CORGIDS: A Correlation-based Generic Intrusion Detection System

Authors:

Ekta Aggarwal, Mehdi Karimibiuki, Karthik Pattabiraman, and Andre Ivanov

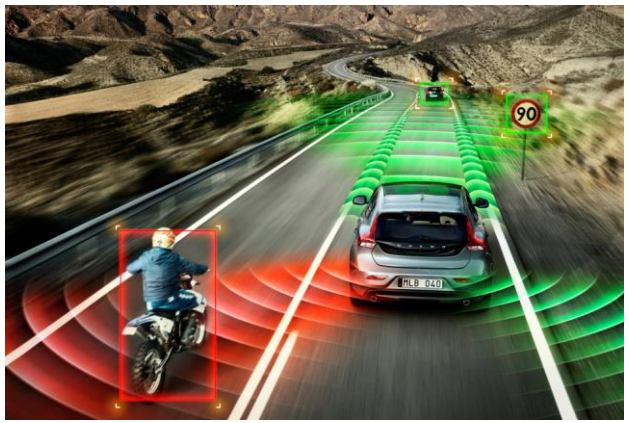
Presented at:

CPS-SPC 2018, Toronto, Canada

October 19, 2018

Introduction

- Cyber-Physical system (CPS) consist of **software** and **physical** components **knitted** together.
- Properties in CPS must **follow laws** of physics.
- **Physical properties** of a drone: altitude, distance travelled, speed, and flight time.



Security attacks in CPS

- The Jeep Hack *(http://illmatics.com/carhacking.html)*
- Hackable Cardiac Devices from St. Jude *(https://medsec.com/stj_expert_witness_report.pdf)*
- TRENDnet Webcam Hack *(https://www.wired.com/2012/02/home-cameras-exposed/)*

Distance Spoofing Attack

Distance Spoofing Attack

Altitude, Distance, Speed, Time
97.9, 600, 4, 42.37

Distance Spoofing Attack

Altitude, Distance,
97.9, 600,

Altitude, Distance, Speed, Time
97.9, 630, 4, 44.37

Distance Spoofing Attack

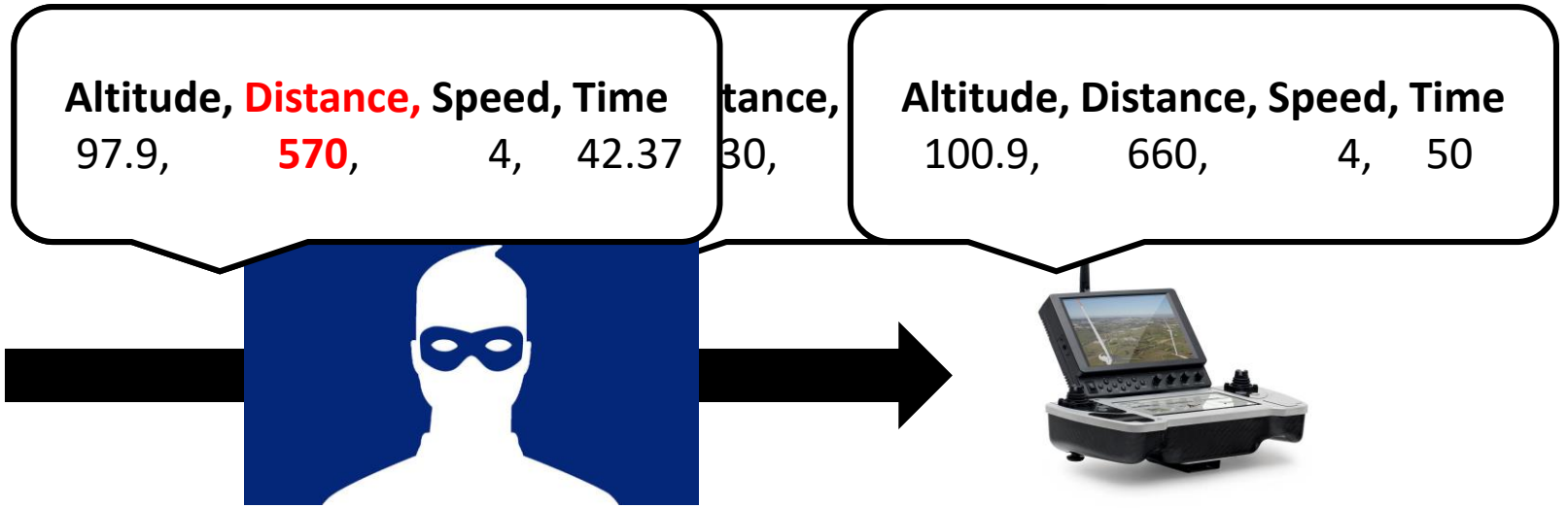
Altitude, Distance,
97.9, 600,

Altitude, Distance,
97.9, 630,

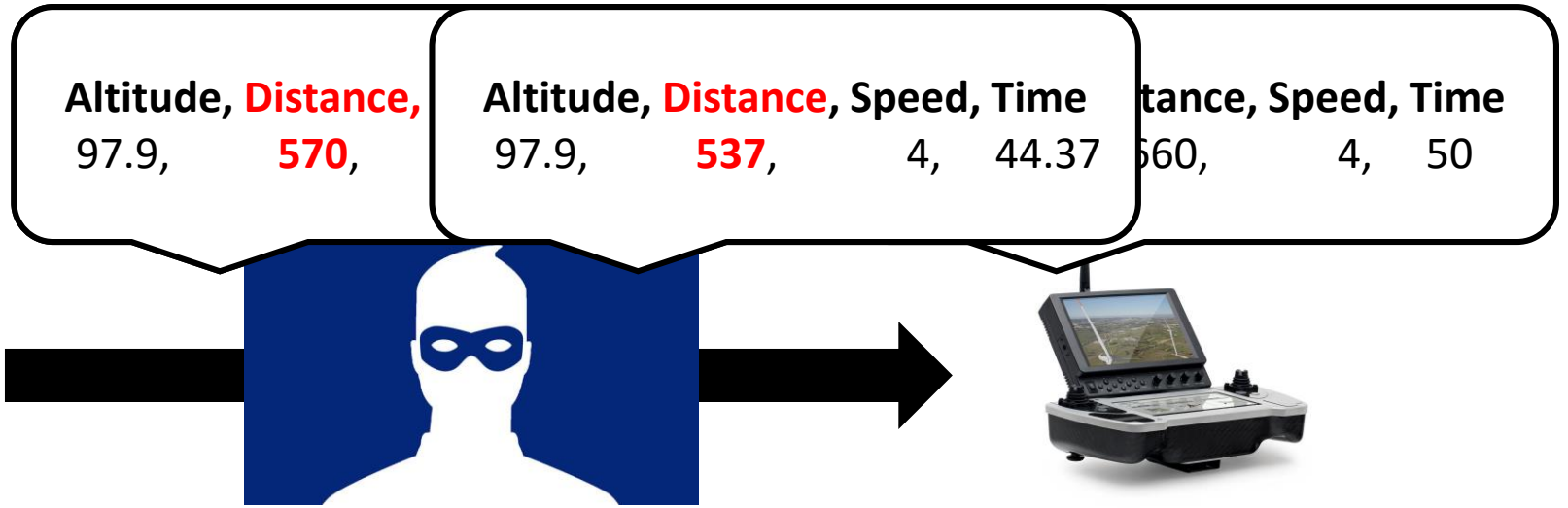
Altitude, Distance, Speed, Time
100.9, 660, 4, 50

