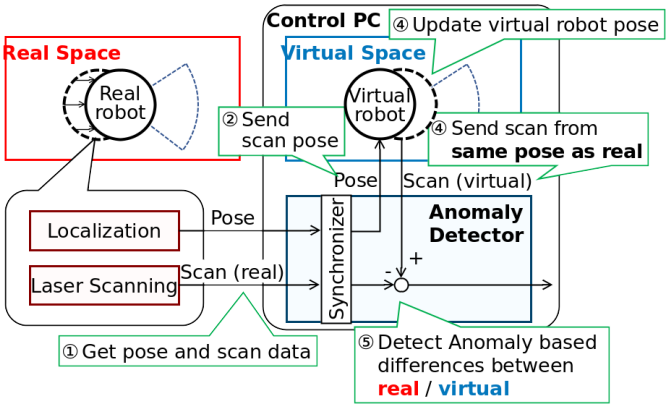
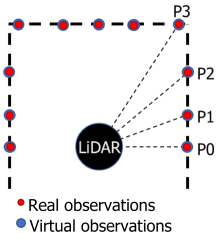
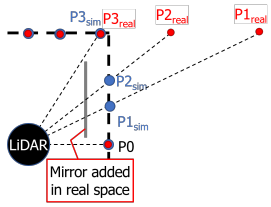
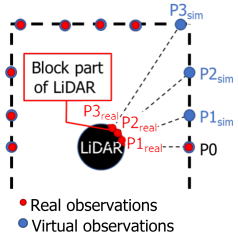
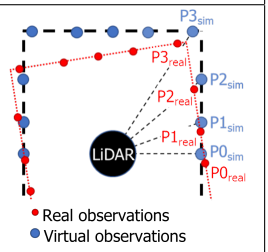


Fig. 3: Software configuration: The sensor data of the real robot and the virtual robot are gathered in the anomaly detection node on the control PC. The sensor data of the real and virtual spaces is sequentially compared, and anomalies are identified from the temporal changes in their differences.

TABLE I: Differences in Trends due to Abnormalities

Condition	① Normal Conditions	② Abnormalities in the Environment	③ Abnormalities in the Robot	④ Abnormalities in the Network
Abnormal Content	None	Addition of an Object	Physical Obstruction of LiDAR	Falsification of LiDAR Information
Example Observation				
Discrepancy	None (observation points coincide)	Occurs in the direction of the mirror	Occurs in the direction of the obstruction	Occurs across the entire field of view
Time Series Variation	None (slight variation due to noise)	Direction transitions as the robot moves	Always in a fixed direction relative to the robot	Changes irregularly

differences. In this verification, we focus on the anomalies occurring in 2D LiDAR observation data, and assume no discrepancy between the observation locations in the real and virtual spaces. Therefore, we do not simulate the robot's position in the virtual space but reflect the robot's position in the real space, and perform the comparison of the observation data at the same location.

C. Anomaly Detection Method

In this paper, we aim to detect four distinct classes of conditions for a robotic system equipped with 2D LiDAR, based on the discrepancies between the robot's virtual perception and actual reality. A learning-based method is employed to distinguish these classes, each of which represents a different type of anomaly or normal operation. We have short-handed the names of these classes as Default, Mirror, Block, and Spoofed for ease of reference.

1) **Default (Normal Conditions):** The ideal state, where the robot's virtual and real-world perceptions are perfectly aligned. As there are no discrepancies or abnormalities in this state, any detected data anomalies will be close to zero, indicating that the system is functioning as expected.
2) **Mirror (Abnormalities in the Environment):** This class represents situations where an unexpected object, specifically a mirror, is introduced into the robot's environment. The mirror, not being part of the robot's virtual map, creates unusual reflections and disturbances for the LiDAR sensor. This results in a fixed spatial discrepancy between the real world and virtual space due to the unexpected reflective properties of the mirror. These continuous discrepancies can be utilized to detect environmental anomalies created by such reflective surfaces.
3) **Block (Abnormalities in the Robot):** Abnormalities are linked to physical disruptions in the robot's equipment, particularly its LiDAR system. If the LiDAR system is obstructed, the robot's perception in a particular direction will be affected. This leads to discrepancies that are always in the direction of the LiDAR's obstruction, regardless of the robot's motion. Thus, abnormalities associated with the robot's LiDAR can be identified based on a fixed-direction discrepancy.
4) **Spoofed (Abnormalities in the Network):** Involves anomalies due to cyber-attacks, such as replay attacks that falsify the information received from the LiDAR. Such attacks may cause discrepancies across the entire field of view of the robot, and these irregularities are expected to increase with the duration of the attack. This class can be identified based on irregular discrepancies across the robot's field of view.

