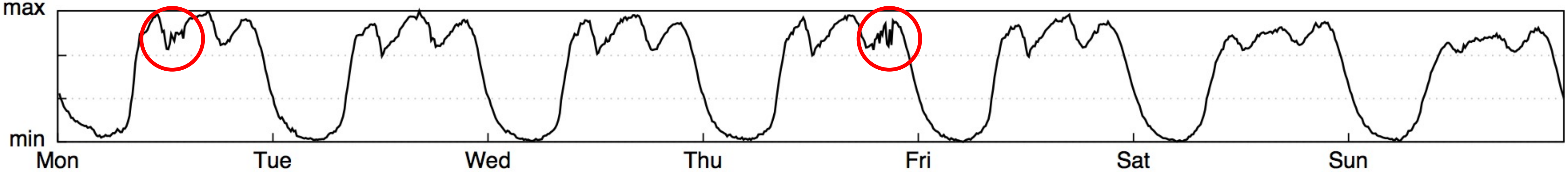
Unsupervised Anomaly Detection

- Rule-based (e.g. static threshold, regular expression) anomaly detection does not work
- Labels are in general not available
  - Have to be labeled by experts, thus cannot be crowdsourced
  - Experts are unwilling to label, even though they are the users of the tool
- Common idea: somehow capture the "normal" patterns in the historical data (metrics, logs, HTTP requests), then any new data points that "deviate" from the normal patterns are considered "anomalous".

Dapeng Liu (liudp10@mails.tsinghua.edu.cn)

Metrics (Univariate Time Series) Anomaly Detection



Page views (PV) of Baidu

Metrics: A set of performance measures that evaluate the service quality or entity status

Metric anomalous (unexpected) behaviors → Potential failures, bugs, attacks…

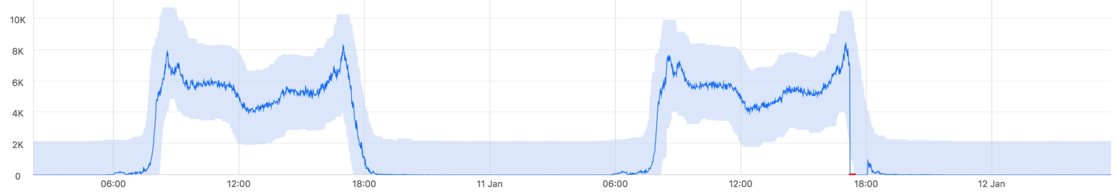
Anomaly detection matters: Find anomalous behaviors of the metric curve

→ Diagnose and fix it

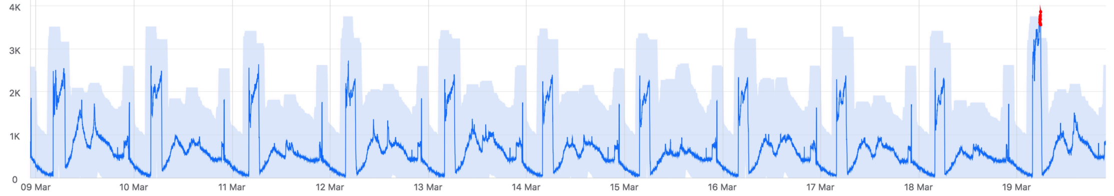
→ Avoid further influences and revenue losses

