Dynamic Data Driven Applications Systems 2020

DDDAS2020

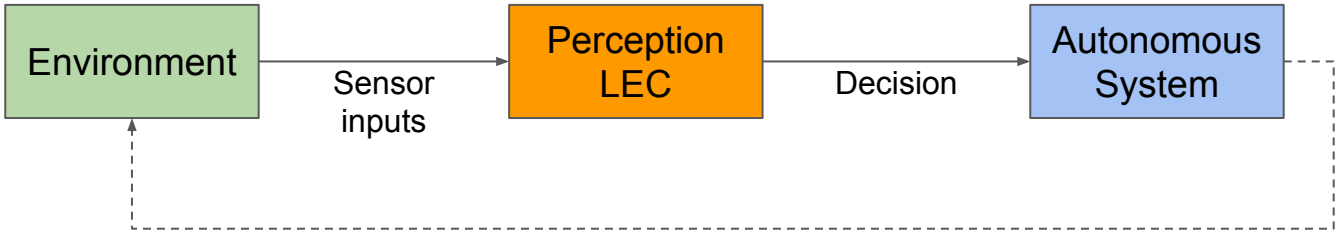
Improving Prediction Confidence in Learning-Enabled Autonomous Systems

DIMITRIOS BOURSINOS AND XENOFON KOUTSOUKOS

INSTITUTE FOR SOFTWARE INTEGRATED SYSTEMS
ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
VANDERBILT UNIVERSITY

VANDERBILT UNIVERSITY

Assurance Monitoring of autonomous systems



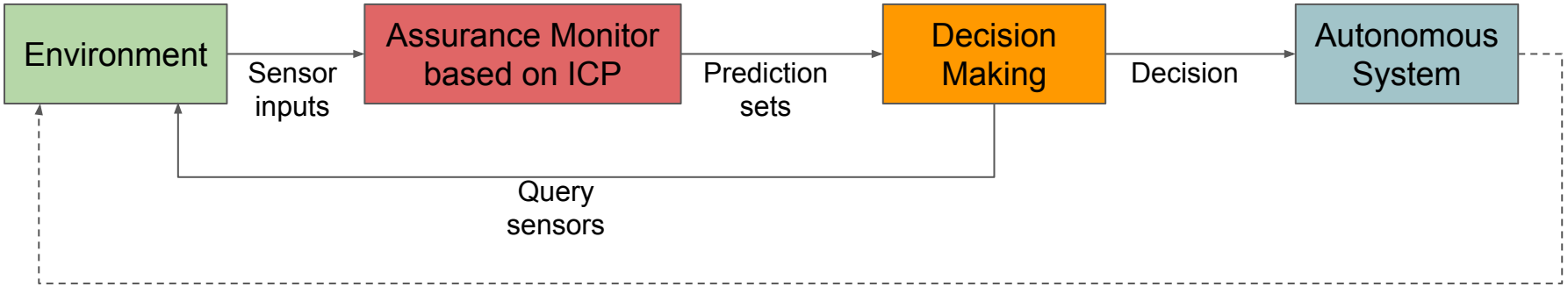
Machine learning components are being used by autonomous systems because of their ability to handle dynamic and uncertain environments.

- Deep neural networks (DNNs)
- High dimensional inputs
- Non-transparent

Problem:

- Computation of a significance level along with each decision
- Well-calibrated
- Limited false alarms
- Real-time
- Sequential inputs

Overview of the approach



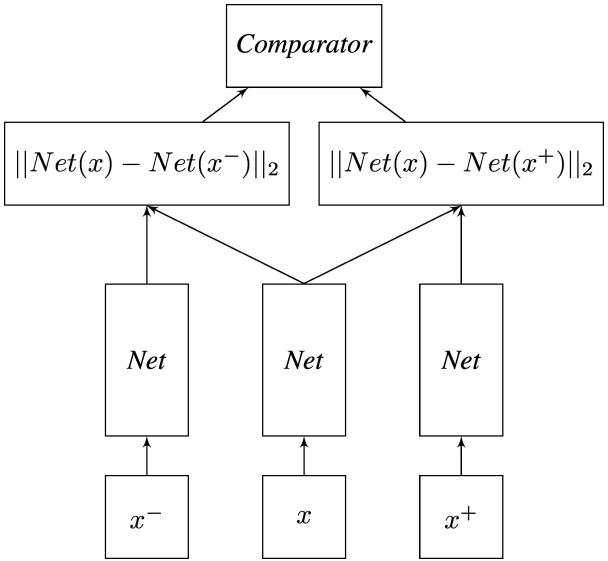
Real-time assurance monitor

- Distance learning using triplet network
- Inductive Conformal Prediction (ICP) based on distance learning