The learning-based method enables the system to distinguish between these classes based on their specific discrepancy patterns, as can be seen in Fig. 4. This facilitates monitoring and verifying if the system is operating under normal conditions or identifying various types of abnormalities.

V. Evaluation Experiment

The proposed method's effectiveness was evaluated using a physical robot in a real-world experiment. The robot operated in a simple rectangular field, as shown in Fig.5, tasked with detecting anomalies listed in Table I based on the observational data it collected. Initiated from a starting point, the robot progressed at a speed of 0.1[m/s] as indicated in Fig.5(c), capturing observational data to discern potential anomalies. The synchronization calculation cycle was set at 5[Hz], enabling the generation of a time-series data set for observing trend differences attributable to each anomaly. The

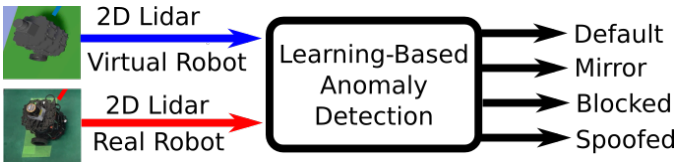
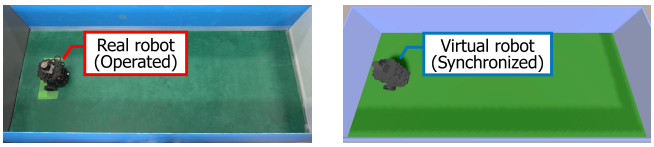
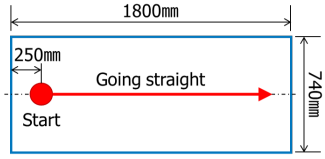


Fig. 4: Overview of Anomaly Detection.



(a) Real space (b) Virtual space



(c) Field configuration

Fig. 5: Operation field: Straight line operation is assumed on a field with a simple structure. Additional conditions are applied for experimentation, according to the anomalies to be simulated.

robot's current position was estimated using wheel rotation and IMU-based odometry data, with an assumption that the collected observational data was independent of this position estimate. Over the course of the experiment, 700 samples were collected, providing a robust data set for validating the proposed methodology's capacity to effectively identify and differentiate between various types of anomalies.

The following describes the reproduction environments used to extract data about each anomaly:

1) Normal state
   No additional conditions to those stated above. The environment is as described in Fig. 5.

2) Addition of a mirror object
   An unexpected object is placed in the real environment, as shown in Fig. 6.

3) Physical obstruction of LiDAR
   An object is placed on the side of the LiDAR to obstruct part of its field of view, as shown in Fig. 7.

4) Falsification of LiDAR information
   By means of a replay attack, observational data from a different route, shown in Fig. 8, is transmitted. For this verification, the rosbag function of ROS, which can record and replay data, is used to simulate the replay attack.

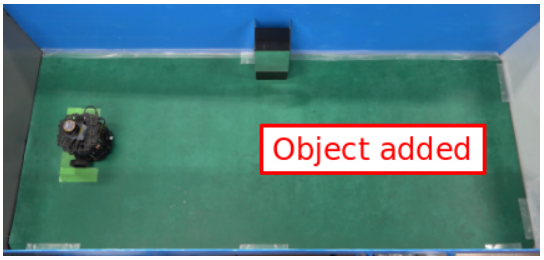


Fig. 6: Field during object addition: A stationary mirror object is placed to the front-left in the direction of travel in real space.

