Arming IDS Researchers with a Robotic Arm Dataset

Arpan Gujarati, Zainab Saeed Wattoo, Maryam Raiyat Aliabadi, Sean Clark, Xiaoman Liu,
Parisa Shiri, Amee Trivedi, Ruizhe Zhu, Jason Hein, and Margo Seltzer

University of British Columbia (UBC), Vancouver, Canada

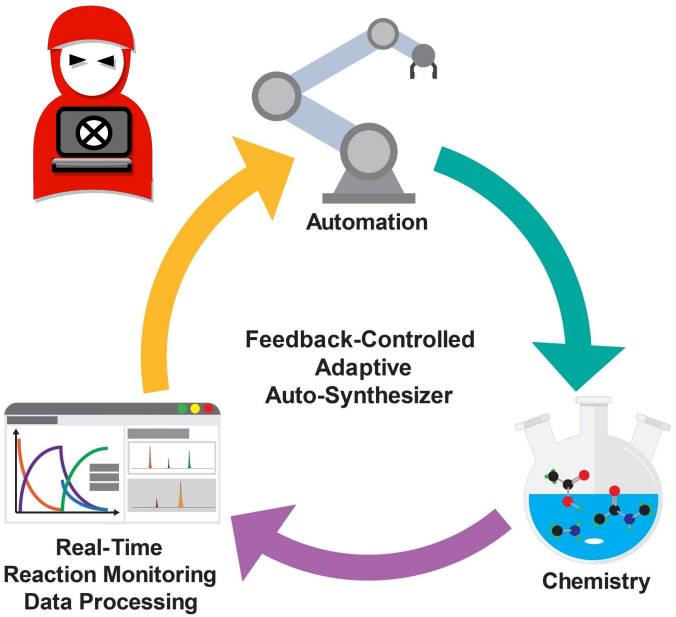
Self-driving laboratories are at the core of Industry 4.0

What are self-driving laboratories?

- Fully automated labs without humans in the loop
- Goal: Reduce the cost and time for autonomous discoveries
- Tools & Technologies: Robotic arms, smart devices, and AI

Problem

- Networked components are vulnerable to security attacks
- Security attacks can lead to catastrophic outcomes
  - Robot arms can be misconfigured to break expensive equipment
  - Hazardous materials in the vicinity can be misused to cause explosions



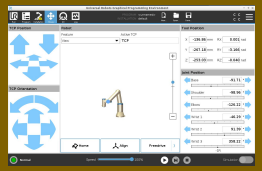
Requirements

Large Datasets and High-Quality, Domain-Specific Benchmarks

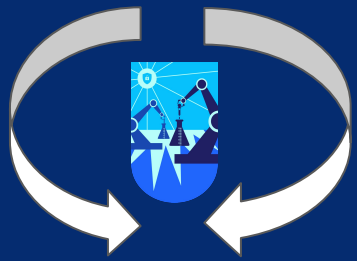
AURSAD by Leporowski et al. (2021)

- Simple automated screw-driving operations

Robot Arm Simulators



Securing Self-Driving Laboratories



Design and Develop Intrusion Detection System (IDS)

Gap: Existing datasets do not apply to real-world scenarios

- Real-world scenarios are more complex, use heterogeneous devices, and consisting of long procedures

Requirements

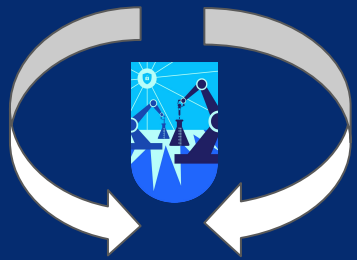
Large Datasets and High-Quality,
Domain-Specific Benchmarks

This Work

Generating and understanding **datasets** from real-world workloads

In collaboration with **Hein Lab**, a state-of-the-art lab that blends **advanced robotics** with **synthetic organic chemistry**

