Leibniz Universität Hannover

Master thesis

Anomaly detection in streaming data using autoencoders

Student: Bin Li

Supervisor: Prof. Dr. Eirini Ntousi

Outline

- Motivation
- Previous works
- Proposed model
- Experiments
- Conclusion and outlook
- References

Motivation

- **Anomaly detection applications**
  - Industrial: Predictive maintenance
  - Commercial: Credit card fraud detection

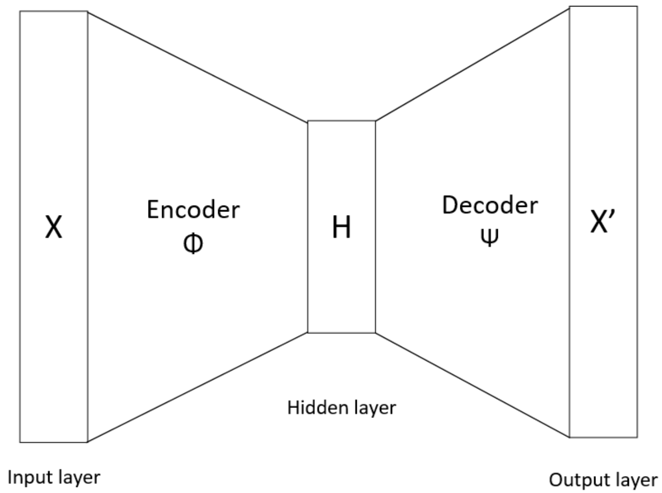
- **Challenges**
  - High-volume data (out of memory)
  - High-velocity streaming data (concept drift, bias classes)
  - Contextual anomaly

Previous works

- **Traditional approaches**
  - One-Class SVM [Schölkopf et al.] [Tax and Duin]
  - Local Outlier Factor [Breunig et al.]
  - Distance based approaches …
  - Density based approaches…

Previous works

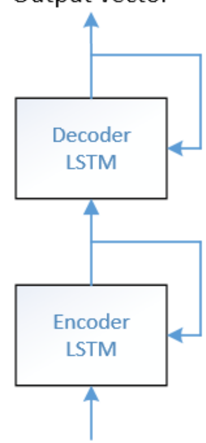
- **Autoencoder based approaches**
  - Vanilla autoencoder [Martinelli et al.]
  - LSTMs-Autoencoder [Malhotra et al.]
  - Autoencoders for stream learning [Dong et al.]