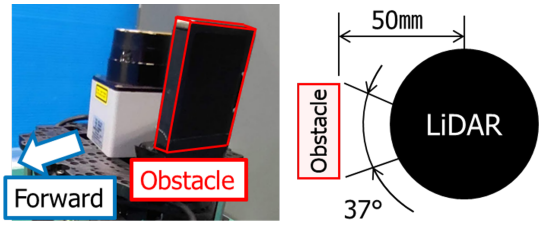


Fig. 7: Blocking the LiDAR: An obstacle is placed on the right side of the LiDAR's direction of travel, blocking a part of its view.

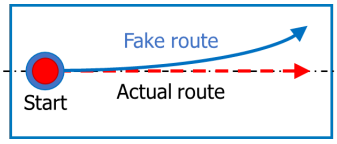


Fig. 8: Operation path during replay attack: A replay attack is conducted using data from a false route run.

Regarding the virtual environment, it remains consistent and unaltered, as depicted in Fig. 5. Given that our simulations focus on potential attacks occurring within a real environment, we presume that the virtual environment remains secure, possessing the most current information. The LiDAR data representation from both real and virtual environments yields identical types of data, as illustrated in Fig. 9. It is important to note that we employ a LiDAR sensor with a limited angular range, and synchronization is maintained between the data streams from the two environments, ensuring the validity of our comparative analysis.

In order to assess the effectiveness of our anomaly detection approach, we utilized eight distinct learning-based methods to validate our proposed methodology. The utilized algorithms encompass Nearest Neighbors [17], Linear SVM [18], RBF SVM [19], Gaussian Process [20], Decision Tree [21], Random Forest [22], Neural Network [23], and QDA (Quadratic Discriminant Analysis) [24]. All methods were trained utilizing the same dataset, which had been both randomized and

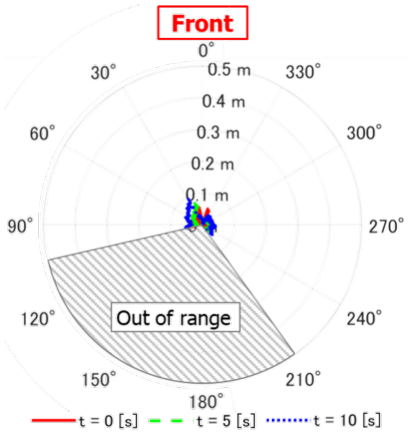


Fig. 9: 2D LiDAR data example in a default scenario.

normalized prior to the experiment to ensure fairness and eliminate potential bias.

VI. Experimental Results

Fig. 10 shows the behaviour under each condition. The LiDAR measurements in the real and virtual spaces are represented as green and black points, respectively. Also, the difference in measurements of each laser beam is represented by a red solid line.

The outcomes of the learning-based anomaly detection methods are presented in Table II. An analysis of the data reveals that the Random Forest algorithm outperforms the others, achieving a superior F1 score of 92%, accompanied by a precision of 93% and a recall rate of 91%. Additionally, it is noteworthy that all utilized learning methods consistently exhibit precision, recall, and F1 scores exceeding the threshold of 80%, attesting to the robustness of these methods in the context of anomaly detection.

TABLE II: Abnormal Detection Classifier's Results

Classifier	Precision	Recall	F1
Nearest Neighbors	0.87	0.87	0.87
Linear SVM	0.84	0.84	0.83
RBF SVM	0.84	0.79	0.81
Gaussian Process	0.87	0.89	0.88
Decision Tree	0.87	0.82	0.84
Random Forest	**0.93**	**0.91**	**0.92**
Neural Net	0.86	0.86	0.85
QDA	0.89	0.87	0.88

The confusion matrix from Fig. 11 provides a detailed breakdown of the classification results. It appears that the classifier was mostly accurate with 'Default', 'Mirror', 'Block', and 'Spoofed' classes, achieving precision rates of 90%, 90%, 82%, and 85% respectively. However, the 'Default' class was occasionally misclassified as 'Block' or 'Spoofed' (8% and 2% respectively). The 'Mirror' class saw a minor confusion with the 'Default' and 'Block' classes (5% each). The 'Block' class experienced confusion with 'Default' and 'Spoofed' classes (11% and 7% respectively), and the 'Spoofed' class was primarily confused with 'Default' and 'Block' classes (6% and 9% respectively).