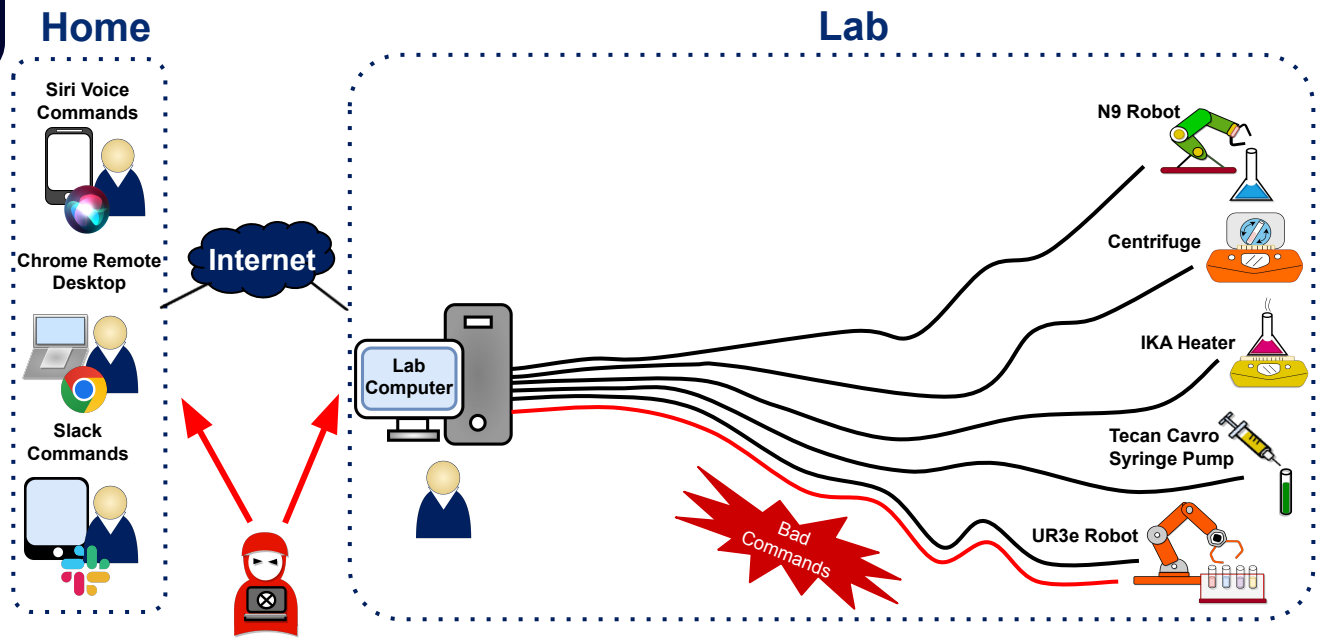
Securing Self-Driving Laboratories



Design and Develop
Intrusion Detection System (IDS)

Hein Lab: A self-driving laboratory at UBC Chemistry

"Accelerating the rate of research and discovery by integrating these instruments with autonomous robotics to develop self-driving laboratories."



Requirements

Large Datasets and High-Quality, Domain-Specific Benchmarks

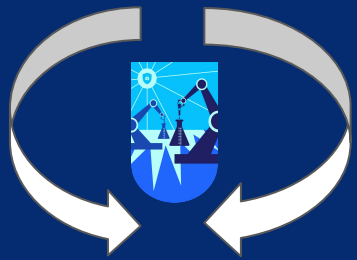
This Work

Robotic Arm Tracer (RATracer)

Robotic Arm Dataset (RAD)

Preliminary Analyses

Securing Self-Driving Laboratories



Design and Develop Intrusion Detection System (IDS)

Requirements

Large Datasets and High-Quality, Domain-Specific Benchmarks

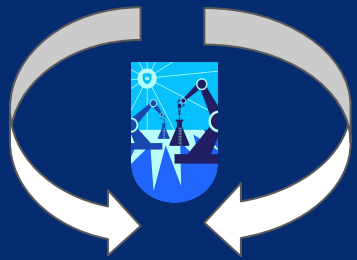
This Work

Robotic Arm Tracer (RATracer)

Robotic Arm Dataset (RAD)

Preliminary Analyses

Securing Self-Driving Laboratories



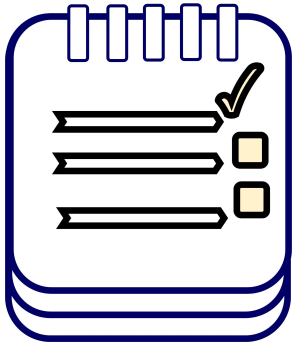
Design and Develop Intrusion Detection System (IDS)