Diverse Metrics and Their Diverse Anomalies

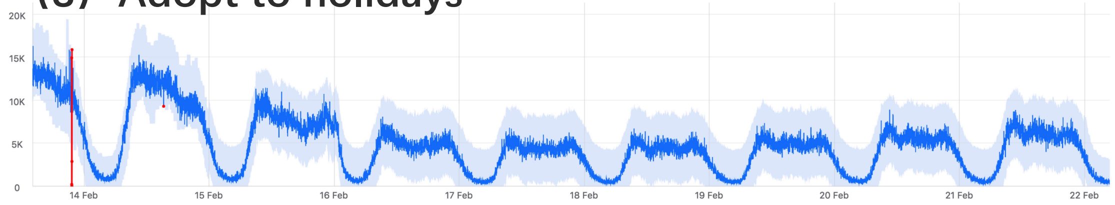
(1) Seasonal metrics



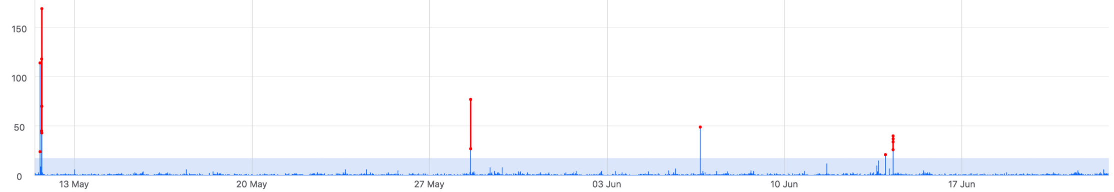
(2) Periodicity shift



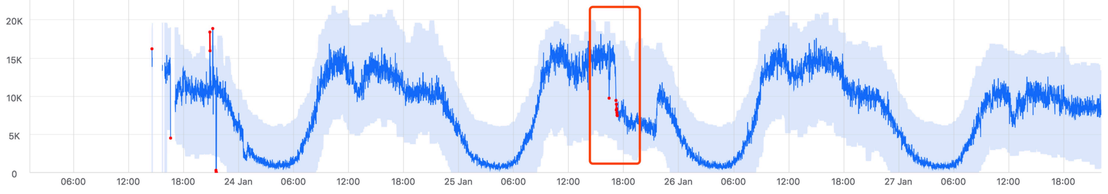
(3) Adopt to holidays



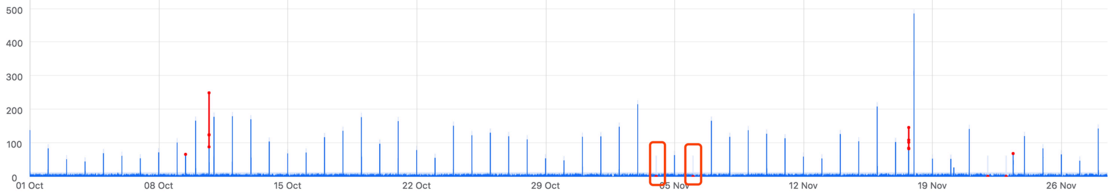
(4) Identify variable metrics and obtain extreme threshold



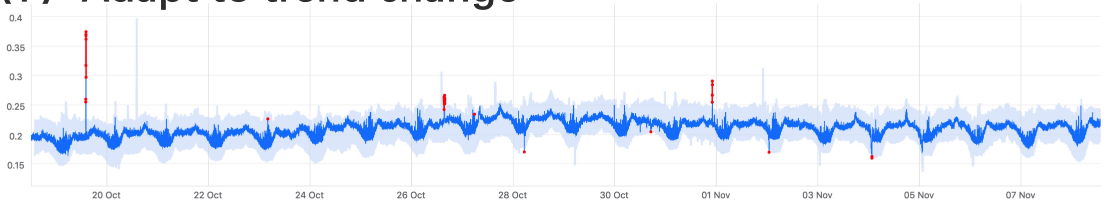
(5) Detect too rapid a change



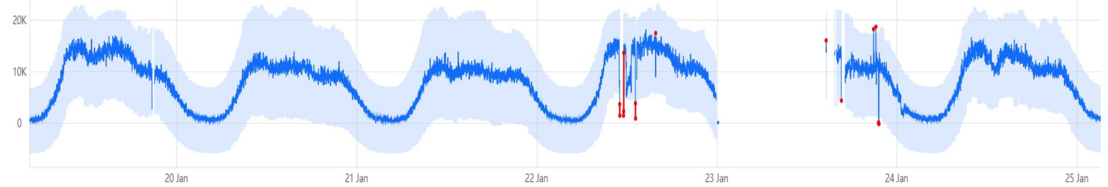
(6) Detect the lack of seasonality.