Decision Making

- Significance level estimation to minimize monitoring alarms
- Feedback-loop design
- Evaluation on the GTSRB dataset

Triplet Network



Distance deep metric learning using Triplet network:
Estimate the similarity of different inputs

Structure:

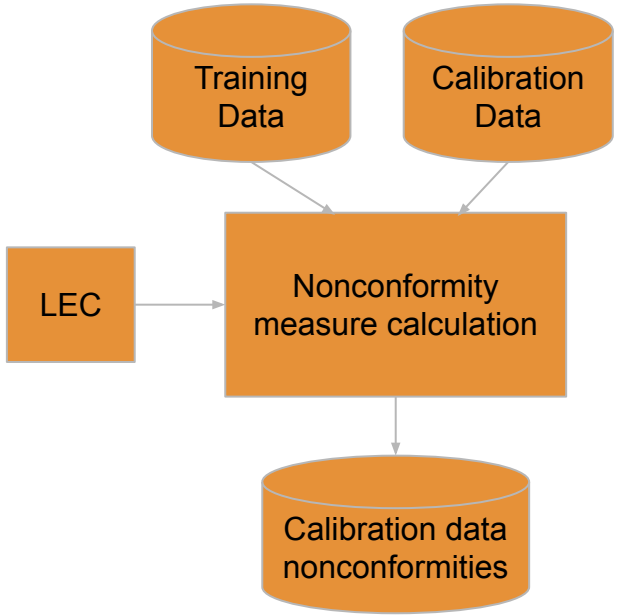
- A triplet network is composed using three copies of the same neural network with shared parameters.
- The last layer of each of the 3 DNNs produce an embedding representation of each input.
- The Euclidean distance between embeddings is a measure of similarity.

Training:

- We form triplets of input data, an anchor input *x*, a positive input x^+ that belong to the same class as *x* and a negative input x^- of a different class.
- The training aims in minimizing the euclidean distance between embeddings of the same class and maximizing the Euclidean distance of embeddings belonging in different classes.
- Faster training by mining sample triplets such that $|Net(x) - Net(x^-)| < |Net(x) - Net(x^+)|$

E. Hoffer and N. Ailon. Deep metric learning using triplet network. In International Workshop on Similarity-Based Pattern Recognition, pages 84–92. Springer, 2015.

Inductive Conformal Prediction



Nonconformity measure:
A function which measures how different is a test example from the training data set

- **Split the training set into**
  - The proper training set
  - The calibration set
- **Use the proper training set to train the LEC**
- **For each example in the calibration set**
  - Calculate the nonconformity scores using a nonconformity function
- **For each test example,**
  - Calculate the nonconformity score
  - Compute the *p*-value as the fraction of calibration examples that are equally or more conforming.
- **Compute a set predictor with a given confidence based on the *p*-values.**

Shafer, G., & Vovk, V. (2008). A tutorial on conformal prediction. Journal of Machine Learning Research, 9(Mar), 371-421.

Triplet-Based ICP

- Learn representations of the input data that can be used to compute the similarity between test examples and examples in the training data set
- A nonconformity function computes how similar a test input is to the training set.
- It is natural to define the nonconformity functions in the embedding space created by the trained triplet network $f : X \rightarrow V$
- Using the triplet all the input data points x (proper training, calibration and testing) are mapped to representations v , $v = f(x)$.
- The Euclidean distance d computed in the embedding space is a measure of similarity.

Nonconformity Function definition:

***k*-Nearest Neighbors**

$$\alpha(x, y) = |i \in \Omega : i \neq y|$$

p-value:

$$p_j(x) = \frac{|\{\alpha \in A : \alpha \geq \alpha(x, j)\}|}{|A|}$$

Select the significance level

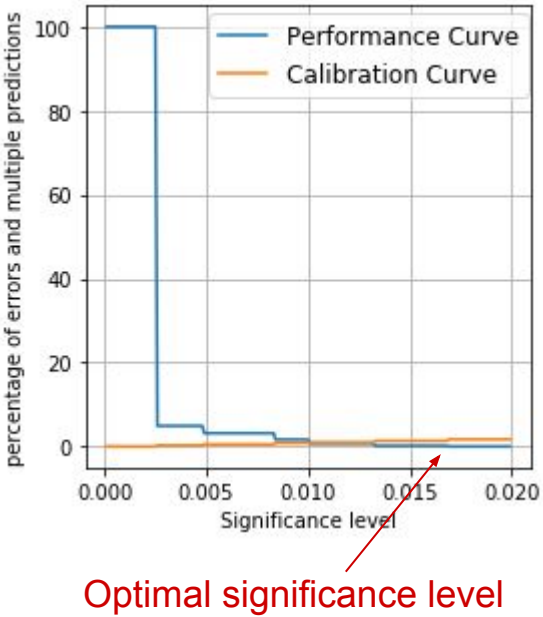
Given a test example x with an unknown label y, ICP forms a set $|\Gamma^{\varepsilon}|$ of possible labels $\tilde{y}$ so that $P(y \notin \Gamma^{\epsilon}) < \epsilon$