RATracer

Design Goals

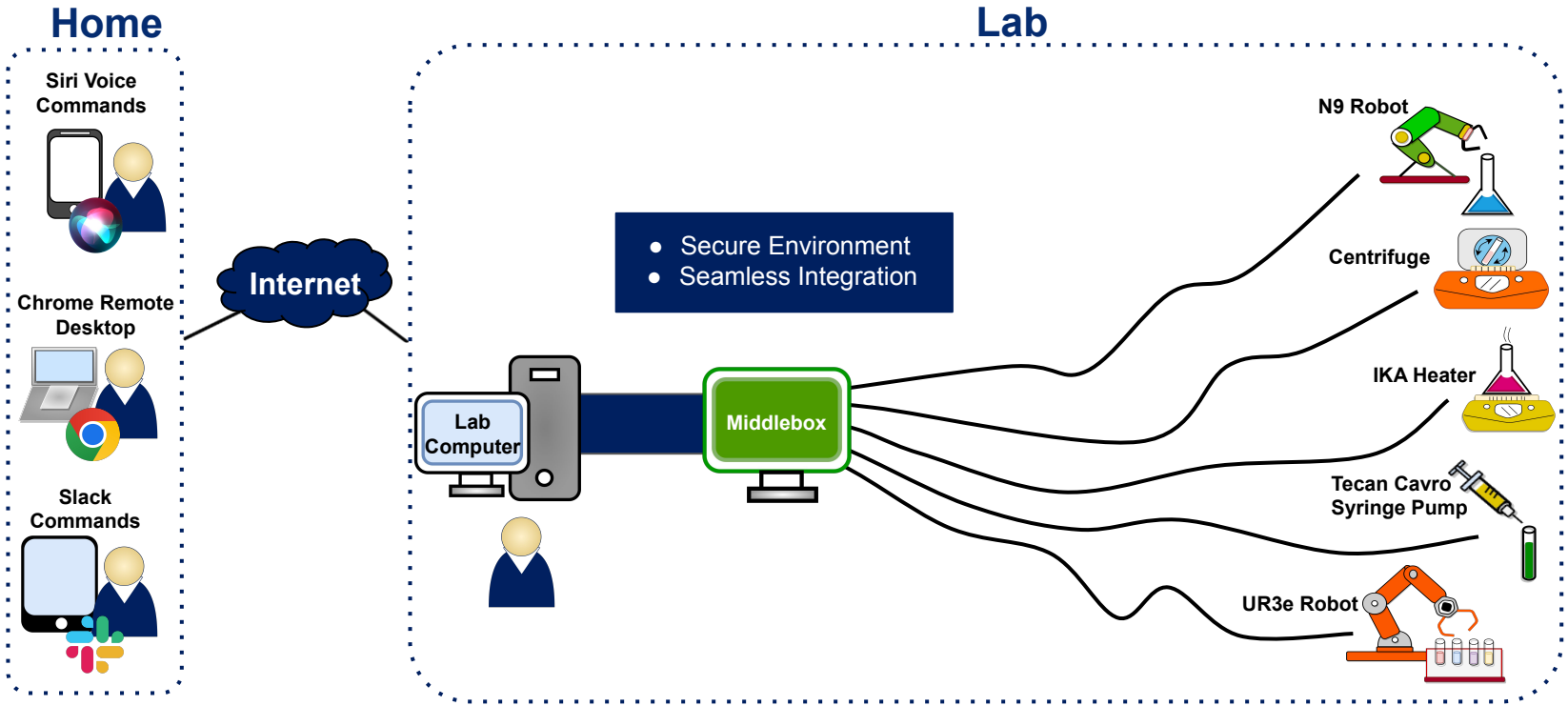
Intercept and trace all communication between CPS devices and experiment scripts

1. **Non-Intrusive:** Not interfering with the workflow
2. **Extensible:** Seamless extension to accommodate other devices
3. **Programmer Friendly:** Minimal modification in the experiment code
4. **Minimal Performance Overhead:** Response time of the tracer to be minimal