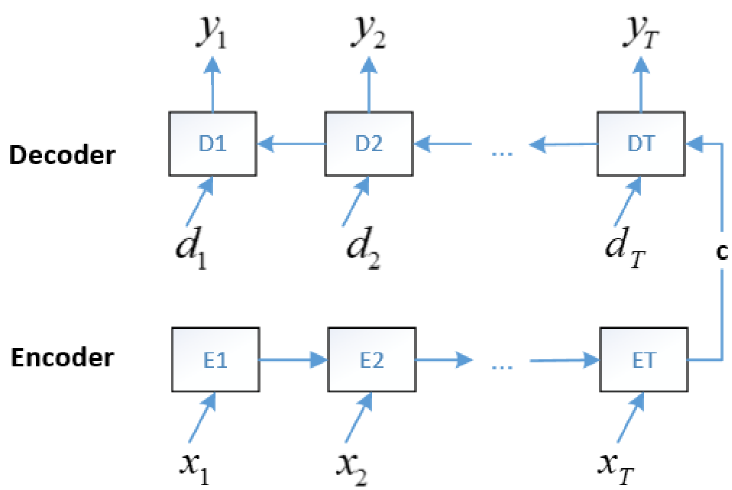
$$\text{Anomaly score} = f(|X' - X|)$$

Proposed model

1. LSTMs-Autoencoder



LSTMs-Autoencoder

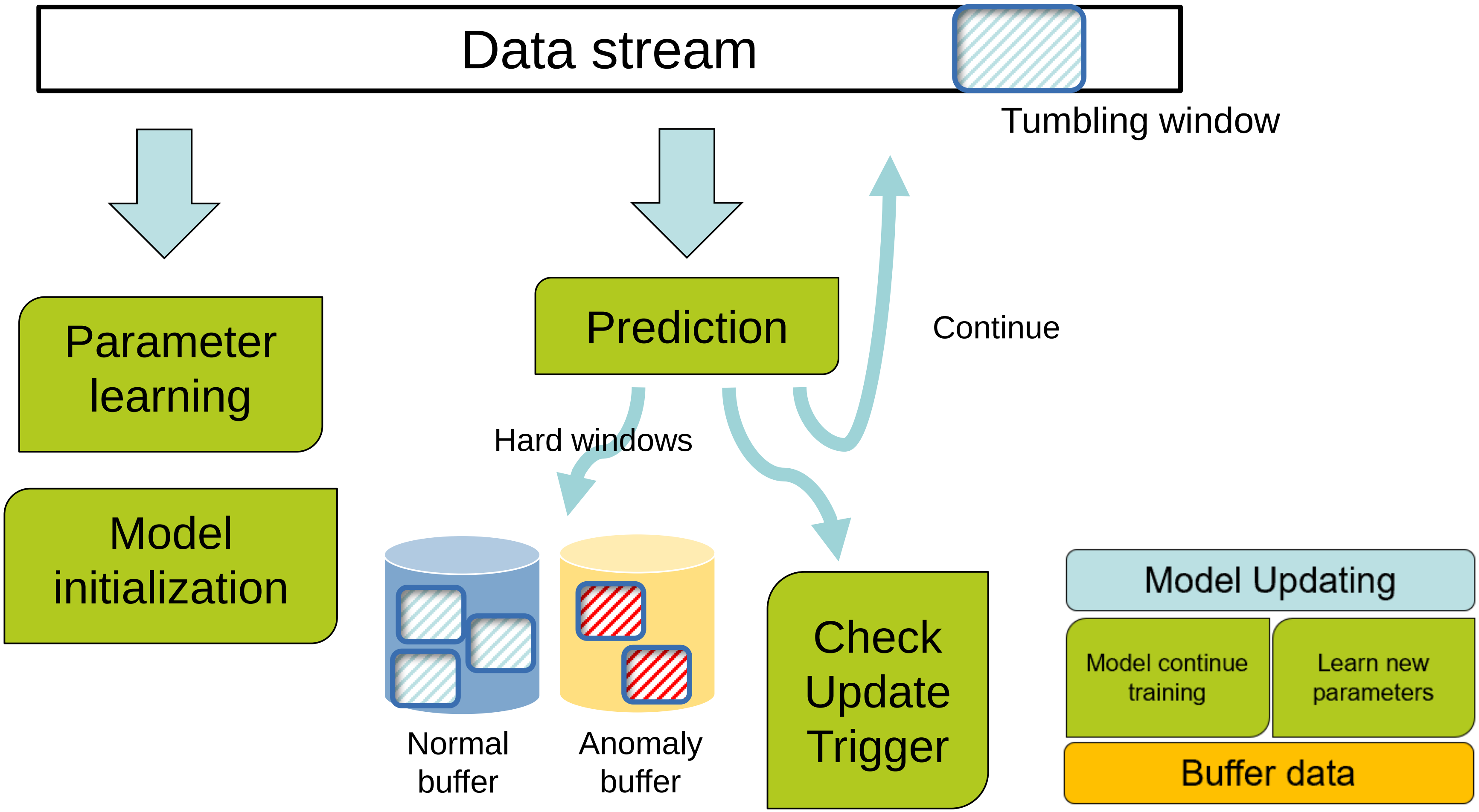


LSTMs-Autoencoder unfolded through time

- Decoder input d_i is the real value of previous time step
- Estimate a normal distribution **D** of normal reconstruction errors
- Anomaly score of a point is defined as its **Mahalanobis distance** to **D**

Proposed model

2. Framework overview



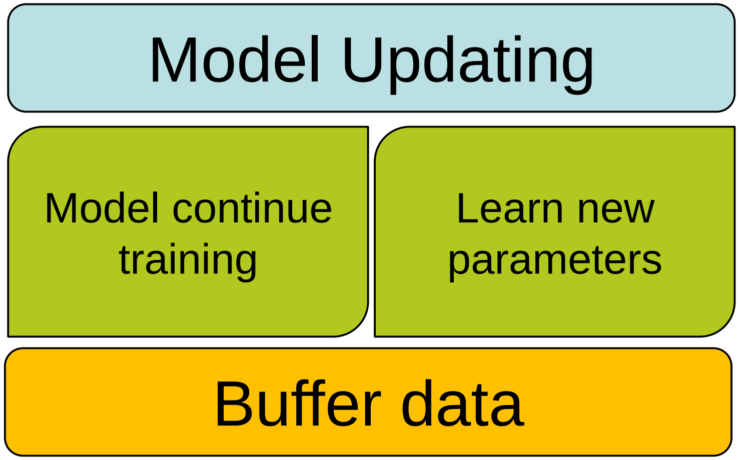
Proposed model

3. Online model updating

- Hard windows criterion
  - Normal window (labeled) with more than $\mathcal{N}$ scores over threshold

- Updating trigger
  - Retrain buffers are full
  - Buffer size is a hyperparameter

- Updating strategy
  - Continue training LSTMs-Autoencoder
  - Learn new anomaly score threshold