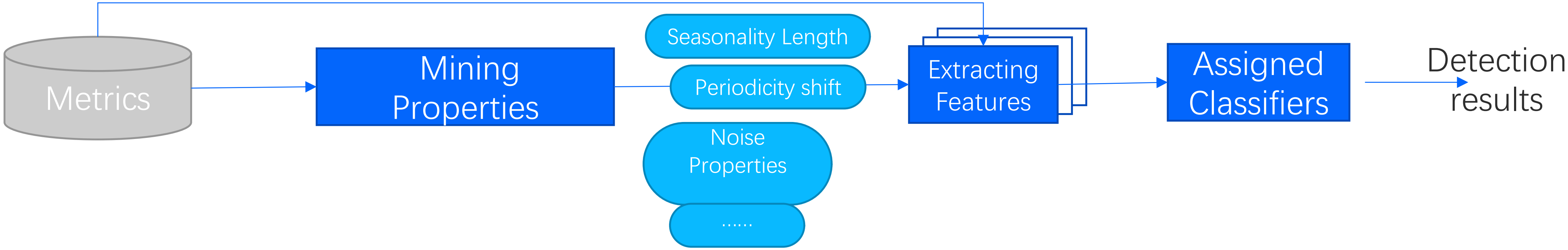
(7) Adapt to trend change

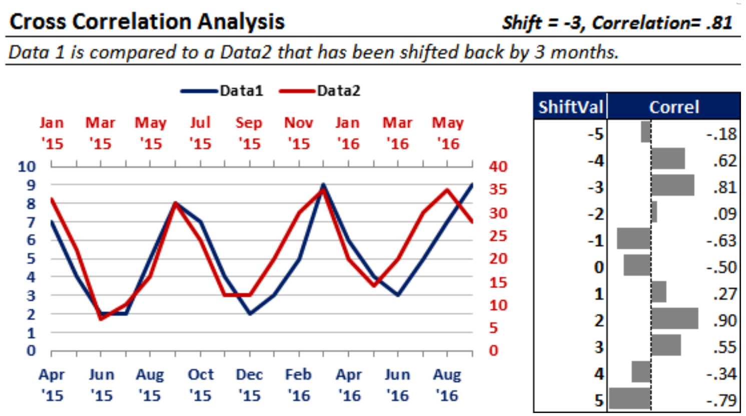


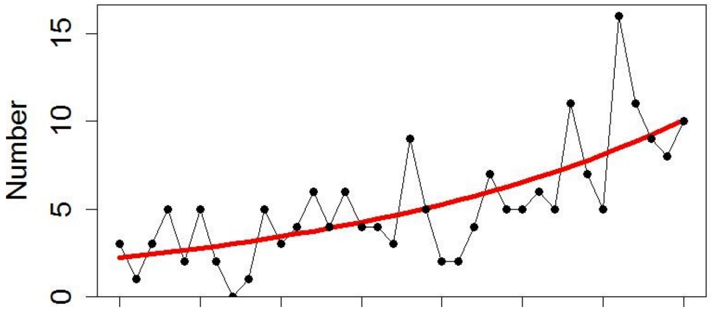
(8) Robust against data loss or interruption



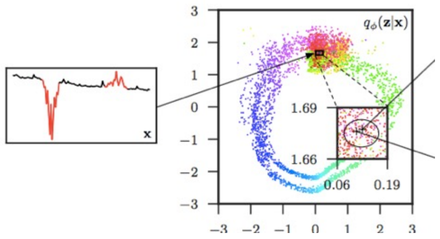
Profiling metrics and then assign appropriate algorithms



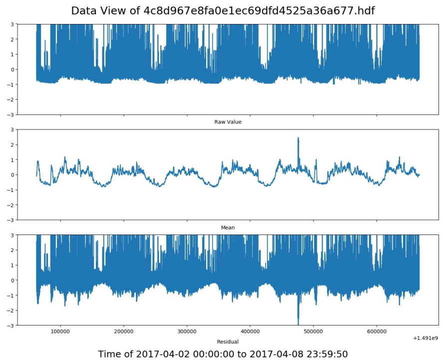




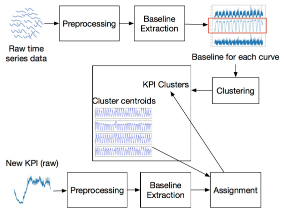
Donut: WWW2018 for smooth time series with Gaussian noises



Buzz: INFOCOM 2019 when noises are non-Gaussian



ROCKA: use cluster centroid' s trained model IWQOS 2018



Unsupervised Anomaly Detection via Variational Auto-Encoder for Seasonal KPIs in Web Applications

Haowen Xu[1] Wenxiao Chen[1] Nengwen Zhao[1] Zeyan Li[1]
Jiahao Bu[1] Zhihan Li[1] Ying Liu[1] Youjian Zhao[1] Dan Pei[1]
Yang Feng[2] Jie Chen[2] Zhaogang Wang[2] Honglin Qiao[2]

[1]Tsinghua University

[2]Alibaba Group

April 26, 2018

Existing Methods

- Statistical
  - Anomaly detectors based on traditional statistical models [INFOCOM2012]
- Supervised
  - Supervised ensemble learning with above detectors – Opprentice[IMC2015], EGADS [KDD2015]

Donut: unsupervised anomaly detection assuming smooth time series

- A recent past of W data points at time t is called a window at time t. Donut tries to model the distribution of normal windows by VAE (Variational Auto Encoder) and find anomalies by likelihood.