RATracer

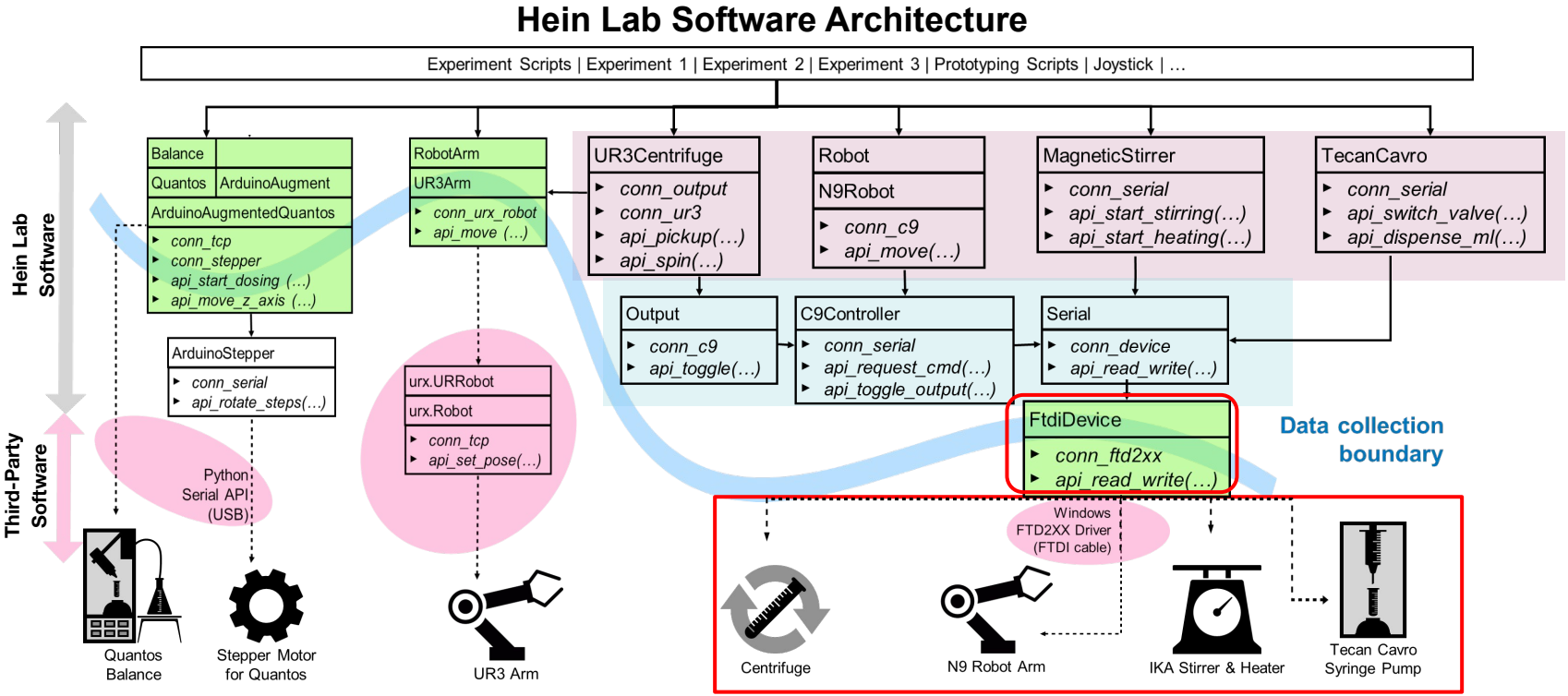
1. **Non-Intrusive**



RATracer

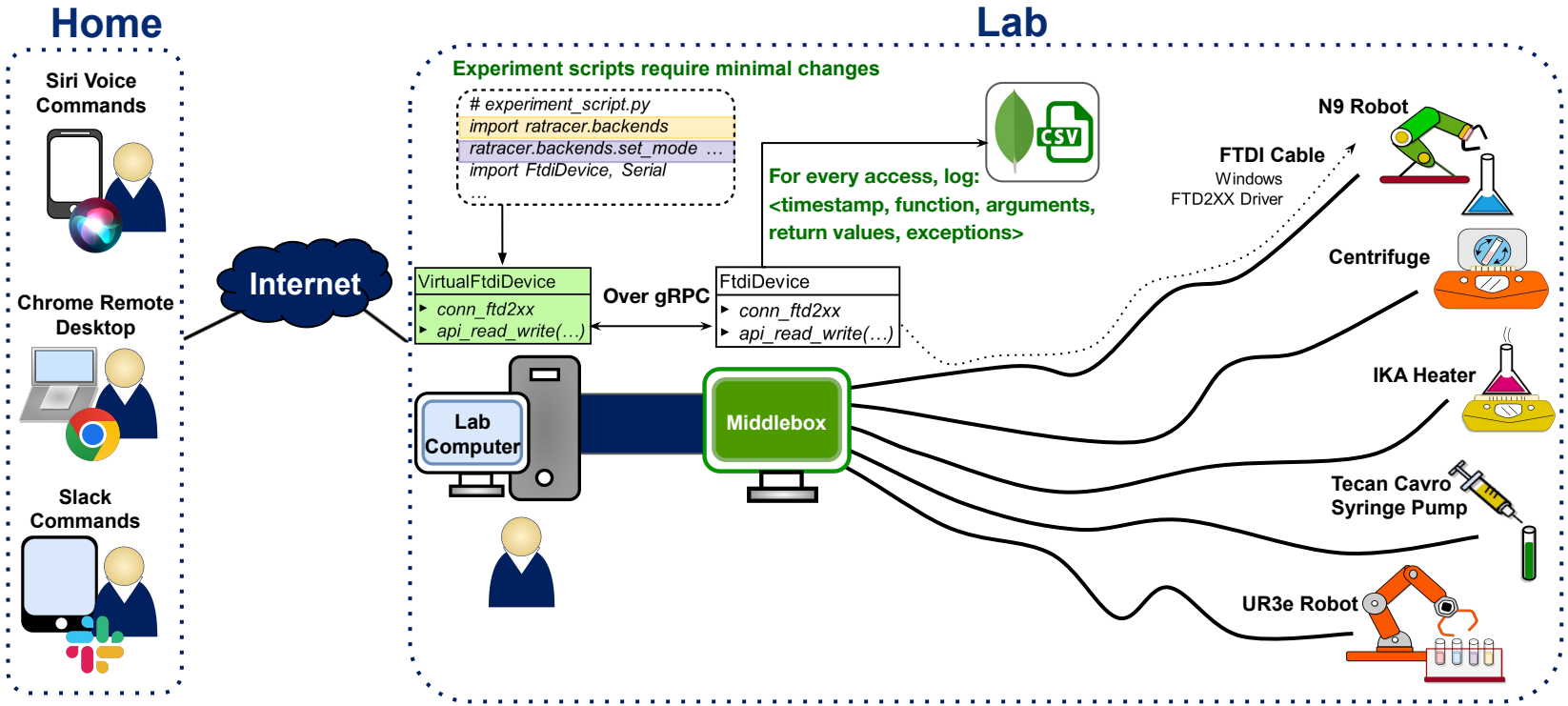
Takeaways:
- Generic class that is used by many different devices
- Easy to reproduce the device commands