VII. Discussion

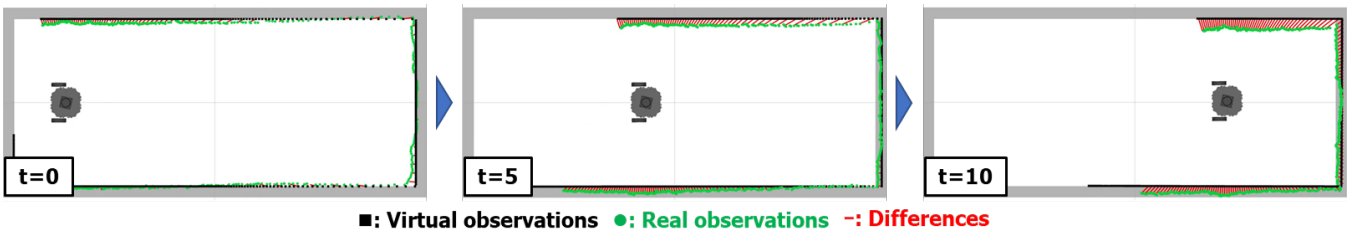
In the normal condition, as illustrated in Fig. 10a, it can be verified that there is minimal distance discrepancy. When an object is added, as represented in Fig. 10b, there is a noticeable difference in distance related to the location where the object was added. Over time, the direction of the resulting distance discrepancy gradually changes, owing to the change in the object's visible direction as the robot moves, indicating a change in the real environment. In the case of a physical interruption of the LiDAR, as shown in Fig. 10c, the distance discrepancy consistently occurs to the right of the robot's course of progress, suggesting that a portion of the LiDAR's field of view is obstructed. Lastly, when the LiDAR information is falsified, as demonstrated in Fig. 10d, the distance discrepancy increases throughout as the robot advances, with discrepancies occurring in all directions and increasing over time. This suggests a widening gap between the actual robot trajectory and the trajectory used in the replay attack, indicating the presence of irregular discrepancies across the entire field of view.

The results presented in Table II, derived from a range of learning-based anomaly detection methods, demonstrate the effectiveness of these methodologies in detecting anomalies, despite the lack of extensive hyperparameter tuning or optimization for the individual classifiers. Notably, the Random Forest classifier achieved the highest scores across precision, recall, and F1 metrics, attaining rates of 0.93, 0.91, and 0.92, respectively, without fine-tuning. This indicates a robust ability to accurately identify true anomalies and capture a high proportion of the total anomalies. Even though there is potential for further performance improvement with more dedicated algorithm-specific tuning, all the classifiers displayed precision and recall rates above 80%, validating the effectiveness of the proposed methodology. More importantly, the efficiency of these methods enables their deployment for real-time or near-real-time anomaly detection, making them suitable for automatic, continuous monitoring applications. Therefore, the primary accomplishment of this study is not merely the high precision and recall rates, but the successful demonstration that the proposed methodology can robustly detect anomalies with high accuracy, providing an efficient solution for anomaly detection in various real-world scenarios.

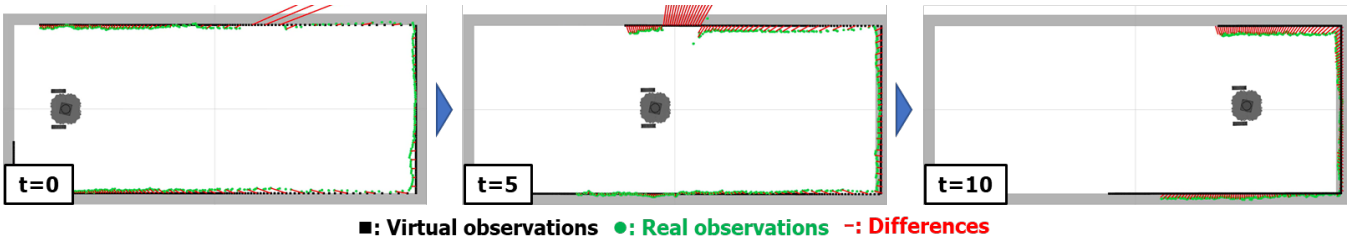
The insights gathered from the confusion matrix are crucial for understanding the model's performance and areas of improvement. Although the model has performed reasonably well in classifying most classes, it shows a slight tendency to misclassify the 'Block' and 'Spoofed' classes as 'Default'. This may be due to the inherent complexity in differentiating these categories, or due to inadequate representative instances in the training data. A similar pattern is observed for the 'Mirror' class, which gets misinterpreted as 'Default' or 'Block'. The matrix highlights the importance of refining the classifier to handle these specific ambiguities. Enhancements could include gathering more diverse training data, fine-tuning the algorithm, or incorporating additional contextual information to help disambiguate the classes.