- The Variational Autoencoder model:
  - Kingma and Welling, *Auto-Encoding Variational Bayes*, *International Conference on Learning Representations (ICLR)* 2014.
  - Rezende, Mohamed and Wierstra, *Stochastic back-propagation and variational inference in deep latent Gaussian models*. ICML 2014.

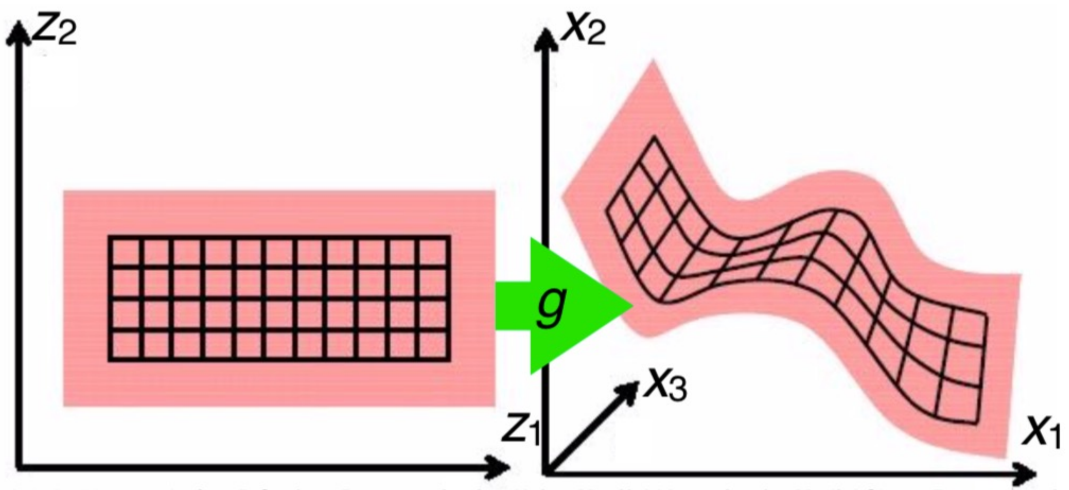
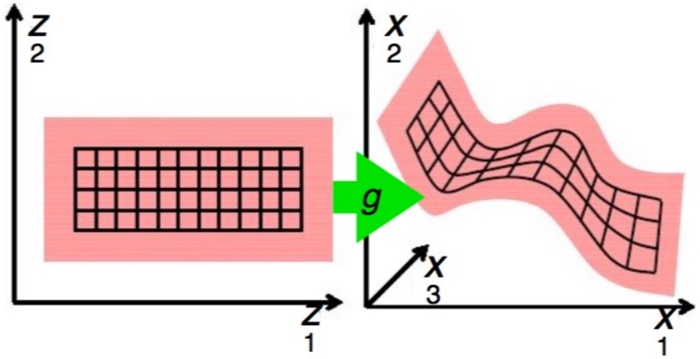
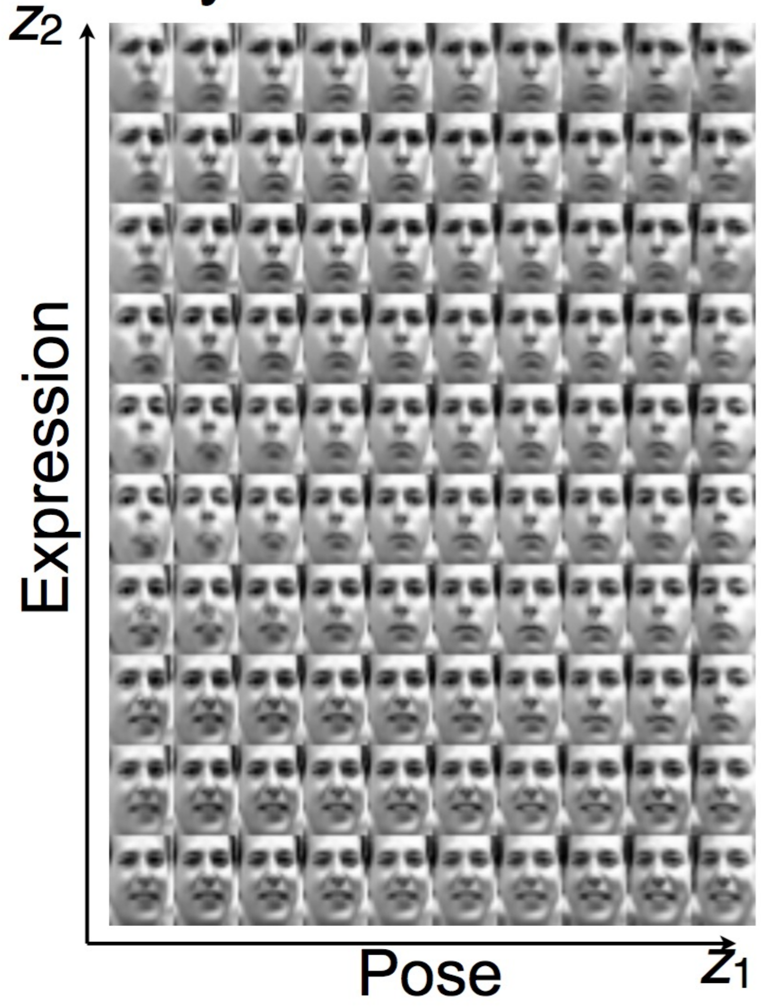