2. Extensible



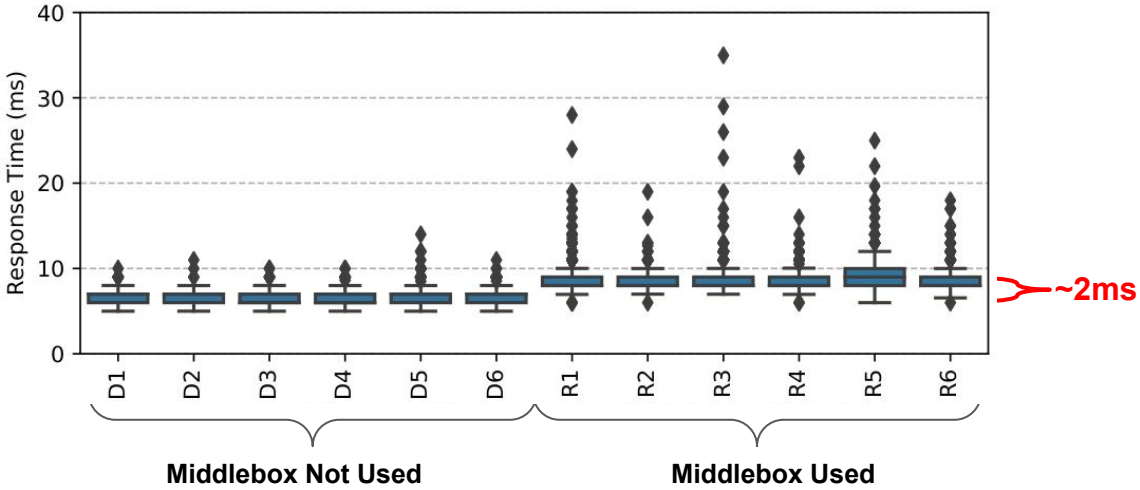
RATracer

3. Programmer Friendly



RATracer

4. Minimal Performance Overhead



Results: Middlebox increases latency by ~2ms

Requirements

Large Datasets and High-Quality, Domain-Specific Benchmarks

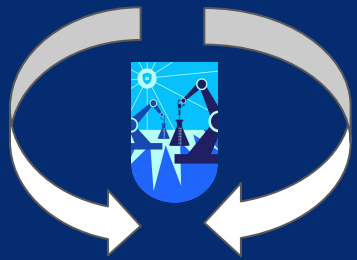
This Work

Robotic Arm Tracer (RATracer)

Robotic Arm Dataset (RAD)

Preliminary Analyses

Securing Self-Driving Laboratories



Design and Develop Intrusion Detection System (IDS)

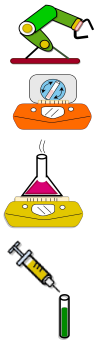
Robotic Arm Dataset (RAD)