Distance Spoofing Attack

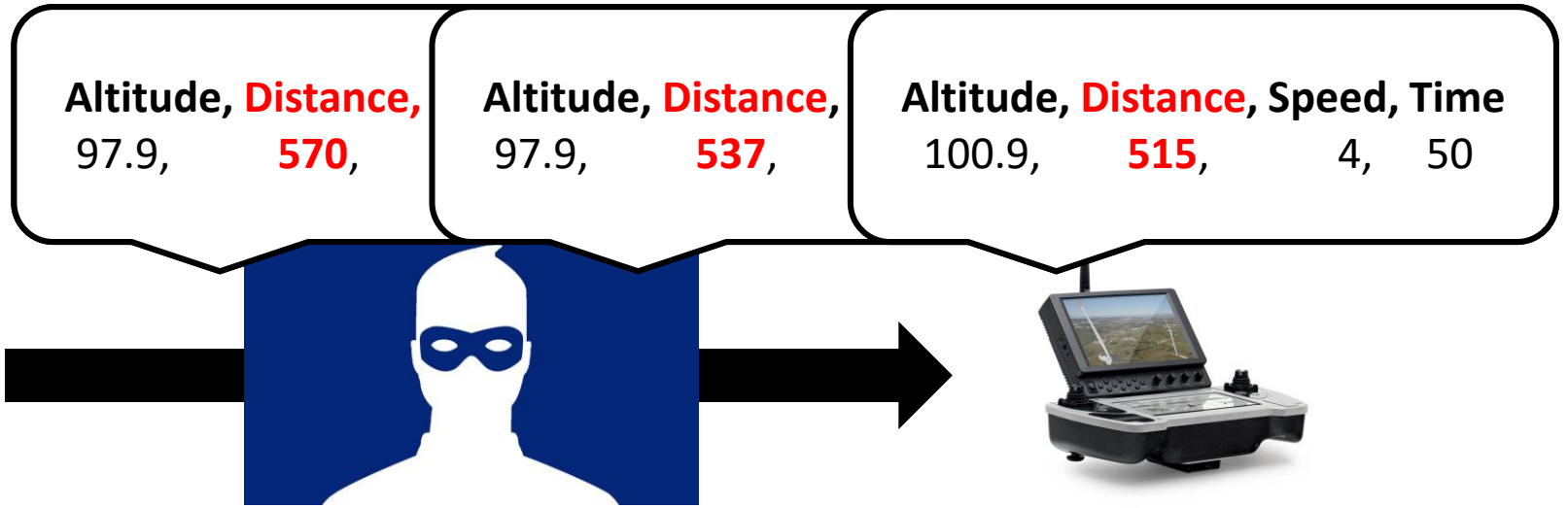
Distance Spoofing Attack



Distance Spoofing Attack

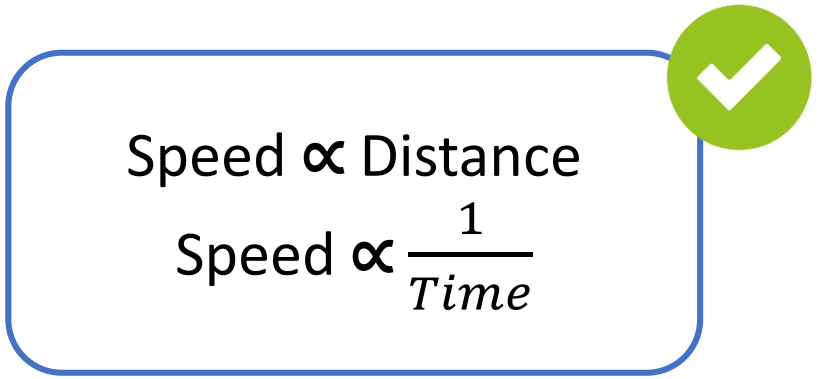


Distance Spoofing Attack

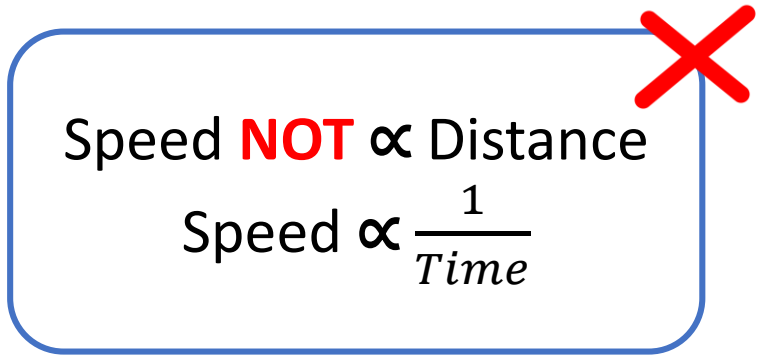


What is an Invariant?

"Something that does not change under a transformation"

