A Method to Evaluate the Performance of Predictors in Cyber-physical Systems

Leonardo Passig Horstmann, Matheus Wagner, Antônio Augusto Fröhlich

{horstmann, wagner, guto}@lisha.ufsc.br

UFSC / LISHA
Introduction

- Cyber-physical Systems are compositions of software and hardware components
  - Sensors, actuators, controllers, storage, processing units, etc
  - Outputs of some components are used as inputs of other components
    - Becoming data-driven designs
  - Behavior is sensitive to the quality of data
  - Sensing is subject to errors

- Predictors
  - Assess data quality
  - Derive new variables
  - Replace faulty data

- Predictors can be interdependent
  - What are the impacts of prediction interdependence?
Predictors

- Multivariate ANN models
LISHA’s Secure IoT+AI Platform

I/oT / OT / M2M

Gateways

Internet

Cloud

Security Agent

Timed

Geolocated

Encrypted

Signed

Analytics

Machine Learning
A Word on ML for CPS

The $2\sigma$ rule! Who cares for those 5% anyway?
A Word on ML for CPS

We have ν ML is often handling the missing cases! \( \pm 3\sigma \)!
Predictors for Confidence Attribution

\[
f(v, \hat{v}) = \begin{cases} 
1, & \text{if } |v - \hat{v}| \leq \beta \times MAE \\
1 - \frac{|v - \hat{v}| - \beta \times MAE}{\alpha \times MAE}, & \text{otherwise}
\end{cases}
\]
Predictors for Anomalies in Wind Turbines
Predictors for Anomalies in Hydroelectric Plants
Predictors for Engine Calibration
Predictors for AV Control
Predictors for Data Imputation

Replace missing data by high-confidence predicted values!
Predictors for Seismic Data Compressor

50 TB per survey, virtually no communication!

Can we delete data and recover them with predictors?

Inputs start being replaced by predictions.
Problem Definition

- Typical mechanisms to evaluate Predictors
  - Accuracy (e.g., MSE, MAE, RMSE)
  - Computing power (e.g., cycles, committed instructions, cache misses)

- As pointed by Yang and others in 2020, such evaluations usually consider **Independent and Identically Distributed Variables**

- Sensing is subject to errors
  - Datasets often contain bad data

- **How can we evaluate interdependent predictors accounting for the impacts of prediction error propagation?**
Proposed Solution

- This work proposes a method to estimate the impact of using predicted values as input for a multivariate predictor based on the stability of a general dynamic system.

- Predictor is a function $v_i = g_i(x_i)$
  - $x_i$ vector of inputs
  - $v_i$ scalar quantity prediction for $i_{th}$ variable in a set

- $g_i$ is assumed to be infinitely differentiable
  - Sigmoid, Hyperbolic Tangent, Softmax, Swish and CoLU (but not ReLU)

- $g_i$ expanded into a Taylor series
  - Evaluate error propagation dynamics over the Taylor series to verify error boundedness.
Procedure for Analysis

- The gradient of \( g_i \) is \( \frac{\partial g_i(\hat{x}_i)}{\partial \hat{x}_i} \)

\[
\hat{\delta}_i = \hat{\delta}_i^* + \frac{\partial g_i(\hat{x}_i^*)}{\partial \hat{x}_i} (\hat{x}_i - \hat{x}_i^*) + \frac{1}{2} \frac{\partial^2 g_i(\hat{x}_i^*)}{\partial \hat{x}_i^2} (\hat{x}_i - \hat{x}_i^*)^2 + ...
\]

- Considering the deviation of the predictor’s input is small, or \( g_i \) resembles a linear function, we can truncate the Taylor series to the first order terms
  - Other terms would be negligible
  - The deviation of the prediction can be related to the deviation of the input

\[
\hat{\delta}_i - \hat{\delta}_i^* = \frac{\partial g_i(\hat{x}_i^*)}{\partial \hat{x}_i} (\hat{x}_i - \hat{x}_i^*)
\]
Procedure for Analysis

- Considering the $N$ components of the input vector, the error can be summarized as

$$\hat{e}_i = \sum_{j=0}^{N-1} \frac{\partial g_i(\hat{x}_i^*)}{\partial x_{i,j}} e_j + MAE_i$$

- Using a linear approximation for linear time-invariant system
  - Predictor gradient changes
    - Bounded in absolute value (worst-case)
    - Error propagation Dynamics
    - Bounded-Input Bounded-Output (BIBO) stability (property of linear systems)

$$\|\hat{e}_i\| \leq \sum_{j=0}^{N-1} \left\| \frac{\partial g_i(\hat{x}_i^*)}{\partial x_{i,j}} \right\| \|e_j\| \leq \sum_{j=0}^{N-1} \max \left\{ \left\| \frac{\partial g_i(\hat{x}_i^*)}{\partial x_{i,j}} \right\| \right\} \|e_j\|$$
Types of Predictor Interdependence

Cascade Prediction

Feedback Prediction

Loop Prediction
Estimation Error Stability Conditions

- The propagation of error has different impacts for each of the presented scenarios
- Considering stability as the boundedness of the error propagation
  - Cascade chains are stable (as long as there are a finite set of predictors)
  - Loop and Feedback scenarios are infinite due to recurrent predictions (circle)
- Even in a stable propagation, the error can eventually exceed the tolerance defined by the application
  - We can track the estimated error and decide whether a new prediction is believed to exceed this margin or not following the equation for the prediction error
Estimation Error Stability Conditions