Experiments

1. Datasets

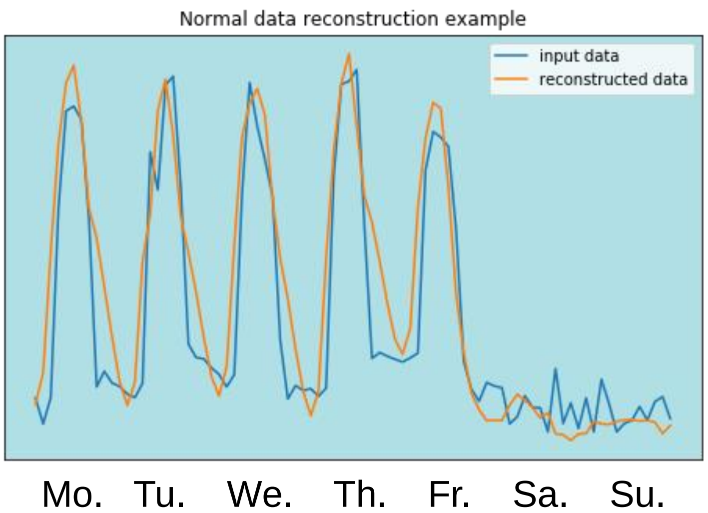
	Dimensionality	# instances	Anomaly proportion (%)
Power Demand	1	35 040	2.20
SMTP[1]	34	96 554	1.22
HTTP[1]	34	623 091	0.65
SMTP+HTTP[2]	34	719 645	0.72
Forest Cover[3]	7	581 012	0.47

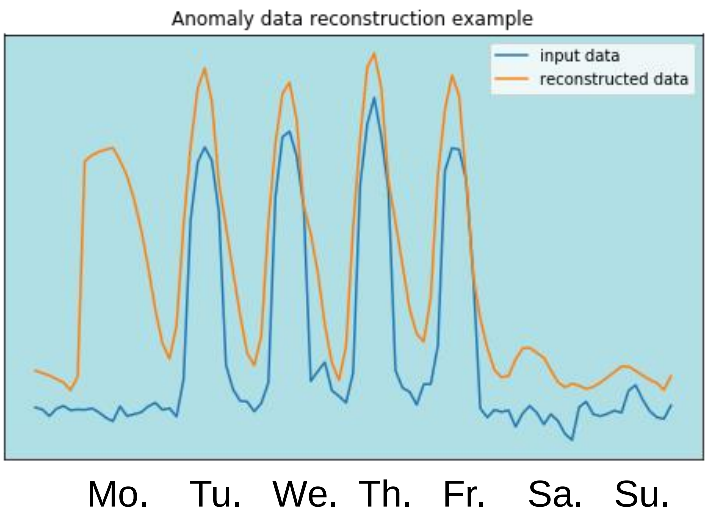
- [1] extracted from KDD99Cup dataset
- [2] is derived by connecting SMTP and HTTP
- [3] contains 7 kinds of forest cover types, here take the smallest subset TYPE4 as anomaly