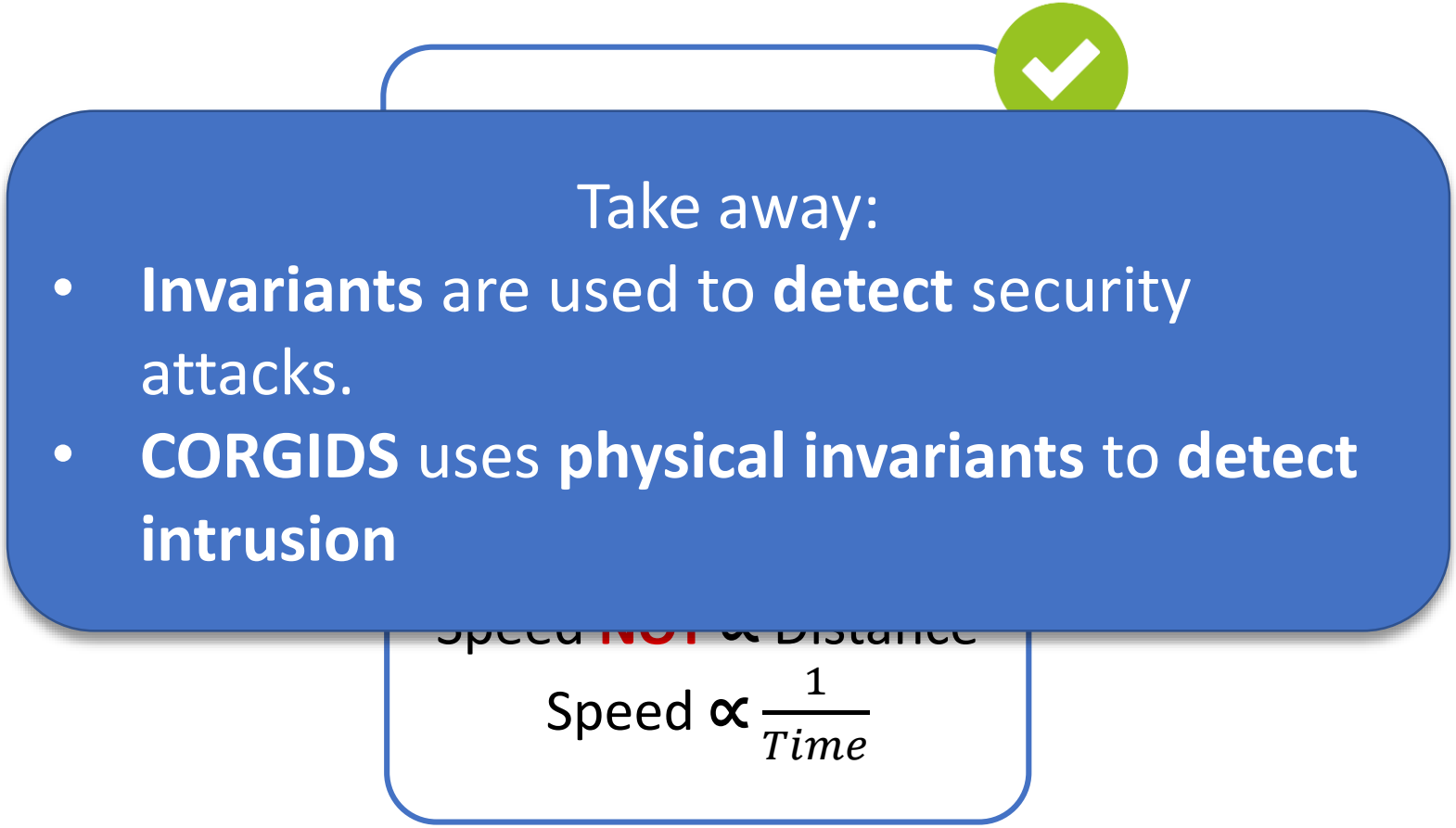


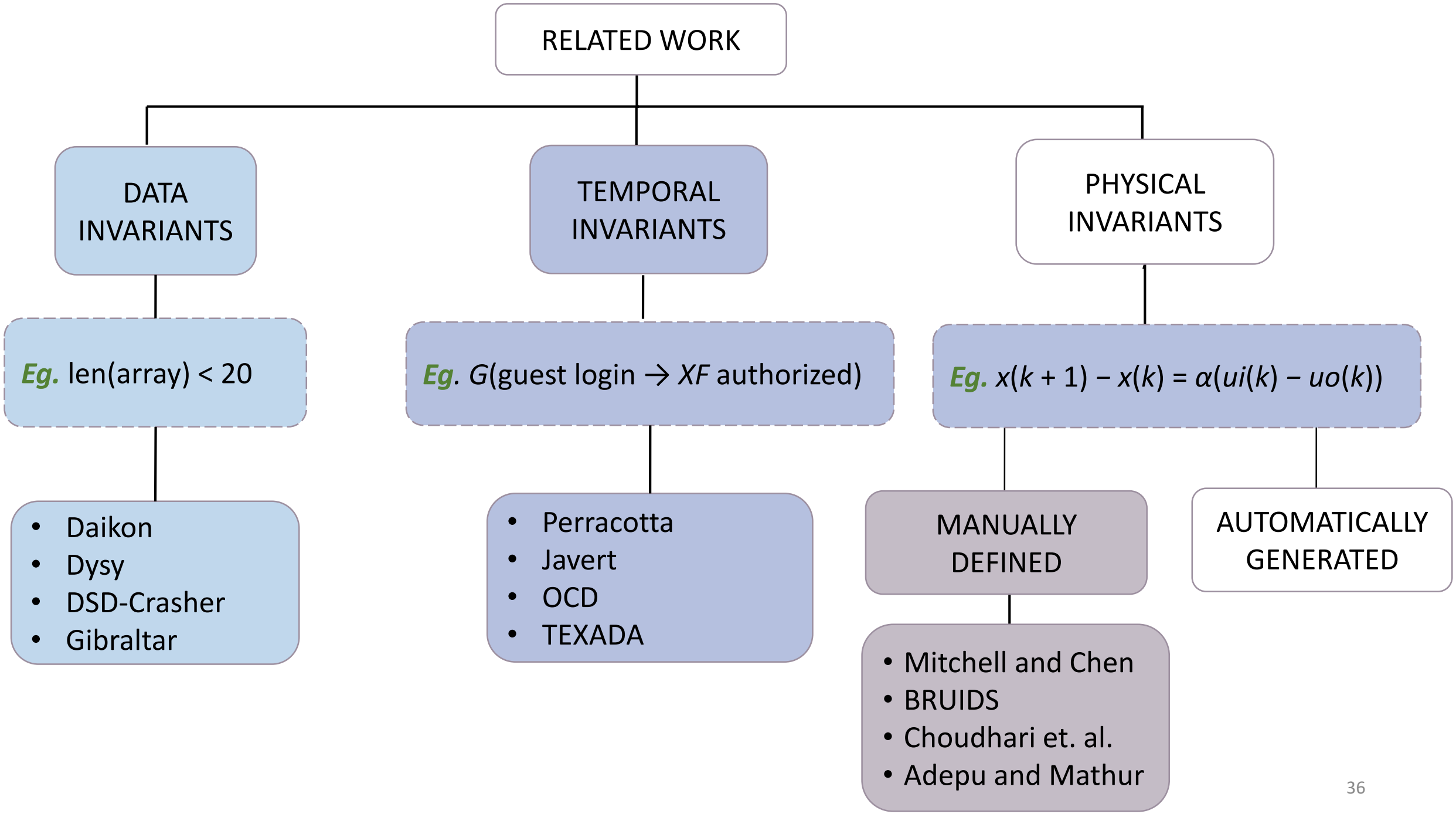
During execution, observation is:



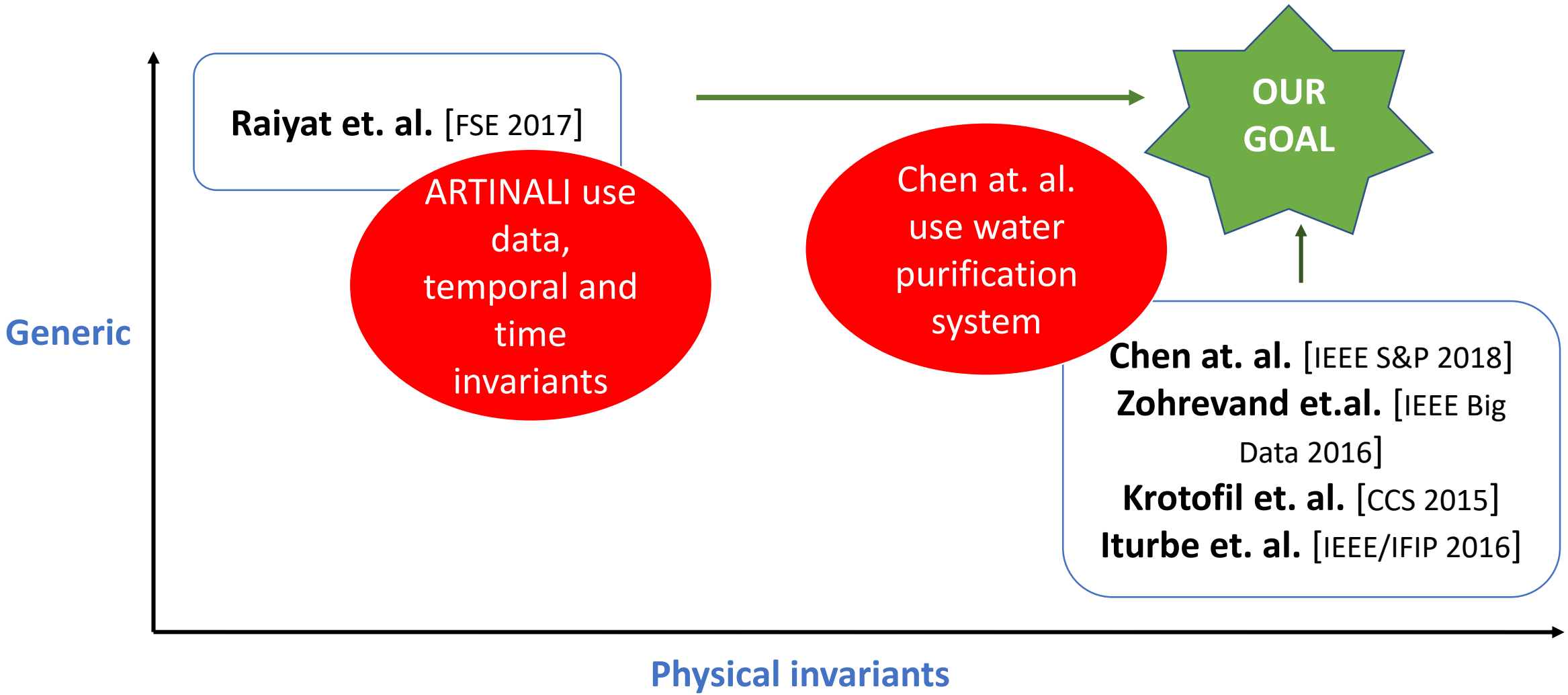
What is an Invariant?