Regardless of the type of anomaly, once it is detected, it is possible to prompt the robot itself to verify the anomaly. Concerning the difference in anomaly trends mentioned above, it is expected that specific behaviors, such as robot movement or stoppage, can facilitate anomaly identification by allowing additional observations. Furthermore, it is naturally possible to alert humans to the occurrence of an anomaly. In this case, specifying potential locations of anomaly occurrence can facilitate human response.

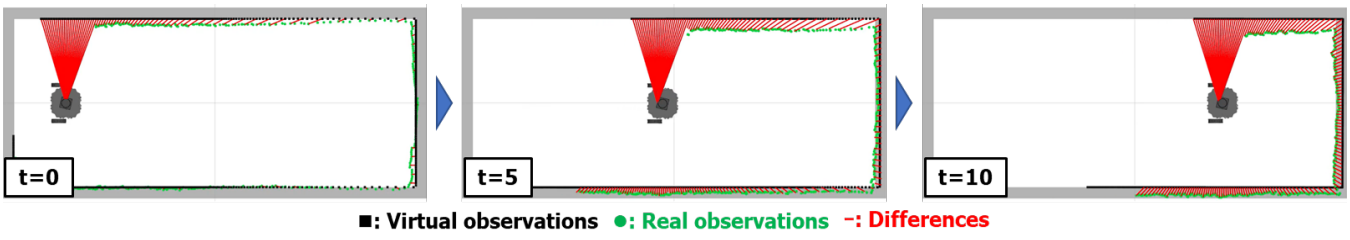
Despite the promising results, this study acknowledges its limitations and recognizes the necessity for further investigations. Specifically, the verification of a wider range of cyber attacks, beyond the replay attack examined here, warrants consideration. Conducting extensive evaluations with diverse



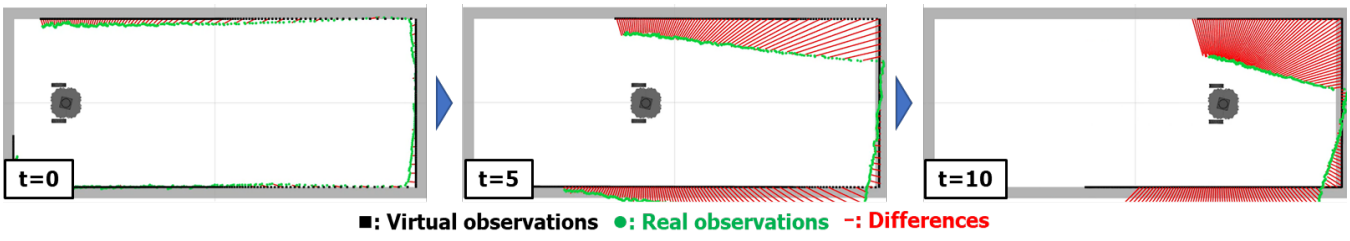
(a) Normal condition: The distance discrepancy is slight as the robot's virtual and real-world perceptions are almost aligned.



(b) Mirror added: The distance discrepancy occurs for where the object was added, although it can't be measured directly due to the reflective properties of the mirror.



(c) LiDAR physically blocked: The distance discrepancy consistently occurs in the direction where the LiDAR field of view is obstructed.



(d) LiDAR data spoofed: The distance discrepancy increases throughout as the robot advances, with differences occurring in all directions.