A candidate label $\tilde{y}_j$ is added to the set Γ^{ε} if

$$p_j(x) > \epsilon$$

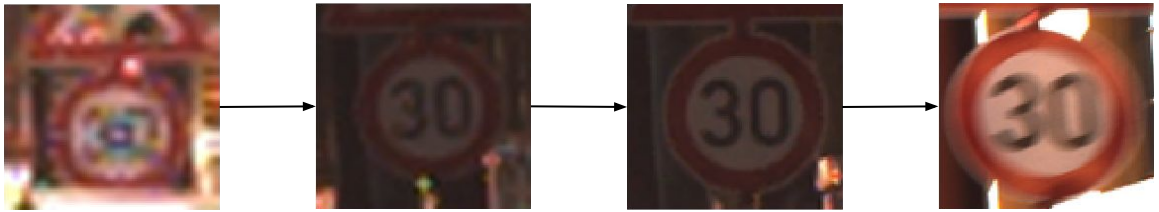
Select ε to minimize cases of $|\Gamma^{\epsilon}| > 1$

- Given a validation set, we compute the number of set predictions with multiple classes for different values of ε.
- We select the lowest ε value that doesn't produce any set of multiple classes.

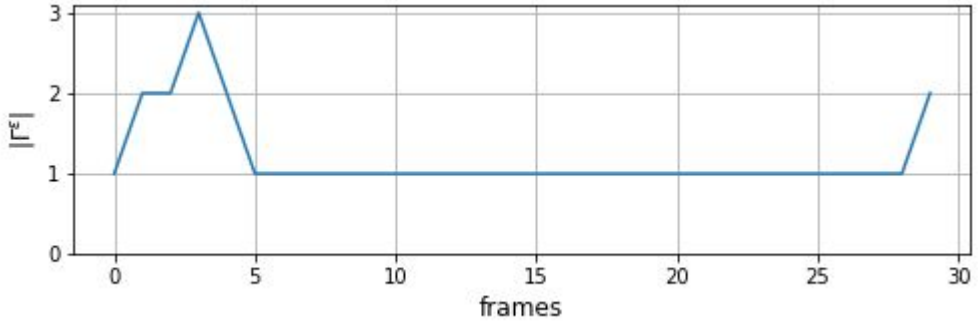


Optimal significance level

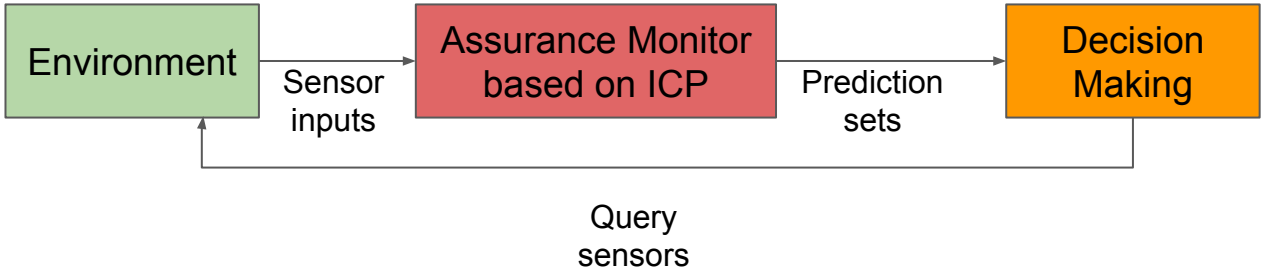
Decision Making



- The ICP framework works well when inputs are IID.
- Individual inputs of a sequence might be of low quality leading to $|\Gamma^{\epsilon}| > 1$



Feedback-loop for querying the sensors



- Taking into account a number of sequential inputs can improve the perception information.
- A feedback-loop is utilized that reduces the incorrect predictions for low quality individual inputs by requiring $|\Gamma^{\epsilon}| = 1$ with an identical single label for *k* consecutive sensor measurements.

EVALUATION

Experimental Setup

GTSRB Dataset
Task:
Traffic Sign Recognition on images captured by vehicle camela.