"Something that does not change under a transformation"

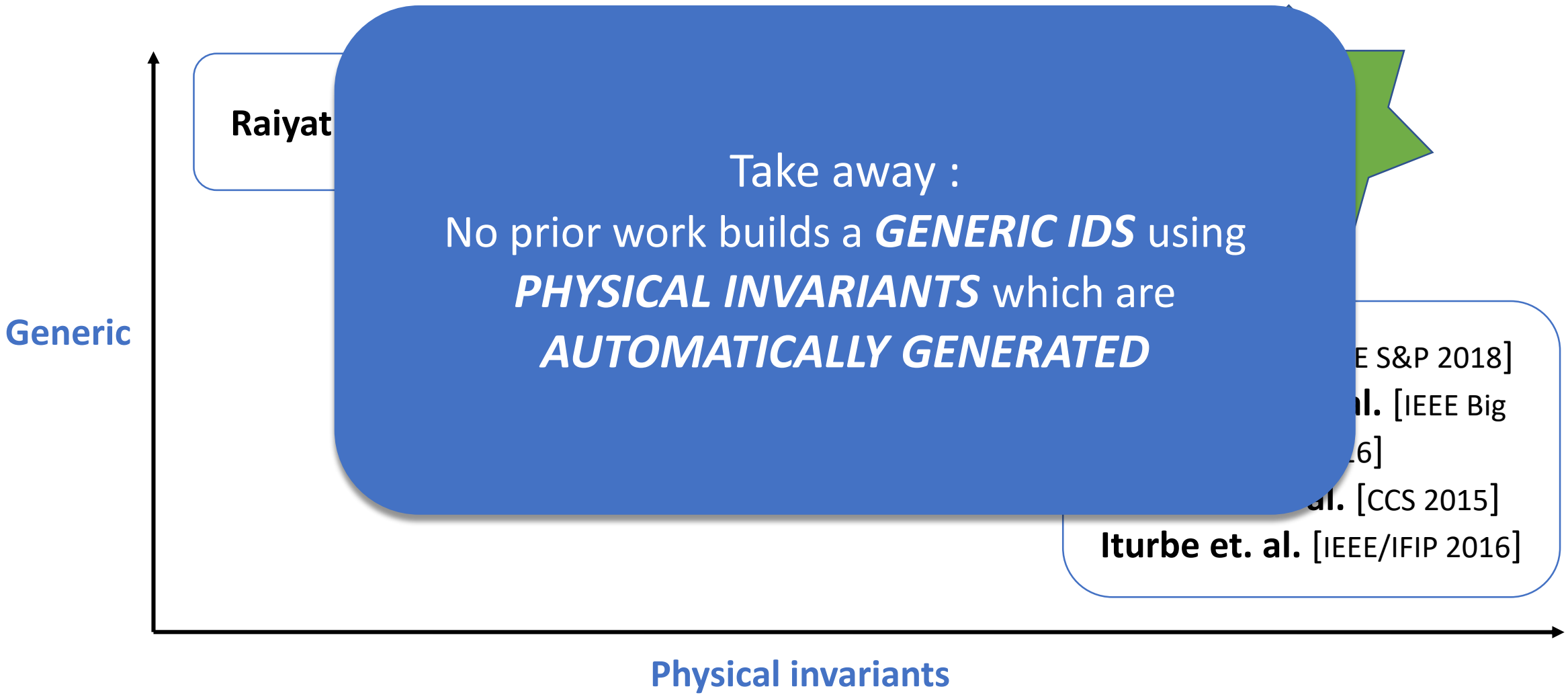



RELATED WORK
DATA INVARIANTS
TEMPORAL INVARIANTS
PHYSICAL INVARIANTS
Eg. len(array) < 20
Eg. G(guest login → XF authorized)
Eg. x(k + 1) − x(k) = α(ui(k) − uo(k))
• Daikon
• Dysy
• DSD-Crasher
• Gibraltar
• Perracotta
• Javert
• OCD
• TEXADA
MANUALLY DEFINED
AUTOMATICALLY GENERATED
• Mitchell and Chen
• BRUIDS
• Choudhari et. al.
• Adepu and Mathur

Automatically Generated Physical Invariants



Automatically Generated Physical Invariants



Contributions

- Use **Hidden Markov Models (HMM)** to infer the logical correlations to **detect intrusions**.
- Design **COR**relation based **G**eneric **I**ntrusion **D**etection **S**ystem **- CORGIDS.**
- Demonstrate CORGIDS on two CPS – an **unmanned aerial vehicle (UAV)** and a **smart artificial pancreas (SAP)**.
- Perform **five targeted attacks** on the CPS.
- CORGIDS is able to **successfully detect** attacks.

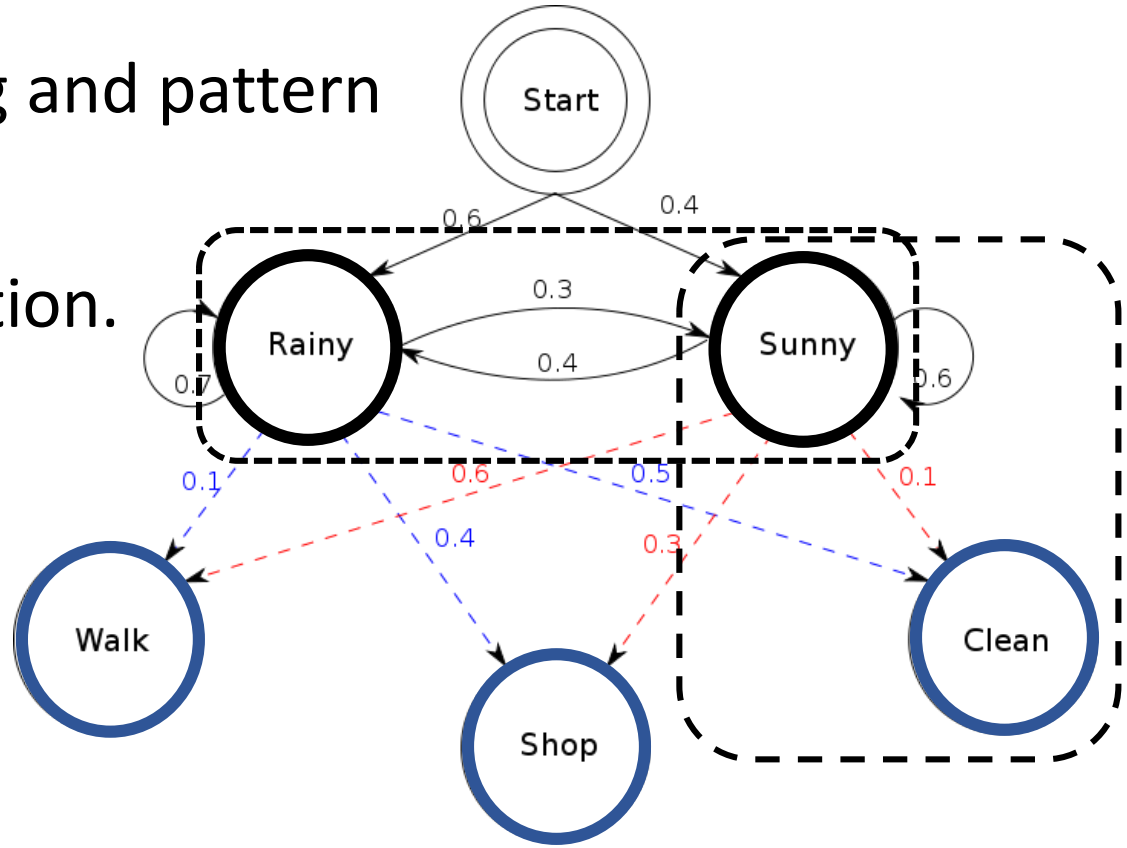
Threat Model

- Capability to **gain read and write access** to the **communication channel** between the system under test (SUT) and controller.
- Has **root access** to the SUT.
- Capable of **spoofing, flooding, tampering, and rebooting.**

Hidden Markov Model (HMM)

Finite model used to **describe probability** distribution over possible sequences of a given system.

Example: Reinforcement learning and pattern recognition such as speech, handwriting and gesture recognition.