Fig. 10: Result of the difference in each anomaly.

attack methodologies may offer valuable insights into trends that differentiate various types of attacks. Simultaneously, the effective implementation of the proposed method relies on several assumptions. These include the construction of a comprehensive virtual representation of the environment, the presumption of a static environment devoid of unspecified crowd dynamics, and the requirement for precise synchronization of position between the virtual and real spaces. Future work should aim to address these limitations and assumptions to enhance the robustness and generalizability of the proposed method.

Expanding on the discussed limitations and proposed future investigations, an enhancement to the current anomaly detection system could potentially be achieved through the integration of additional sensor types or the inclusion of observations from alternative robotic platforms. The current system discerns anomalies by juxtaposing observations from real and virtual environments, categorizing any disparities as indicative of abnormal occurrences. This suggests that an increase in the diversity of the observational perspectives could bolster anomaly detection, effectively broadening the scope of identifiable anomalies. Moreover, the sophistication required to fabricate deceptive information across multiple viewpoints simultaneously heightens the challenge for potential threats, thereby fortifying system security. Consequently, future research endeavors will seek to devise methodologies to amalgamate diverse observational data types within a unified space, thereby enhancing the robustness of the anomaly detection system.

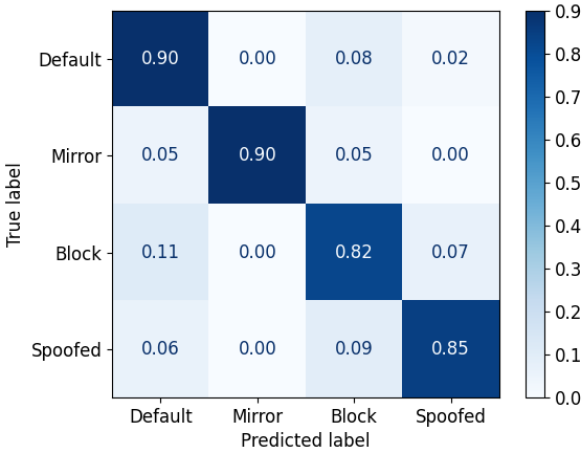


Fig. 11: Confusion Matrix of Random Forest.

VIII. Conclusion

In this study, we proposed an innovative approach aimed at detecting anomalies of various origins, a crucial factor for ensuring robotic systems' security. Our approach capitalizes on a virtual environment mirroring the real one, enhancing the observational perspectives and relying on the observed disparities between these spaces for anomaly detection. Moreover, this methodology identifies the origin of the anomaly based on the distinct temporal trends in these discrepancies.

Through comprehensive evaluation experiments, we substantiated the presence of distinct trends in the discrepancies induced by anomalies of diverse origins, including environmental, robotic, and communication anomalies. Our experiments yielded a high accuracy, with precision and recall rates exceeding 90% for some models, demonstrating that discrepancies between real and virtual observations can be used effectively to detect anomalies.

Moving forward, our strategy involves refining our approach by introducing a quantitative measure for the observed disparities and developing a sophisticated judgement mechanism that would enable robots to autonomously identify and respond to a range of anomalies. Additionally, our anomaly detection system's robustness can be significantly improved by integrating additional sensors like cameras and sharing perspectives among multiple robots. We anticipate that these enhancements will increase the system's efficiency in detecting a wider array of anomalies, thereby strengthening the overall security of robotic systems.

Acknowledgment

This research was conducted as a collaborative research project with the Control System Security Center of the Technological Research Association.

References

[1] Laura Alzola Kirschgens, Irati Zamalloa Ugarte, Endika Gil Uriarte, Aday Muniz Rosas, and Víctor Mayoral Vilches. Robot hazards: from safety to security. *arXiv preprint arXiv:1806.06681*, 2018.

[2] Sebastian Thrun, Dieter Fox, Wolfram Burgard, et al. Monte carlo localization with mixture proposal distribution. In *AAAI/IAAI*, pages 859–865, 2000.

[3] Angelo Nikko Catapang and Manuel Ramos. Obstacle detection using a 2d lidar system for an autonomous vehicle. In *2016 6th IEEE International Conference on Control System, Computing and Engineering (ICCSCE)*, pages 441–445. IEEE, 2016.