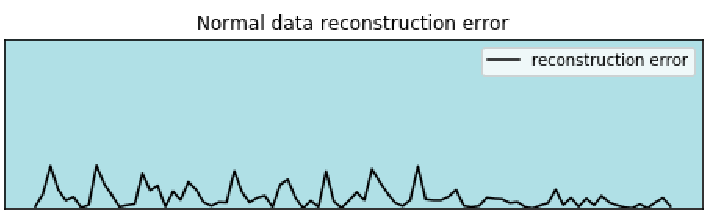
Experiments

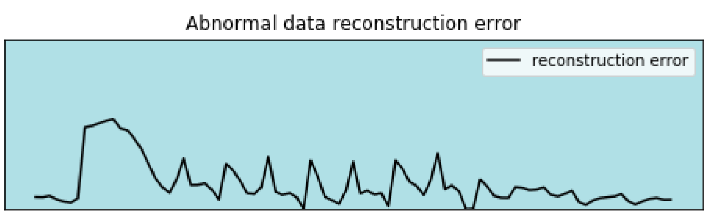
2. Anomaly detection

- Power Demand dataset example









Experiments

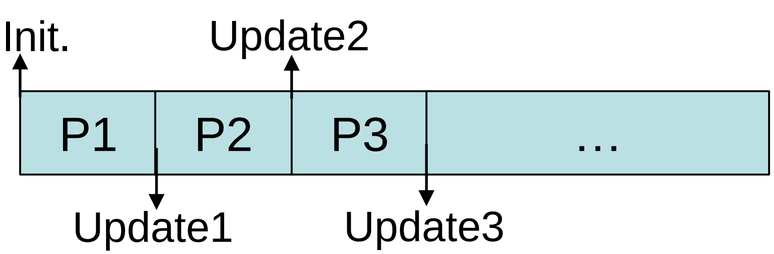
2. With & without updating

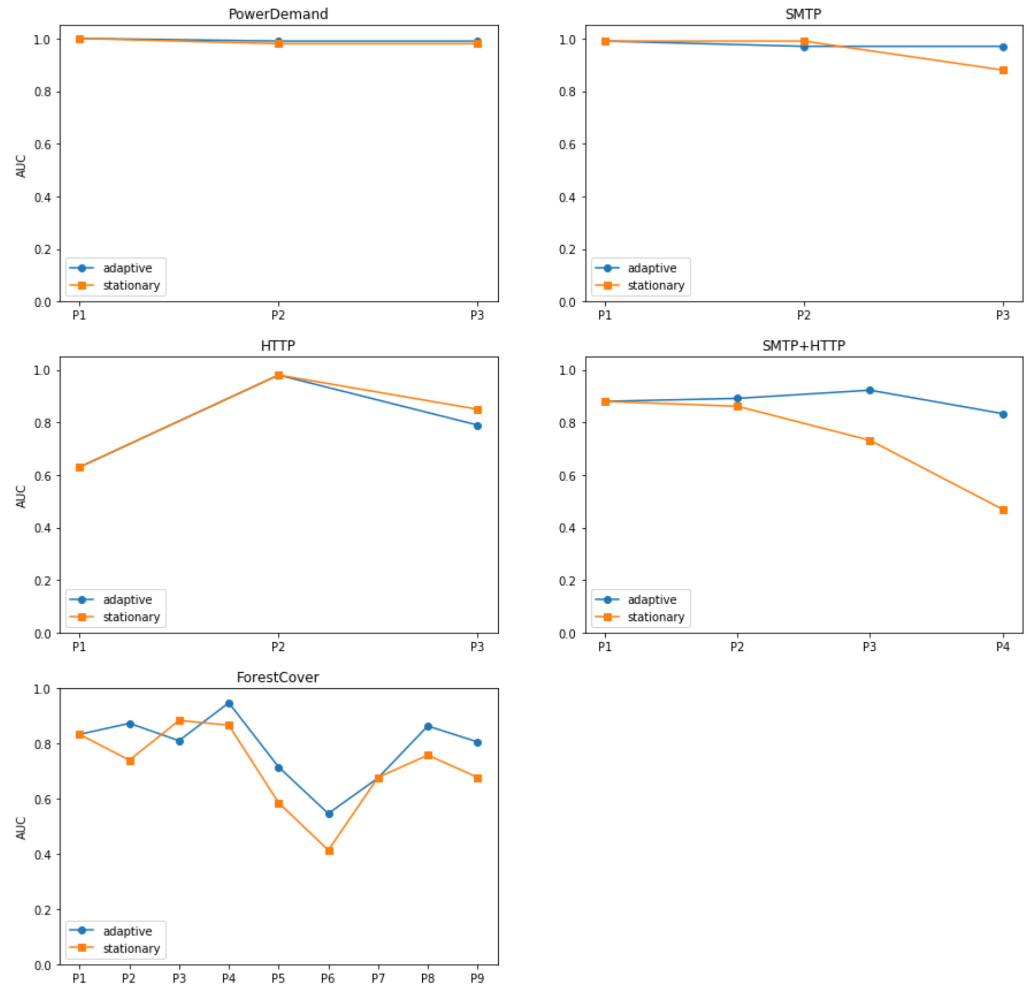
	AUC without updating	AUC with updating	#Updating
Power Demand	0.91	**0.97**	2
SMTP	0.94	**0.98**	2
HTTP	0.76	**0.86**	2
SMTP+HTTP	0.64	**0.85**	3
Forest Cover	0.74	**0.82**	8

Experiments

2. With & without updating

- Stationary
  - Only trained during initialization
- Adaptive
  - Model updating over stream with buffer data

