CSCI 6650 – Intelligent Agents
Midterm Report on Project Proposal
Title: Detection of Anomalous Behavior in Robot Systems using Machine Learning

Members: Sharmin Aktar (saktar@uno.edu), 2581728
Mahfuzul Nissan (minissan@uno.edu), 2599243

1 Introduction and Motivation

The use of robotic systems in various industries has grown rapidly, and it has led to tremendous improvements in productivity and efficiency. However, ensuring the safe and reliable operation of these systems is of utmost importance to prevent potential disasters and ensure the well-being of humans. Despite the best design and engineering practices, robotic systems can malfunction, leading to potential safety risks. For instance, a malfunctioning surgical robot can result in severe injuries to a patient, while a self-driving car malfunction can lead to fatal accidents. Therefore, researchers and engineers are working tirelessly to develop new methods to improve the safety and reliability of these systems. This includes using advanced control techniques, safety sensors, and machine learning algorithms to detect and prevent potential anomalies in the system's behavior. By doing so, we can continue to benefit from the advancements of robotic systems while ensuring the safety of the individuals who interact with them.

In this context, machine learning techniques such as autoencoders have shown effectiveness in detecting anomalous behavior[3]. Autoencoders can learn a compressed representation of the system's normal behavior and use it to identify deviations from the normal one. In this project, we plan to explore the use of autoencoders for detecting anomalous behavior in robotic systems based on system logs, which can provide valuable information for diagnosing and addressing system anomalies. The evaluation of their performance using various metrics will provide insight into the effectiveness of this approach and its potential for improving the security and reliability of robotic systems.

2 Objective

The objective of this project is to develop a machine learning-based approach for detecting anomalous behavior in robotic systems using autoencoders. Specifically, we aim to:

- Develop an autoencoder-based approach for detecting anomalous behavior in robotic systems.
- Formulate the problem of anomaly detection in robotic systems as a binary classification problem using system logs or image data.
- Create a context-specific data set for normal behavior in robotic systems, using a defined path planning algorithm.
- Create a context-specific data set for abnormal behavior in robotic systems, by introducing deviations from the normal behavior path planning algorithm.
- Evaluate the performance of the autoencoder-based method for anomaly detection in robotic systems using the normal and abnormal behavior data sets.

3 Related Work

Ji et al. [1] proposed a new approach for detecting anomalous behaviors in robot navigation by predicting the probability of future failure based on planned motions and current observations. They introduced a new framework called **PAAD** for proactive anomaly detection in uncertain environments that combines multi-sensor fusion and deep learning techniques.

Olivato et al. [2] proposed a solution for identifying cyber-physical attacks on an autonomous robotic boat used for water quality monitoring. Their approach is based on analyzing system logs and developing an analyzer module using autoencoders to detect abnormal behaviors in real-time. The system logs, recorded at short time intervals, provide valuable data on the system's behavior, and a transformation process is used to convert the log data into a binary pixel array, which is a sparser and more effective representation for learning specific patterns of normal and abnormal behaviors.

4 Problem Statement

Consider a robotic system S with an internal state characterized by a set of variables V, which can be accessed over time. Let $\boldsymbol{r}_t$ be a record, i.e., a tuple of values of such variables collected at time t, and let $\mathcal{L}$ be a system log of a behavior containing the values $\boldsymbol{r}_1, \boldsymbol{r}_2, \ldots, \boldsymbol{r}_T$ of variables recorded from time to time. We denote $\mathcal{L}$ as the set of all possible logs, with R being the set of all possible records.

Let us consider a scenario where such logs are taken when the system is performing a nominal (correct) behavior. The problem we address in this paper is one-class classification of system logs, which can be expressed as follows: Given a dataset of system logs capturing the nominal behavior of the system, i.e., $D_{\text{normal}} = \mathcal{L}_1, \mathcal{L}_2, \ldots, \mathcal{L}_n$, generate a class model that will be able to classify new instances as normal or abnormal. Formally, the problem can be stated as finding a function $f : R \to 0, 1$, where $f(\boldsymbol{r}) = 0$ if $\boldsymbol{r}$ is normal and $f(\boldsymbol{r}) = 1$ otherwise.

Anomaly detection in robotic systems is crucial for ensuring safety and reliability. The ability to accurately detect and classify abnormal behavior can prevent catastrophic failures and minimize downtime. Our proposed approach aims to address the challenges of anomaly detection in robotic systems using a one-class classification framework.

5 Challenges

Detecting anomalous behavior in robotic systems using machine learning poses several challenges. Here are some of them:

- The internal state of a robotic system may be high-dimensional and complex, making it difficult to identify the relevant features for anomaly detection.
- The system may exhibit different types of anomalies, such as abrupt changes, drifts, and oscillations, which require different detection strategies.
- The training data may be limited or noisy, leading to overfitting or poor generalization performance.
- The system may be subject to environmental disturbances or external factors, which can affect its behavior and make it harder to distinguish between normal and anomalous operation.
- The choice of machine learning algorithm and architecture would depend on the specific application and requirements of the robotic system.

To make our project simpler, we will consider a specific context: a robot executing a simple path planning algorithm in a simulated environment using CoppeliaSim. In this scenario, the robot's task is to follow a predefined path, and deviations from this path will be considered as anomalous behavior. By simplifying the problem, we can focus on implementing and optimizing the autoencoder-based anomaly detection system while avoiding the complexities of real-world robotic systems. However, the insights and techniques learned in this project can be applied to more complex systems in the future.

6 Proposed Methodology

The proposed methodology for detecting anomalous behavior in a mobile robot system involves the use of autoencoder models trained on sensor data generated during the robot's operation. The following steps will be taken to achieve this goal:

1. Define a set of criteria for normal robot behavior, which will be based on the expected behavior of the robot when it is following a predefined path in a simulated environment. The path will be generated using a path-planning algorithm such as A*/Dijkstra, and the simulated environment will be the CoppeliaSim robotics simulator.

2. Train an autoencoder model on a dataset of sensor data generated by the robot during its normal operation. The autoencoder model will learn to reconstruct the input data and will be optimized to minimize the difference between the input and the reconstructed data.

3. During the testing phase, use the trained autoencoder model to detect anomalous behavior by comparing the reconstruction error between the input data and the reconstructed data to a predetermined threshold. Anomalous behavior will be identified when the reconstruction error exceeds this threshold.

4. Evaluate the performance of the autoencoder-based approach for detecting anomalous behavior.

The anomalous behavior that will be tested in the simulated environment will include deviations from the predefined path, collisions with obstacles, and unexpected sensor readings. The performance of the autoencoder model will be evaluated in terms of its ability to accurately detect these anomalous behaviors while minimizing false positives.

References

[1] T. Ji, A. N. Sivakumar, G. Chowdhary and K. Driggs-Campbell, "Proactive Anomaly Detection for Robot Navigation With Multi-Sensor Fusion" in IEEE Robotics and Automation Letters, vol. 7, no. 2, pp. 4975-4982, April 2022, doi: 10.1109/LRA.2022.3153989.

[2] M. Olivato, O. Cotugno, L. Brigato, D. Bloisi, A. Farinelli and L. Iocchi, "A Comparative Analysis on the use of Autoencoders for Robot Security Anomaly Detection," 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), Macau, China, 2019, pp. 984-989, doi: 10.1109/IROS40897.2019.8968105.

[3] Z. Chen, C. K. Yeo, B. S. Lee and C. T. Lau, "Autoencoder-based network anomaly detection," 2018 Wireless Telecommunications Symposium (WTS), Phoenix, AZ, USA, 2018, pp. 1-5, doi: 10.1109/WTS.2018.8363930.