Source: https://en.wikipedia.org/wiki/Hidden_Markov_model

An Example:
Hidden states = (“Rainy”, “Sunny”)
Observations = (“Walk”, “Shop”, “Clean”)

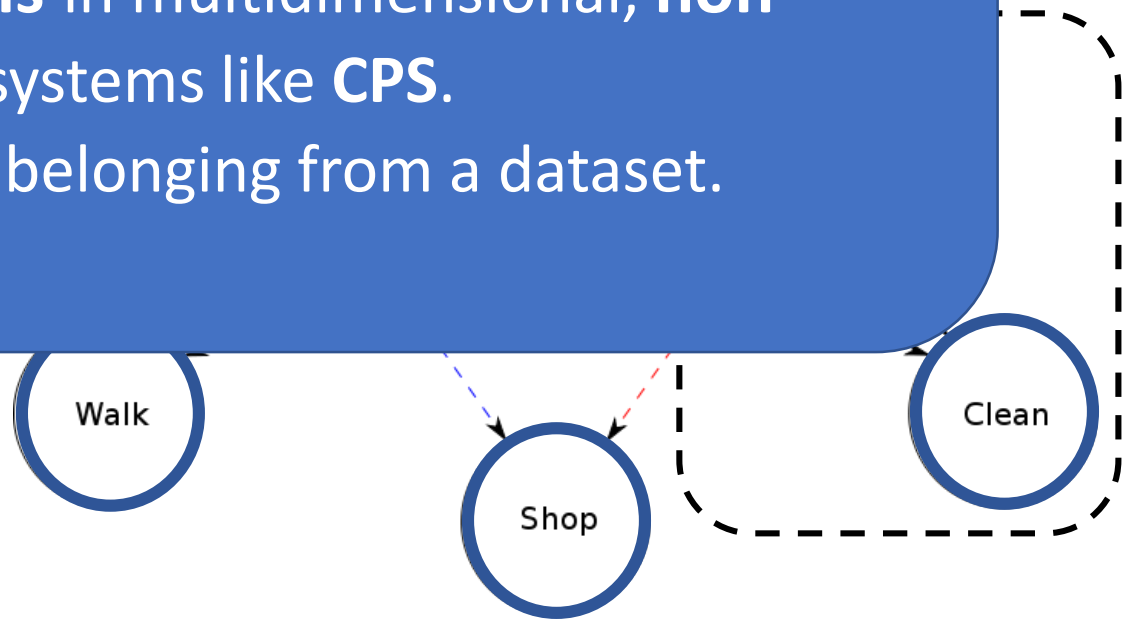
Hidden Markov Model (HMM)

Finite mod… …le
sequence…
Example:
recognitio…
handwriti…

HMM

- **Finding correlations** in multidimensional, **non-linear time series** systems like **CPS**.
- **Likelihood of data** belonging from a dataset.

An Example:
Hidden states = (“Rainy”, “Sunny”)
Observations = (“Walk”, “Shop”, “Clean”)