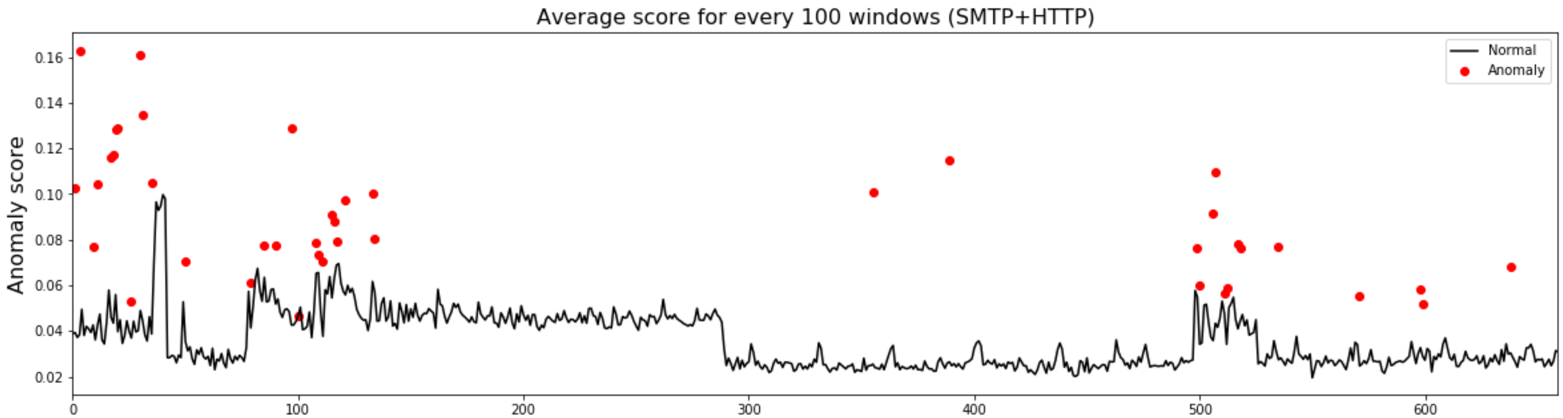


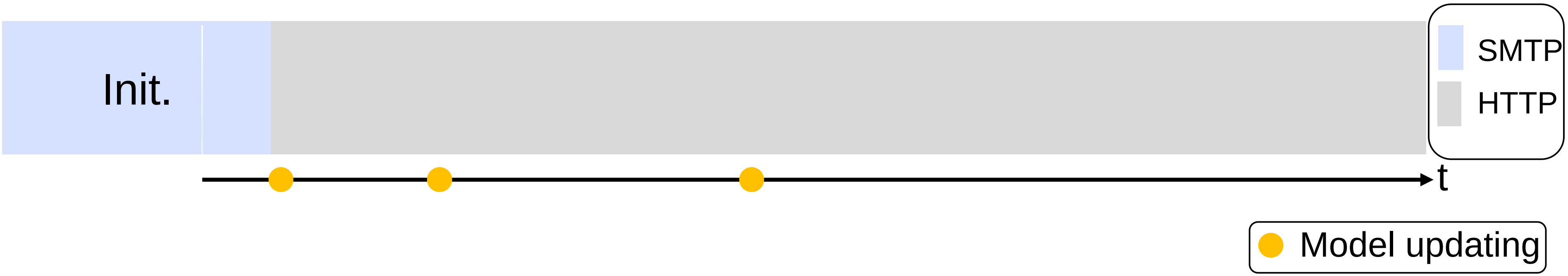


Experiments

3. Reaction of concept drift (SMTP+HTTP)

- Concept drift happened between SMTP and HTTP

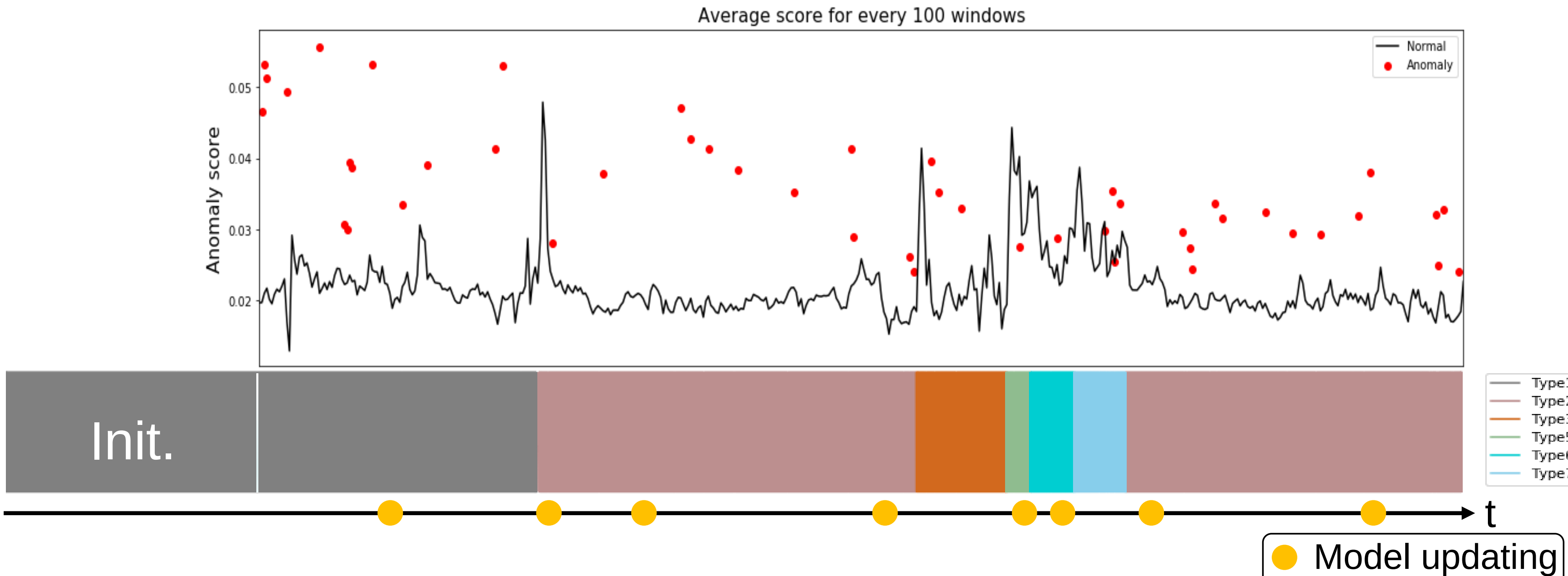




Experiments

3. Reaction of concept drift (FOREST)

- Data arrive type by type
- After each type change, performance is shortly influenced
- Model updating in time



Conclusion and outlook

- Contributions
  - Robust detection of contextual anomaly
  - In time and efficient online model updating
  - Keep hard data for model updating
- Future work
  - Adaptive model updating according to different data coming rate
  - Optimal hyperparameters learning approach for different data (Buffer size, hard window criterion etc.)