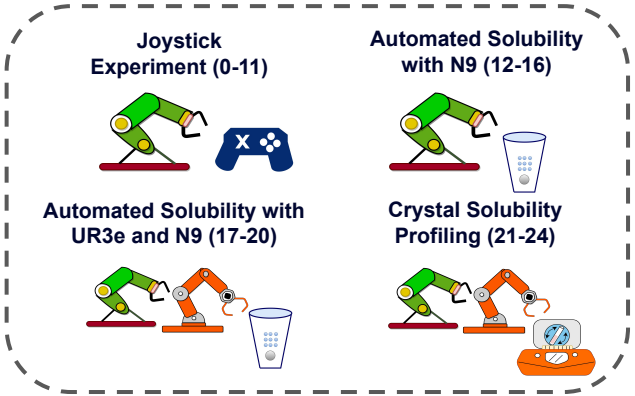
1. **Command Dataset:** Data collected from intercepting the Hein Lab's software stack
2. **Power Dataset:** Power monitoring data collected directly from UR3e Robot Arm

Robotic Arm Dataset (RAD)

1. Command Dataset

Commands	Arguments	Responses	Exceptions
move_arm	Location: 1,2,3,4,5,6	None	None
run_centrifuge	Duration: 300s	None	None
read_temperature	None	20	None
dispense_liquid	Volume: 10	None	None
. . .	. . .		





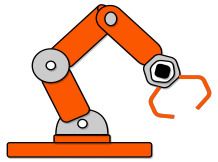
25 Supervised Experiments

Time Period: Three Months
Number of Command Instances: 128,785
Number of Command Types: 52

Robotic Arm Dataset (RAD)

2. Power Dataset

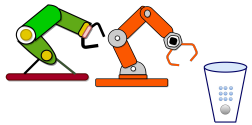
Joint_Current_1	Joint_Current_2	Joint_Current_3	Joint_Current_4
10	11	54	23
20	33	12	43
30	12	31	11
. . .	. . .	. . .	. . .



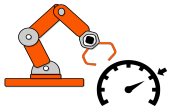
UR3e's real-time monitoring API

Collected after Time Duration: 40ms
Number of Entries: More than 40 million
Number of Physical Properties: 122

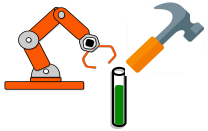
Automated Solubility with UR3e and N9 (17-20)



UR3e Movements with Different Velocities



UR3e Movement with Different Payload Weights



Requirements

Large Datasets and High-Quality, Domain-Specific Benchmarks

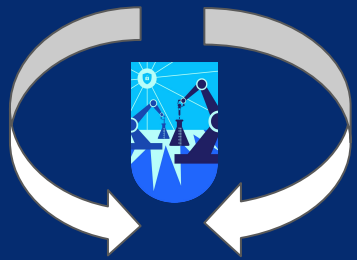
This Work

Robotic Arm Tracer (RATracer)

Robotic Arm Dataset (RAD)

Preliminary Analyses

Securing Self-Driving Laboratories



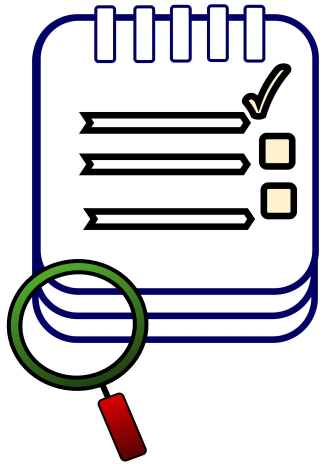
Design and Develop Intrusion Detection System (IDS)

Analyses

Objectives

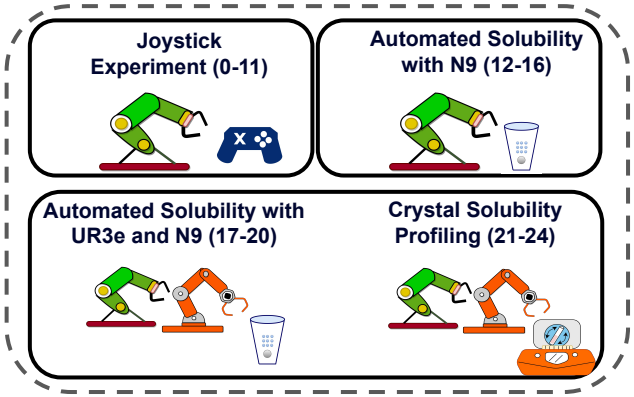
Goal: find underlying patterns in the dataset that can help design domain-specific IDS

1. Can we identify the experiment being run?
2. Can we identify unexpected variations within the experiment?
3. Can power dataset substitute command dataset?