[4] Ji-Il Park, Jihyuk Park, and Kyung-Soo Kim. Fast and accurate desnowing algorithm for lidar point clouds. *IEEE Access*, 8:160202–160212, 2020.

[5] Abu Ubaidah Shamsudin, Kazunori Ohno, Thomas Westfechtel, Suzuki Takahiro, Yoshito Okada, and Satoshi Tadokoro. Fog removal using laser beam penetration, laser intensity, and geometrical features for 3d measurements in fog-filled room. *Advanced robotics*, 30(11-12):729–743, 2016.

[6] Rafael R Teixeira, Igor P Maurell, and Paulo LJ Drews. Security on ros: analyzing and exploiting vulnerabilities of ros-based systems. In *2020 Latin American robotics symposium (LARS), 2020 Brazilian symposium on robotics (SBR) and 2020 workshop on robotics in education (WRE)*, pages 1–6. IEEE, 2020.

[7] Vincenzo DiLuoffo, William R Michalson, and Berk Sunar. Robot operating system 2: The need for a holistic security approach to robotic architectures. *International Journal of Advanced Robotic Systems*, 15(3):1729881418770011, 2018.

[8] Ying Zhou, Thomas A Mazzuchi, and Shahram Sarkani. M-adaboost-a based ensemble system for network intrusion detection. *Expert Systems with Applications*, 162:113864, 2020.

[9] Anna Gorbenko and Vladimir Popov. Abnormal behavioral pattern detection in closed-loop robotic systems for zero-day deceptive threats. In *2020 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)*, pages 1–6. IEEE, 2020.

[10] W. Lawson, E. Bekele, and K. Sullivan. Finding anomalies with generative adversarial networks for a patrolbot. In *2017 IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pages 484–485. IEEE, 2017.

[11] D. Tarapore, J. Timmis, and A. L. Christensen. Fault detection in a swarm of physical robots based on behavioral outlier detection. *IEEE Transactions on Robotics*, 35(6):1516–1522, 2019.

[12] Jean-Paul A Yaacoub, Hassan N Noura, Ola Salman, and Ali Chehab. Robotics cyber security: Vulnerabilities, attacks, countermeasures, and recommendations. *International Journal of Information Security*, pages 1–44, 2022.

[13] Bas GB Stottelaar. Practical cyber-attacks on autonomous vehicles. Master's thesis, University of Twente, 2015.

[14] Andrea Castellani, Sebastian Schmitt, and Stefano Squartini. Real-world anomaly detection by using digital twin systems and weakly supervised learning. *IEEE Transactions on Industrial Informatics*, 17(7):4733–4742, 2021.

[15] Hongjun Choi, Sayali Kate, Yousra Aafer, Xiangyu Zhang, and Dongyan Xu. Software-based realtime recovery from sensor attacks on robotic vehicles. In *RAID*, pages 349–364, 2020.

[16] Pinyao Guo, Hunmin Kim, Nurali Virani, Jun Xu, Minghui Zhu, and Peng Liu. Roboads: Anomaly detection against sensor and actuator misbehaviors in mobile robots. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 574–585, 2018.

[17] Naomi S Altman. An introduction to kernel and nearest-neighbor nonparametric regression. *The American Statistician*, 46(3):175–185, 1992.

[18] Corinna Cortes and Vladimir Vapnik. Support-vector networks. *Machine learning*, 20(3):273–297, 1995.

[19] Bernhard Schölkopf and Alexander J Smola. Learning with kernels: support vector machines, regularization, optimization, and beyond. 2001.

[20] Carl Edward Rasmussen and Christopher KI Williams. *Gaussian processes for machine learning*, volume 1. MIT press Cambridge, 2006.

[21] J. Ross Quinlan. Induction of decision trees. *Machine learning*, 1(1):81–106, 1986.

[22] Leo Breiman. Random forests. *Machine learning*, 45(1):5–32, 2001.

[23] Ian Goodfellow, Yoshua Bengio, and Aaron Courville. *Deep learning*. MIT press, 2016.

[24] Geoffrey McLachlan. *Discriminant analysis and statistical pattern recognition*. John Wiley & Sons, 2004.