Thanks for your attention.

Q&A

References

[Schölkopf et al.] Bernhard Schölkopf, Robert C Williamson, Alex J Smola, John Shawe-Taylor, John C Platt Support Vector Method for Novelty Detection. 2000.

[Tax and Duin] David M.J. Tax, Robert P.W. Duin. Support Vector Data Description. 2004.

[Breunig et al.] Markus M. Breunig, Hans-Peter Kriegel, Raymond T. Ng, Jörg Sander. LOF: Identifying Density-Based Local Outliers. 2000.

[Martinelli et al.] Marco Martinelli, Enrico Tronci, Giovanni Dipoppa, and Claudio Balducelli2. Electric power system anomaly detection using neural networks. 2004.

[Malhotra et al.] Pankaj Malhotra, Anusha Ramakrishnan, Gaurangi Anand, Lovekesh Vig, Puneet Agarwal, and Gautam Shroff. Lstm-based encoder-decoder for multi-sensor anomaly detection. 2016.

[Dong et al.] Yue Dong and Nathalie Japkowicz. Threaded ensembles of autoencoders for stream learning. 2017.

Backup

Model parameters

	Batch size	Hidden size	Window Length	nBuffer trigger size	Hard window criterion	Init. data
PowerDemand	8	15	80	9 Batches	5/10	1 000
SMTP	8	15	10	50 Batches	4/10	60 000
HTTP	8	35	30	100 Batches	5/30	100 000
SMTP+HTTP	8	15	10	100 Batches	4/10	60 000
ForestCover	8	25	10	100 Batches	9/10	100 000