Cascade Prediction

Feedback Prediction

$\|z_1\| = \lambda_i^r \leq 1$

Always Stable

$\lambda_i^j = \max \left\{ \left\| \frac{\partial g_i(\vec{x}_i^*)}{\partial x_{i,j}} \right\| \right\}$

Loop Prediction

$\|z_{1,2}\| = \sqrt{\sum_{j \in D_i} \lambda_i^j \lambda_i^j} \leq 1$
Case Study

- **Dataset**
  - Hydraulic test rig (Helwig et al., 2015)

- **Model Generation**
  - Person Correlation
  - $K$ features
  - Autoregressive and non-autoregressive

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Physical Quantity</th>
<th>Sampling Frequency</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS1</td>
<td>Pressure [bar]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>FS2</td>
<td>Pressure [bar]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>FS3</td>
<td>Pressure [bar]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>FS4</td>
<td>Pressure [bar]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>FS5</td>
<td>Pressure [bar]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>FS6</td>
<td>Pressure [bar]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>MPW</td>
<td>Motor Power [W]</td>
<td>100 Hz</td>
</tr>
<tr>
<td>FS1</td>
<td>Volume Flow [L/min]</td>
<td>10 Hz</td>
</tr>
<tr>
<td>FS2</td>
<td>Volume Flow [L/min]</td>
<td>10 Hz</td>
</tr>
<tr>
<td>TS1</td>
<td>Temperature [°C]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>TS2</td>
<td>Temperature [°C]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>TS3</td>
<td>Temperature [°C]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>TS4</td>
<td>Temperature [°C]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>VS1</td>
<td>Vibration [mm/s]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>CE</td>
<td>Cooling Efficiency [%]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>CP</td>
<td>Cooling Power [W]</td>
<td>1 Hz</td>
</tr>
<tr>
<td>SE</td>
<td>Efficiency Factor [%]</td>
<td>1 Hz</td>
</tr>
</tbody>
</table>

```
<table>
<thead>
<tr>
<th>Target</th>
<th>Selected Inputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>FS1</td>
<td>FS1, MPW, SE, FS1</td>
</tr>
<tr>
<td>FS2</td>
<td>FS2, FS1, SE, FS3</td>
</tr>
<tr>
<td>FS3</td>
<td>FS3, FS1, FS2, SE</td>
</tr>
<tr>
<td>FS4</td>
<td>FS4, CE, TS2, TS4</td>
</tr>
<tr>
<td>FS5</td>
<td>FS5, FS6, TS3, TS4</td>
</tr>
<tr>
<td>FS6</td>
<td>FS6, FS5, TS3, TS4</td>
</tr>
<tr>
<td>MPW</td>
<td>MPW, FS1, SE, FS2</td>
</tr>
<tr>
<td>FS1</td>
<td>FS1, FS3, FS2, SE</td>
</tr>
<tr>
<td>FS2</td>
<td>FS2, TS4, TS3, TS2</td>
</tr>
<tr>
<td>TS1</td>
<td>TS1, TS2, TS4, TS3</td>
</tr>
<tr>
<td>TS2</td>
<td>TS2, TS4, TS1, TS3</td>
</tr>
<tr>
<td>TS3</td>
<td>TS3, TS4, TS2, TS1</td>
</tr>
<tr>
<td>TS4</td>
<td>TS4, TS3, TS2, TS1</td>
</tr>
<tr>
<td>VS1</td>
<td>VS1, FS2, CE, CP</td>
</tr>
<tr>
<td>CE</td>
<td>CE, TS4, CP, TS2</td>
</tr>
<tr>
<td>CP</td>
<td>CP, CE, TS4, TS2</td>
</tr>
<tr>
<td>SE</td>
<td>SE, FS2, FS1, FS1</td>
</tr>
</tbody>
</table>
```

Autoregressive FS

Non-autoregressive FS
Results – Cascade Configuration

- **MPW to PS1**
  - Input impact on predictor

![Graphs showing pressure over time with markers for measurement, prediction with interdependence, and estimated prediction error with interdependence.](image-url)
Results – Stable Feedback Configuration

- PS6
  - Calculate $z$ following feedback stability condition
  - $z \leq 1$

$\lambda_{PS6}^r = 0.36$
$z = 0.36$
Results – Unstable Feedback Configuration

- PS2
  - Calculate $z$ following feedback stability condition
  - $Z \geq 1$

$\lambda_{PS2}^r = 1.01$

$z = 1.01$
Results – Stable Loop Configuration

- PS5 and PS6 (ps5 → ps6, ps6 → ps5)
  - Calculate $z$ following loop stability condition
  - $Z \leq 1$

$$\lambda_{PS5}^{PS6} = 0.70$$
$$\lambda_{PS6}^{PS5} = 0.67$$
$$z = 0.68$$
Results – Unstable Loop Configuration

- PS1 and MPW
  - Calculate $z$ following loop stability condition
  - $Z \geq 1$

$\lambda_{PS1}^{MPW} = 1.03$
$\lambda_{PS1}^{MPW} = 1.01$
$z = 1.02$
Final Remarks

- This work presented a strategy to evaluate a predictor based on its ability to sustain accurate predictions when its inputs are replaced by predictions and face the impacts of prediction error.

- Different datasets impact prediction accuracy
  - Mathematical analysis is valid as long as the activation function is infinitely differentiable.
  - We do not evaluate the predictor’s accuracy but the fact it is able to maintain it when dealing with inputs that are predicted data.
    - Boundedness

- Dataset variability / Input variability
  - Will affect model quality
    - Boundedness still follows the mathematical analysis.