Source: https://en.wikipedia.org/wiki/Hidden_Markov_model

Work-flow of CORGIDS

1. Logging Phase

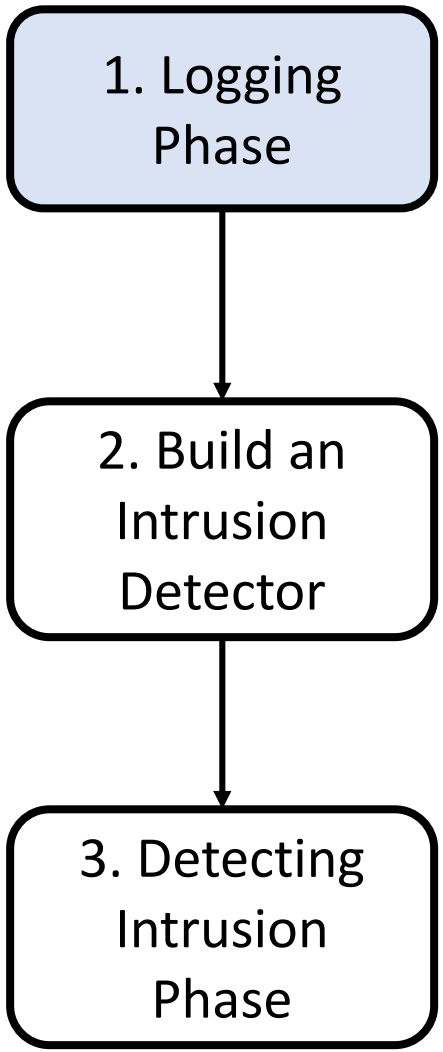
2. Build an Intrusion Detector

3. Detecting Intrusion Phase

Logging module

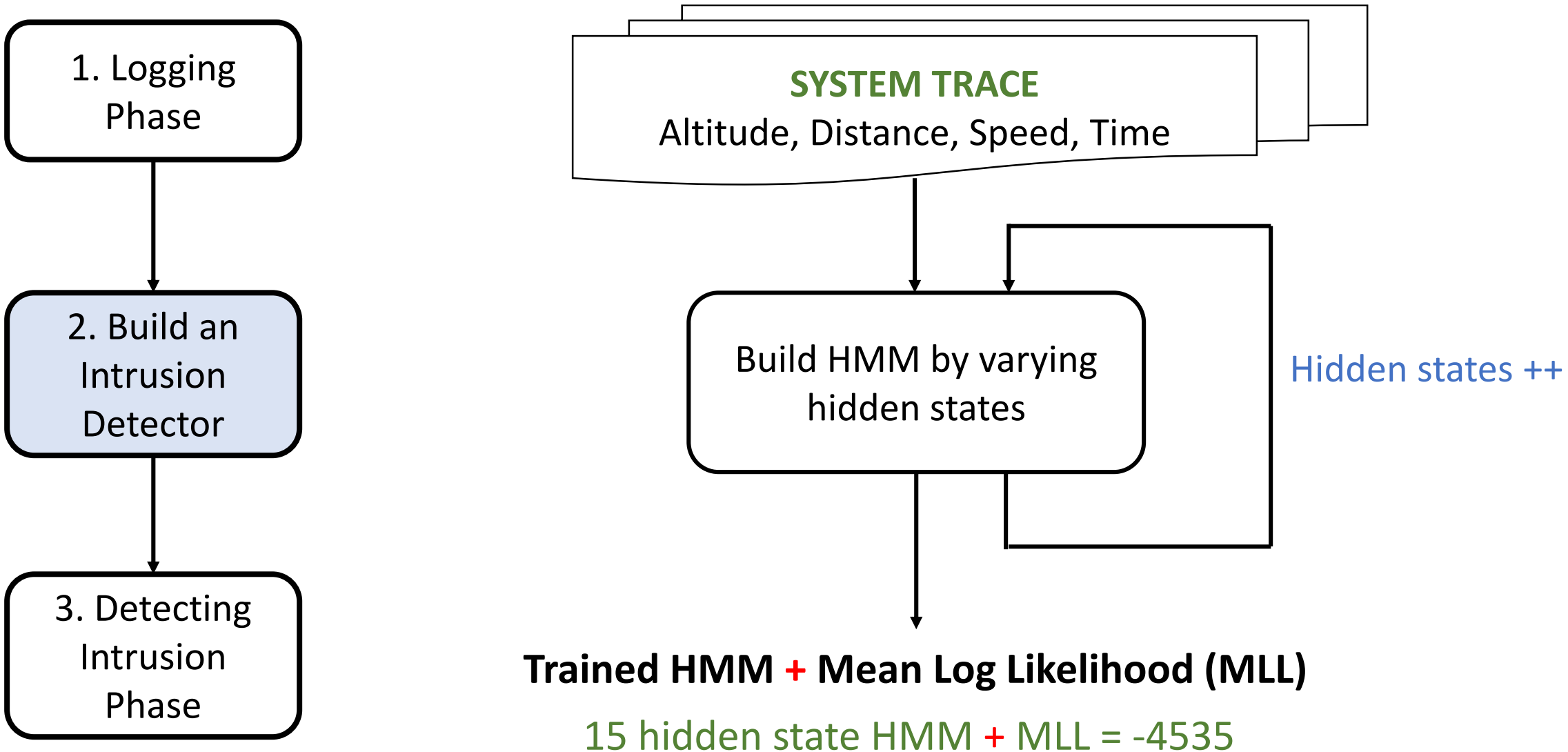
System Traces

Work-flow of CORGIDS

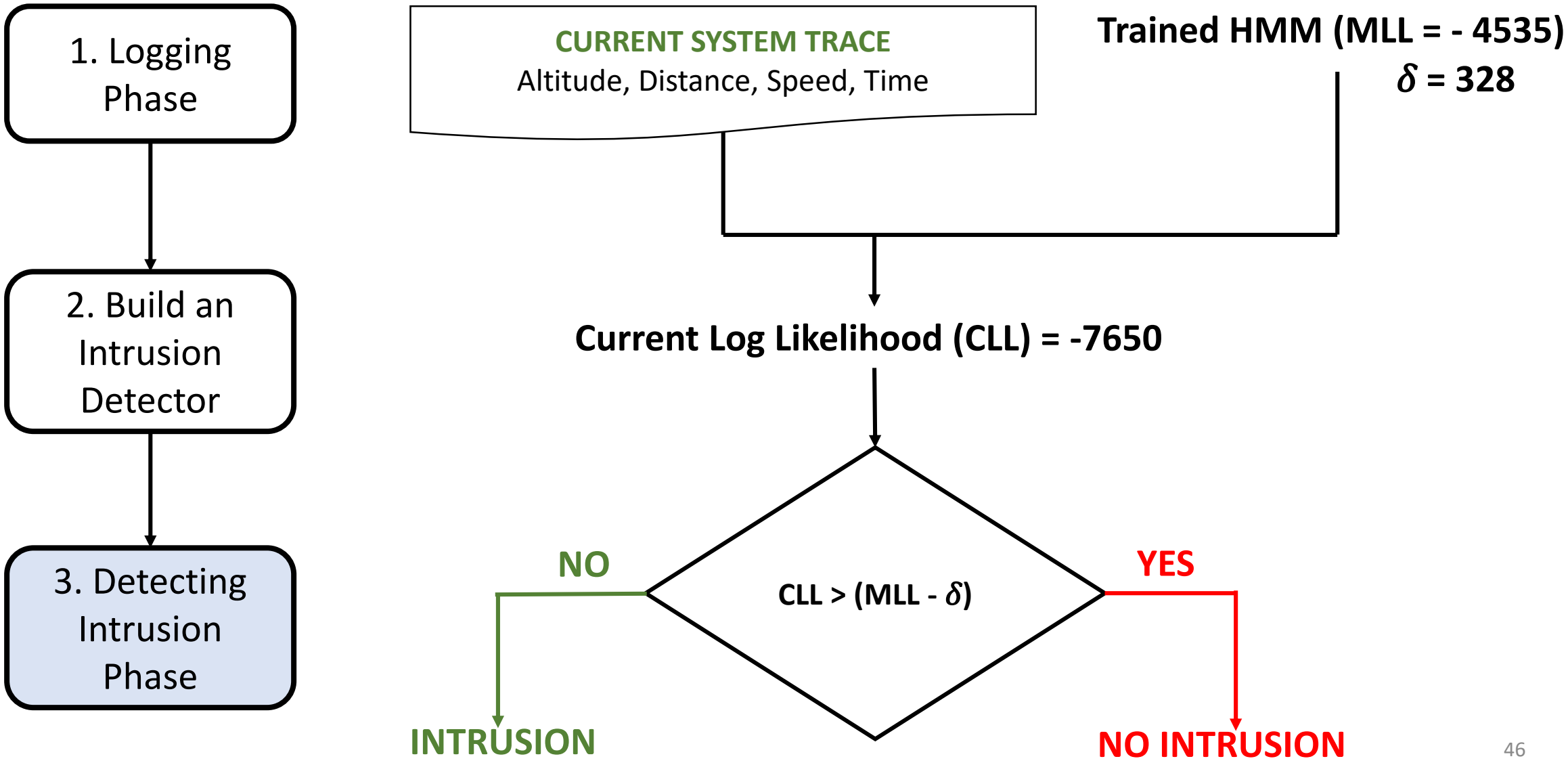


Altitude (m)	Battery left (%)	Distance travelled (m)	Flight time (s)
40	89	42.1445	38.32
40	89	44.2563	39.342
40	89	47.2397	40.356
40	89	51.0202	41.376
40	88	55.2434	42.345
40	88	59.5897	43.346
40	88	64.1632	44.335
41	88	68.8979	45.323
41	88	73.7389	46.351
41	87	78.6564	47.448
41	87	83.6196	48.551

Work-flow of CORGIDS



Work-flow of CORGIDS



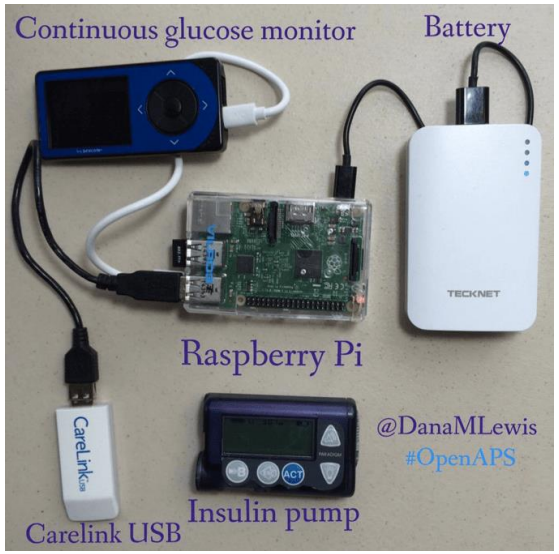
Experimental setup

- **Unmanned Aerial Vehicle (UAV)**

  ArudPilot's Software in the Loop (SITL)
  (http://ardupilot.org/dev/docs/sitl-simulator-software-in-the-loop.html)

- **Smart Artificial Pancreas (SAP)**

  Open Artificial Pancreas System (OpenAPS)
  (https://openaps.org/)



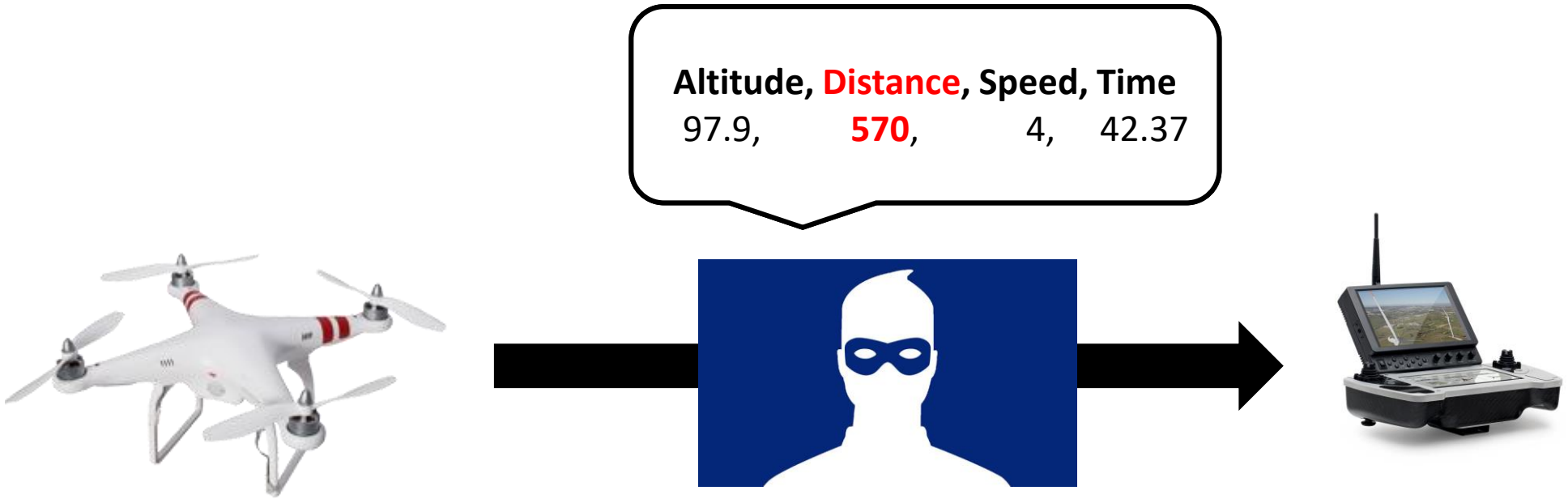
Attacks

- UAV
  - Distance Spoofing
  - Flooding
  - Battery Tampering
- SAP
  - Insulin Tampering
  - Glucose Spoofing