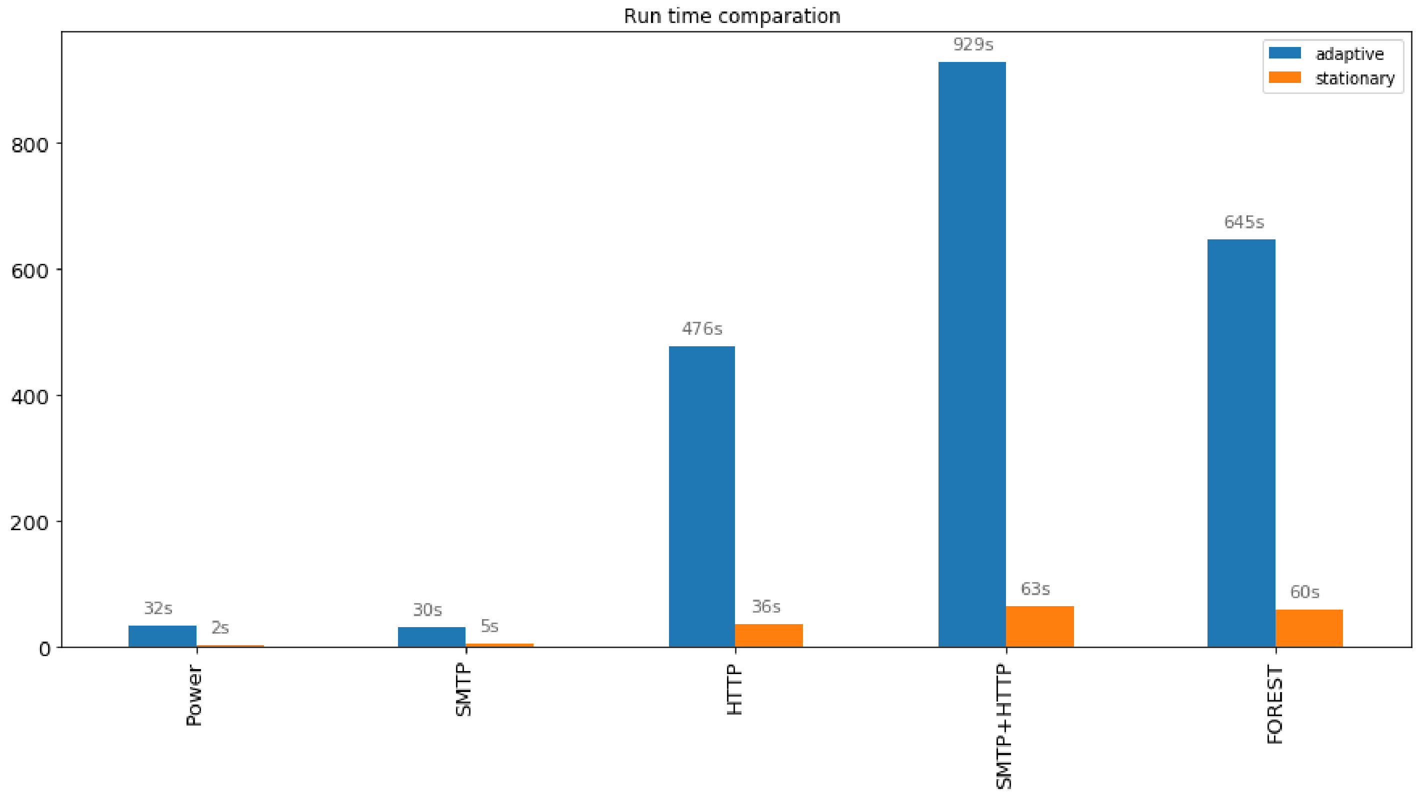
Backup

Adam Optimizer (Default parameters in TensorFlow)

- Learning rate (0.001)
  - The proportion that weights are updated
- beta1 (0.9)
  - The exponential decay rate for the first moment estimates
- beta2 (0.999)
  - The exponential decay rate for the second-moment estimates
- epsilon (1e-08)
  - To prevent any division by zero in the implementation
- Loss function
  - RMSE

Backup

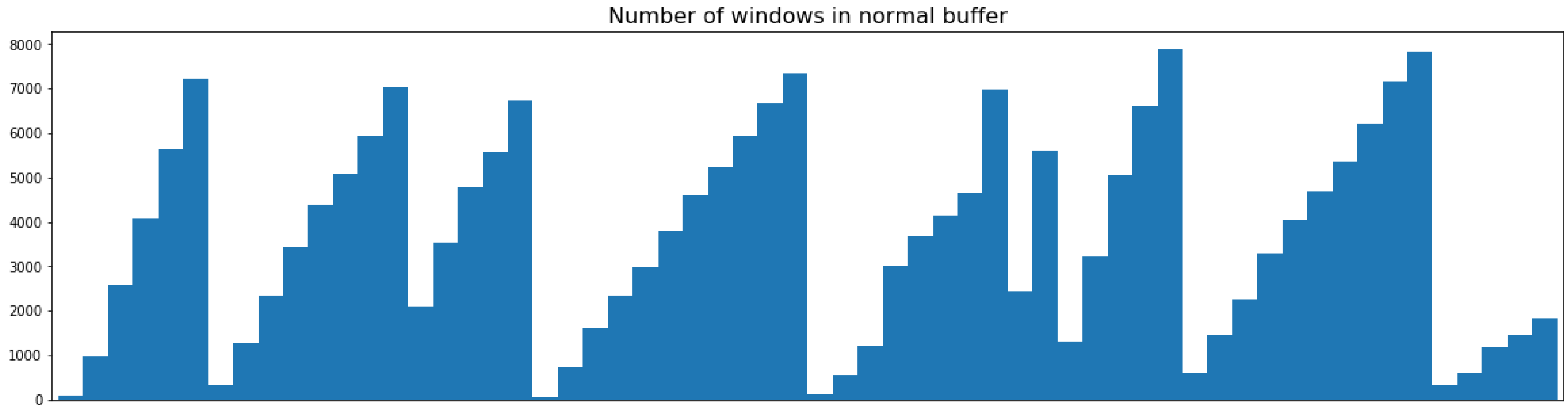
Run time compare: With & without updating