Image size: 96x96

43 different classes
Sequence duration: 30 frames
Dataset:
888 sequences in the training set
88 sequences in test set (test 1)

12630 IID signs
- 10% → Testing using IID signs (test 2)
- 90% → Augmented Training → Proper Training 80%, Calibration 20%

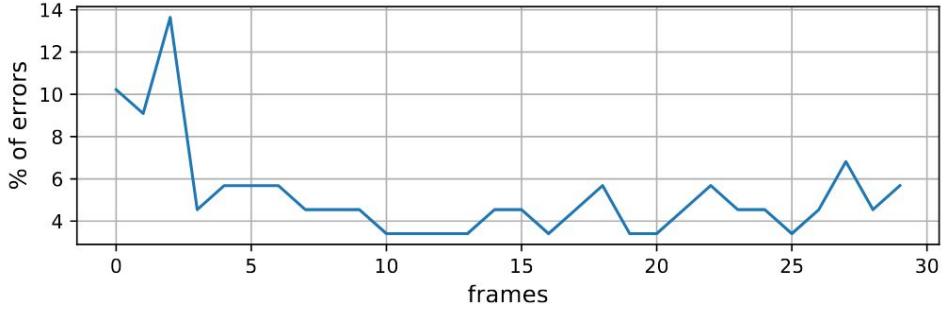
Classification Accuracy of triplet network

The triplet network can be used for point predictions when combined with a *k*-Nearest Neighbors classifier in the embedding space

Classification Accuracy:

Training Accuracy	Validation Accuracy	test 1 Accuracy	test 2 Accuracy
0.991	0.987	0.948	0.986

Confirming the basic hypothesis of machine learning that the training and testing data sets should consist of IID samples

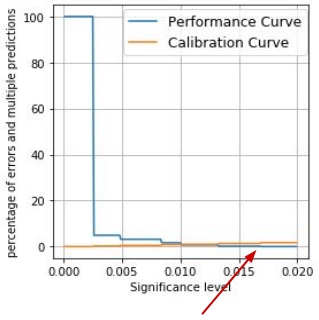


Early frames are responsible for the larger error-rate in the sequences

ICP Performance

- ICP is applied on single inputs to compare the performance when inputs are:
  - part of a sequence (test 1)
  - IID (test 2)

- ε is computed using the augmented calibration data



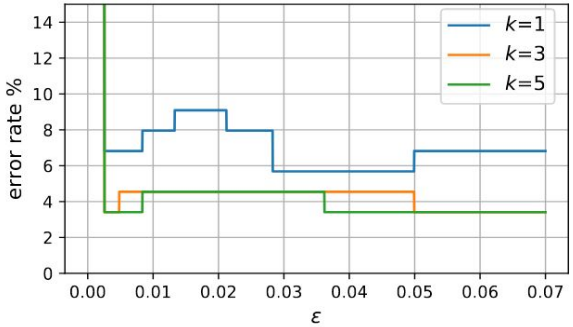
ICP on individual frames:

	test 2		test 1	
ϵ	Errors	Multiples	Errors	Multiples
0.017	1.7%	0%	5.6%	0%

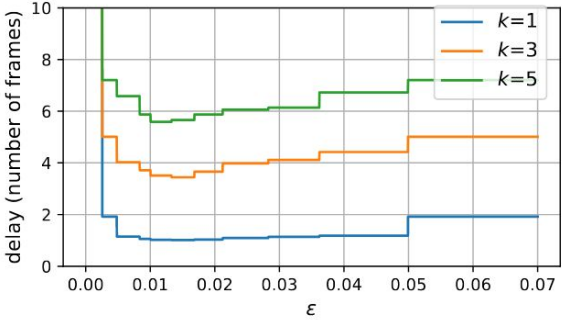
The computed significance level bounds the error-rate only for the IID data

Feedback-loop Performance

Improving the prediction accuracy using the feedback loop:



Error-rate with respect to the chosen significance level for different values of *k*



Number of frames required for a decision with respect to the chosen significance level for different values of *k*

k can be chosen accordingly to control the tradeoff between accuracy and decision time

Execution Time: 1ms
Total Memory=Proper training set representations + Triplet network= 74.4 MB

Illustrative example

Parameters:

ε=0.004

k=5

Test Input

Prediction Set

Prediction

No Prediction

Conclusion

- Assurance monitor in DDDAS
- Inductive Conformal Prediction framework
- Embedding representations learning using a triplet network
- Significance level computation to minimize multiple predictions
- Feedback-loop querying new sensor inputs when a confident decision cannot be made
- Evaluation on the GTSRB dataset
  - Baseline ICP works only for IID data
  - The feedback-loop improves the ICP performance on sequences
  - Real-time
- Future work
  - Design the feedback loop based on the p-values