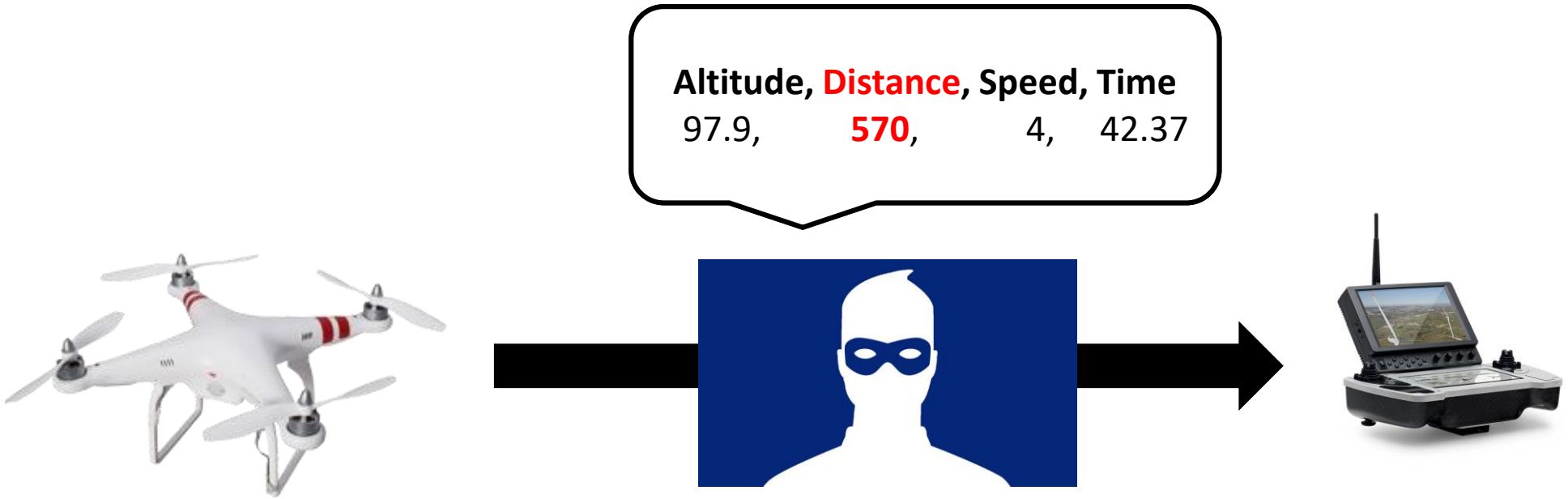
Distance Spoofing Attack

Altitude, Distance, Speed, Time
97.9, 600, 4, 42.37

Distance Spoofing Attack

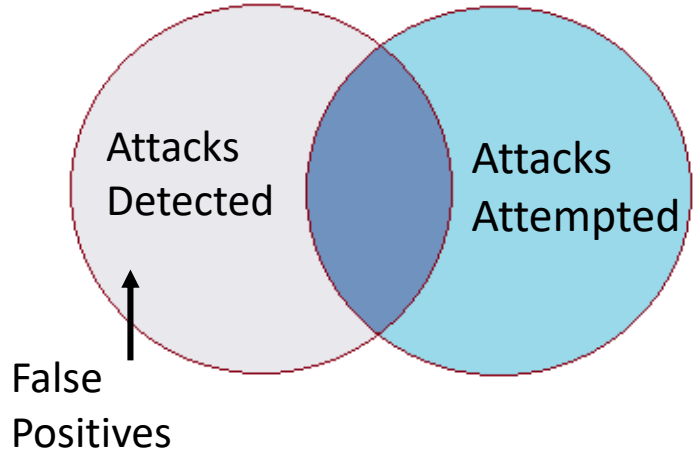


Distance Spoofing Attack

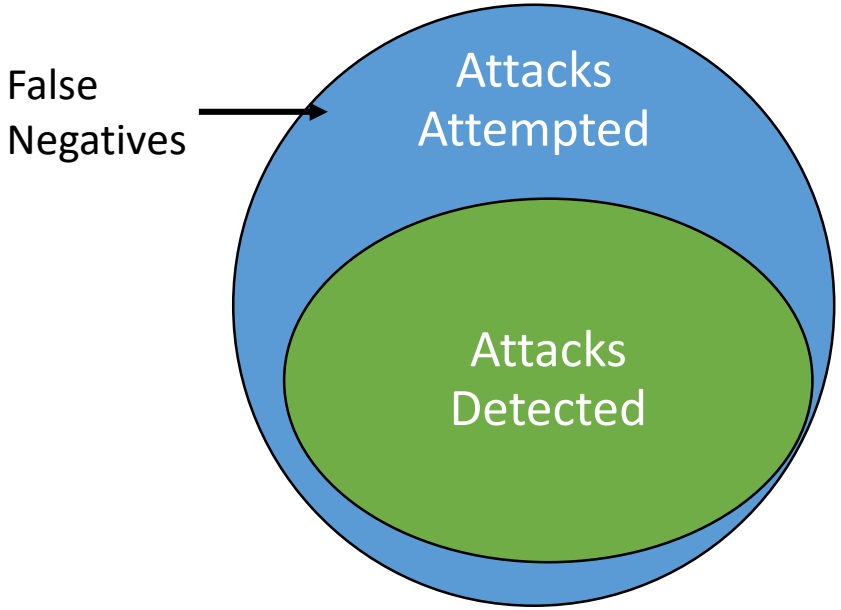


Evaluation Criteria

- **False positive rate (FP)**



False negative rate (FN)



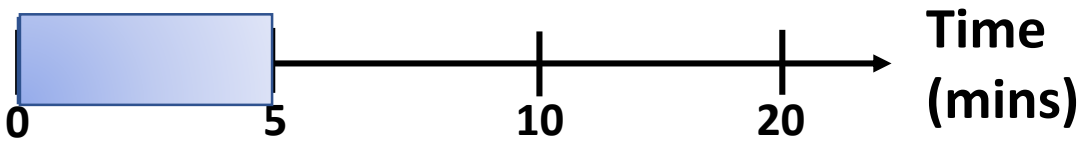
- **Precision** = $\frac{TP}{TP+FP}$
- **Recall** = $1 - FN$
- **Performance overhead** = Additional time take by CORGIDS
- **Memory overhead** = Additional memory take by CORGIDS

Sensitivity Analysis

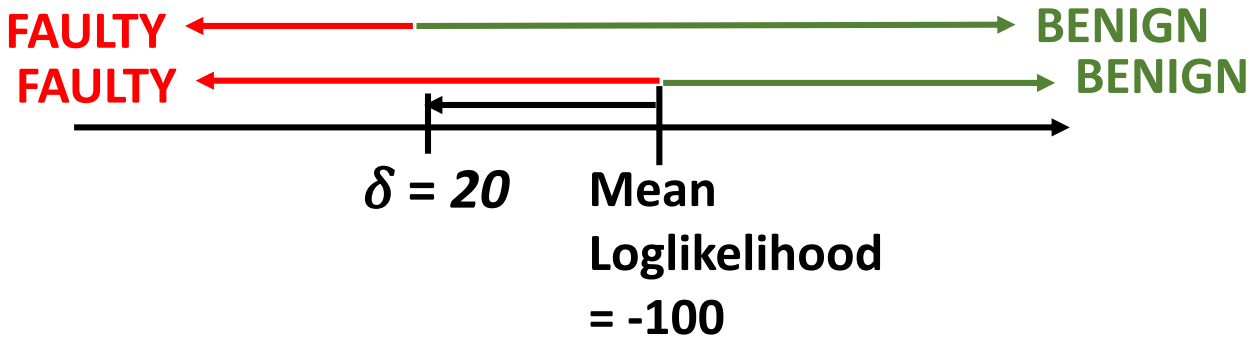
Find values of ***w, δ* and λ** for which highest value of **Precision** and **Recall** is achieved.