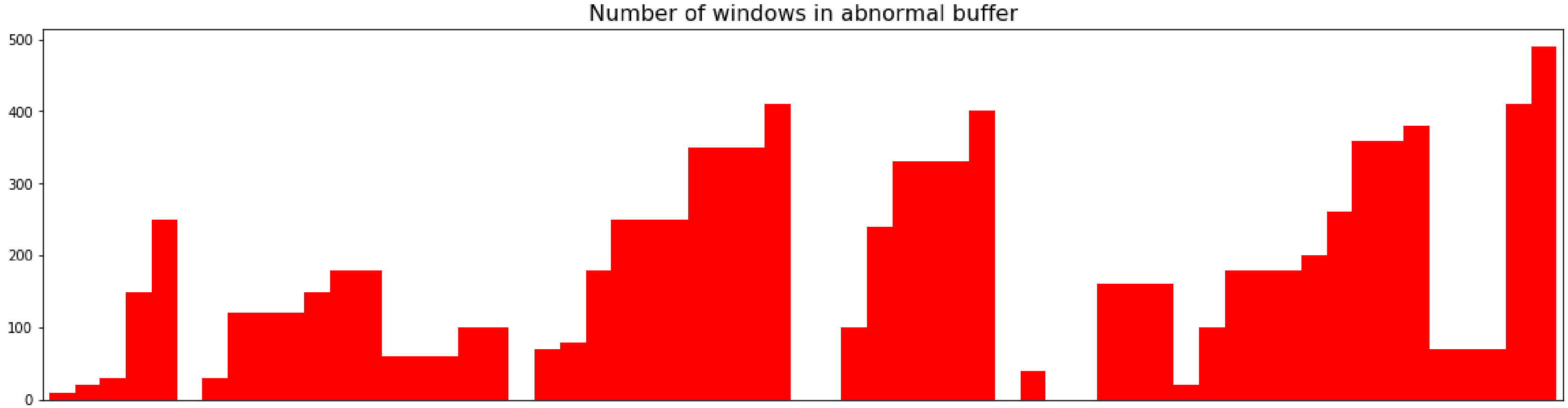


- All experiments ran on 2.6-GHz Intel Core i7 CPU with 16-GB RAM

Backup

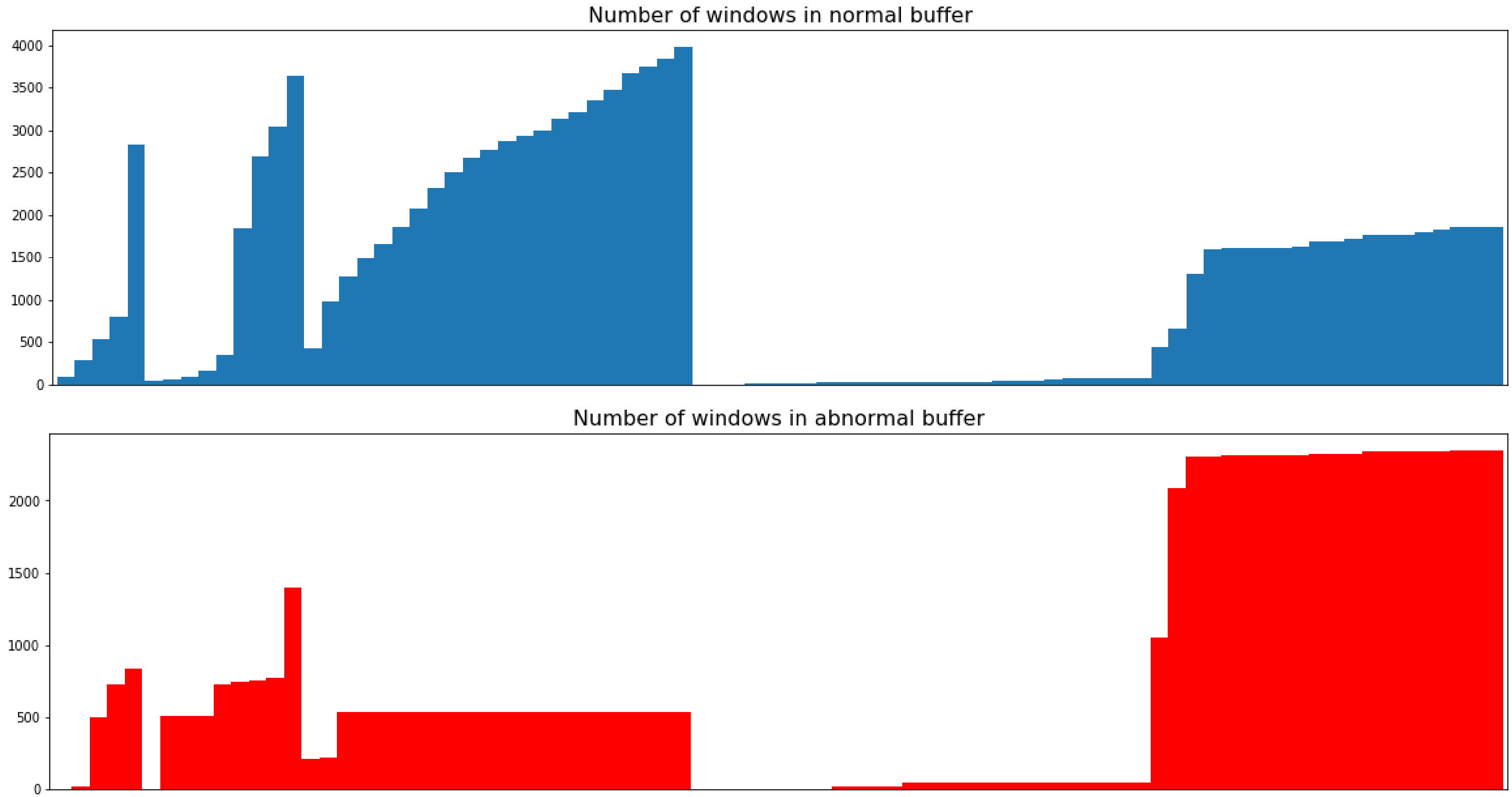
ForestCover buffer





Backup

SMTP+HTTP buffer



Experiments

Reaction of concept drift (SMTP+HTTP)

- Concept drift happened between SMTP and HTTP

Dashed lines: Model updating