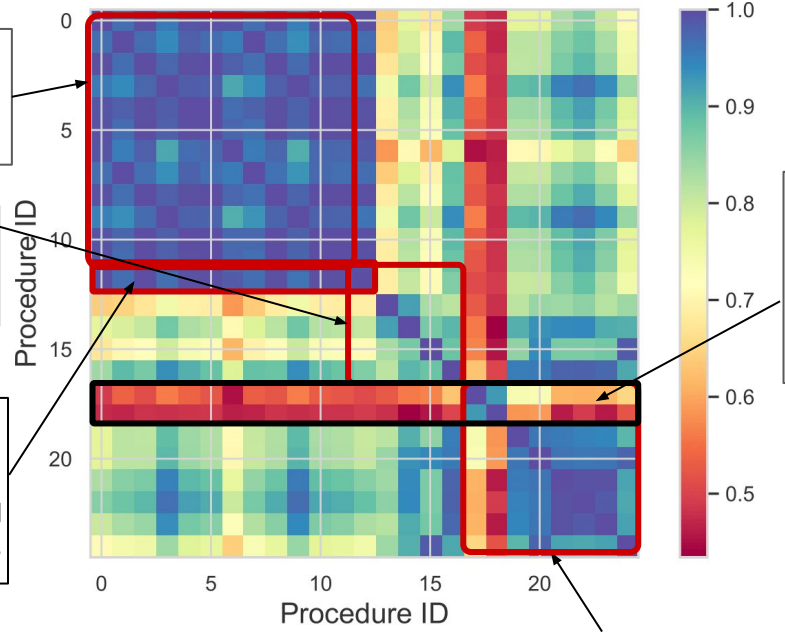


Analyses

1. Can we identify the experiment being run?



Term-Frequency - Inverse Document Frequency (TF-IDF)



1) All joystick experiments are similar.

2) Exp 12-16 are all moderately similar.

3) Exp 12 is most similar to joystick as operator used joystick at the end of the experiment.

5) Exp 17 and 18 were stopped midway showing a red region.

4) Exp 17-24 are all solubility experiments and are similar to each other as all experiments use two robots.

Results: Able to distinguish
- one experiment from another
- different devices

Analyses

2. Can we identify the unexpected variations within experiment?

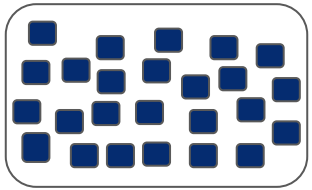
Variation in the command sequences.

N-gram models: distribution of sequences of N consecutive commands

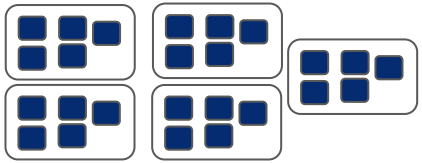
N: 2,3,4

Likelihood of command sequence

Anomalies have less likelihood



25 Supervised Experiments
(3 Anomalies)



5 fold cross-validation

High Recall (*true positives/ (true positives + false negatives)*)

- Model accurately identifies all anomalies

Metrics	Bigram	Trigram	Four-gram
True positives (negatives)	3 (13)	3 (18)	3 (17)
False positives (negatives)	9 (0)	4 (0)	5 (0)

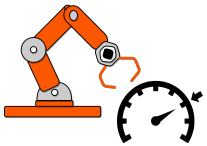
False positives decreases from bigram to trigram but moving to four-gram does not help

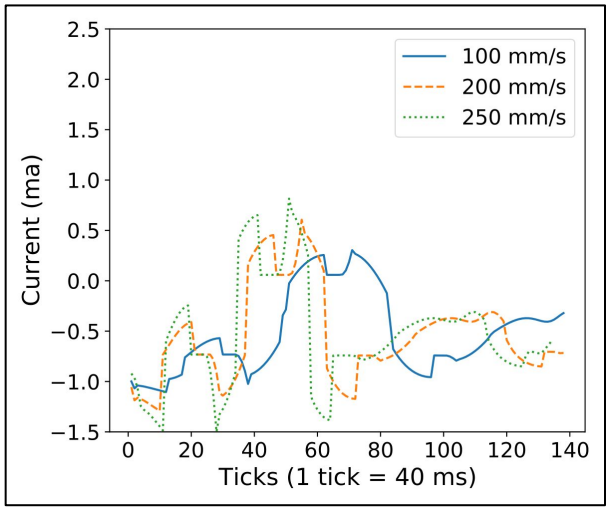
- Choosing an ideal model size is nontrivial
- Larger and varied supervised dataset might help

Analyses

3. Can power dataset substitute command dataset?

UR3e Movements with Different Velocities





Results:

- Traces are similar in shape
- 100mm/s line is stretched compared to others

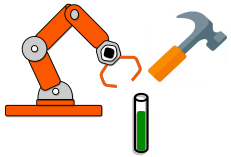
Takeaway:

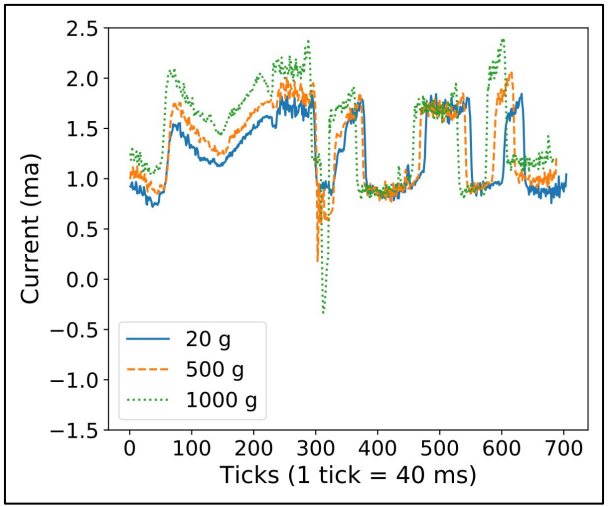
- Power dataset can be used to derive parameters such as velocity without the need for tracing

Analyses

3. Can power dataset substitute command dataset?

UR3e Movements with Different Payload Weights





Results:

- Traces are similar in shape
- 1000g draws more current compared to 20g

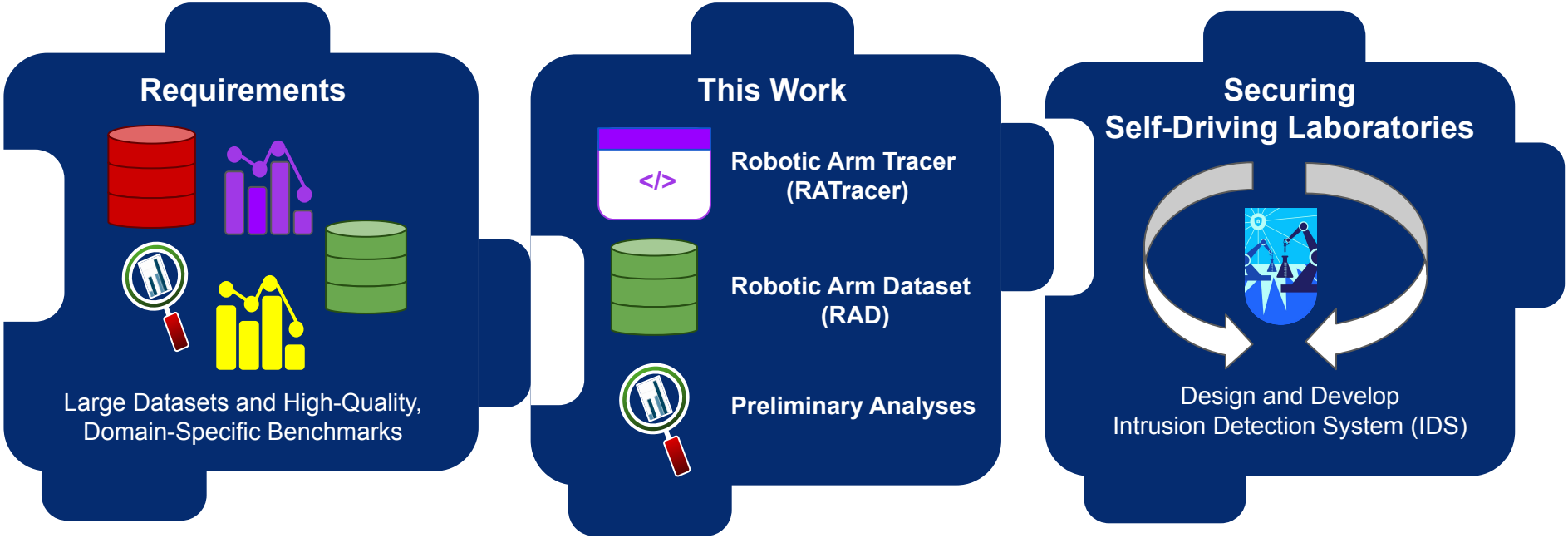
Takeaway:

- Power dataset can be used to collect information that is not captured as part of the command dataset such as payloads

Key Takeaways

- RATracer is **easily extensible** to python-based frameworks
- **Tracing commands** reveal important information about the experiment being run
  - which **can help develop an effective domain-specific IDS**
- In the absence of command data, **side channels like power can be used** instead

Summary



Dataset and code: https://github.com/ubc-systopia/dsn-2022-rad-artifact/