Three experimental factors:

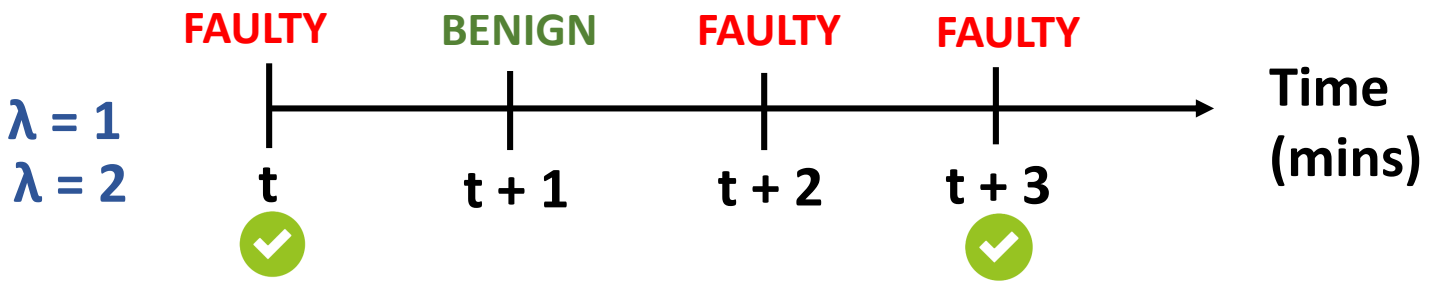
- Window size (***w***) in minutes



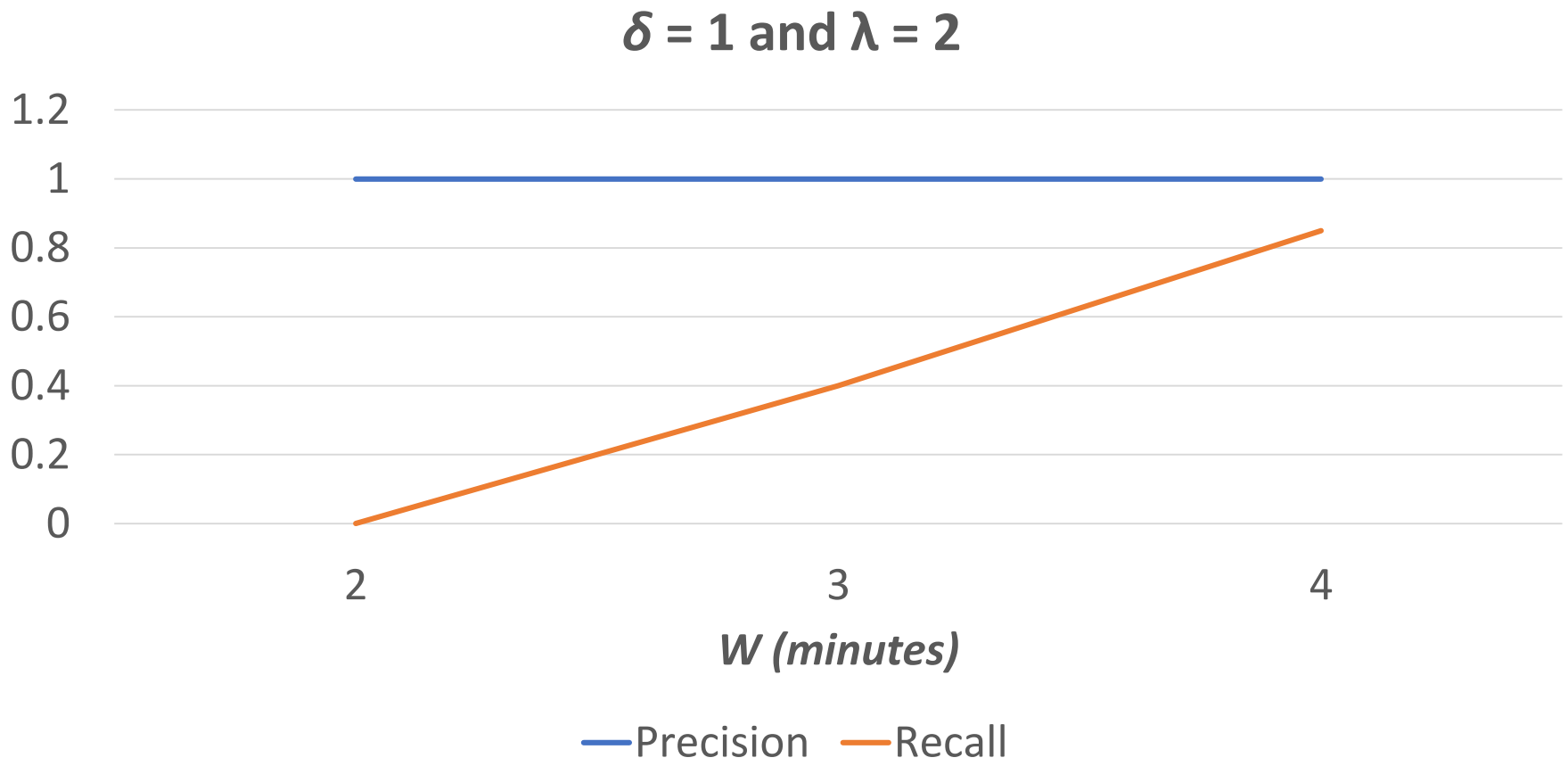
- Acceptable range (*δ*) in standard deviations



- Threshold of consecutive decisions (**λ**)



Sensitivity Analysis: Result



w ↑ Precision & Recall ↑

δ ↑ Precision & Recall ↓

λ ↑ Precision & Recall ↓

Evaluation

TESTBED	TARGETED ATTACKS	FP (%)	FN (%)
UAV	Battery Tampering	0.0	12.20
	Flooding	0.0	11.30
	Distance Spoofing	0.0	12.80
SAP	Insulin Tampering	5.60	4.20
	Glucose Spoofing	2.80	8.40

Table: FP and FN obtained by CORGIDS

Overheads

OpenAPS platform: **Raspberry Pi3**

Approximately 1GB of RAM

With quad-core 64-bit ARM Cortex running at 1.2 GHz

Average of 10 executions

- Memory overhead

  CORGIDS consumed **36.15 MB**

- **Memory overhead comparable with other IDS.**
- **CORGIDS** is **initial implementation** and overhead can be **reduced** by **optimization**.

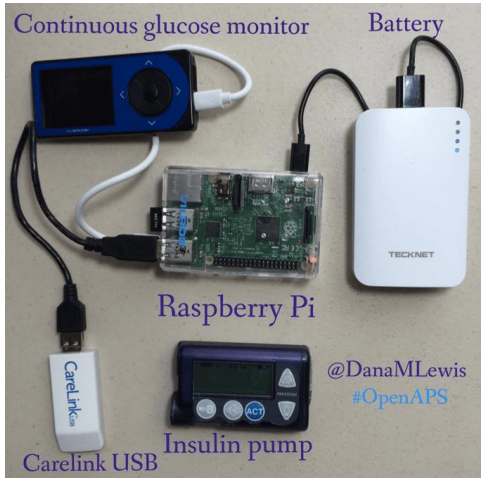
- Performance overhead

  CORGIDS took **1.25 seconds**

- Execution cycle time – 5 minutes
- **Time taken by CORGIDS was negligible.**

Summary

- **Physical properties** of CPS are **indicative** of its behavior.
- **HMM** are **good** at finding **correlations among properties**.
- **CORGIDS** was able to **detect intrusion** with **higher Precision** and **Recall**.



Contact email: **ektaa@ece.ubc.ca**