Image from: Ward, A. D., Hamarneh, G.: **3D Surface Parameterization Using Manifold Learning for Medial Shape Representation**, *Conference on Image Processing, Proc. of SPIE Medical Imaging*, 2007 7

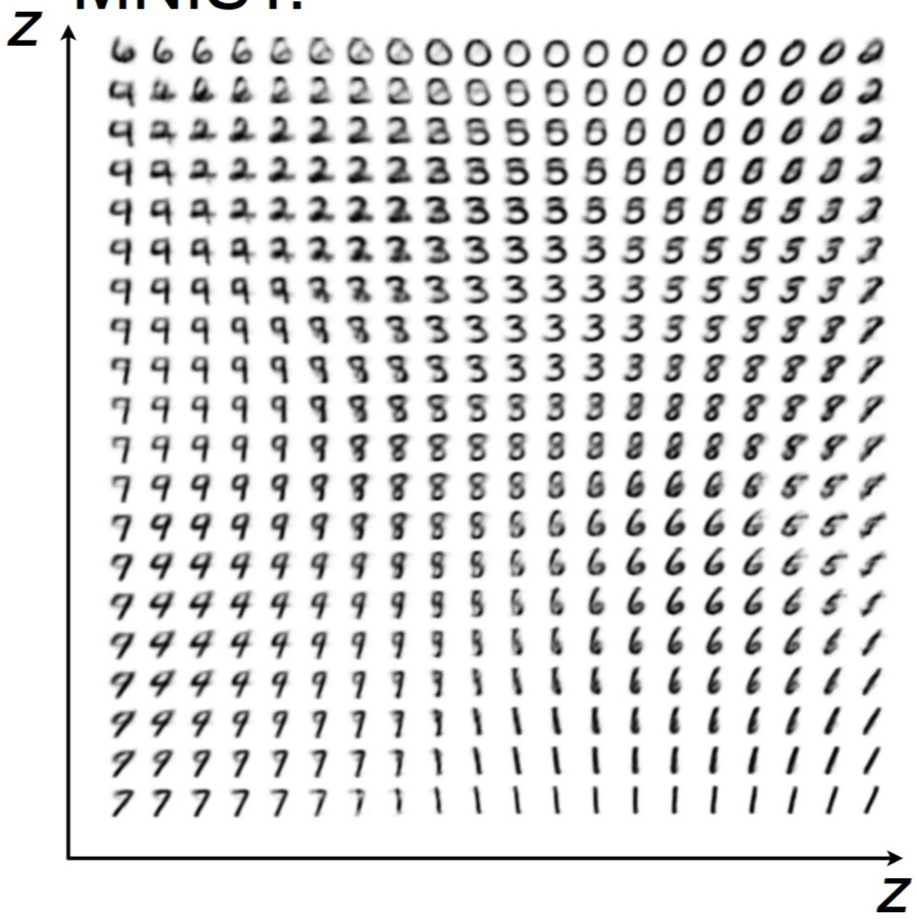
Latent Variable Models



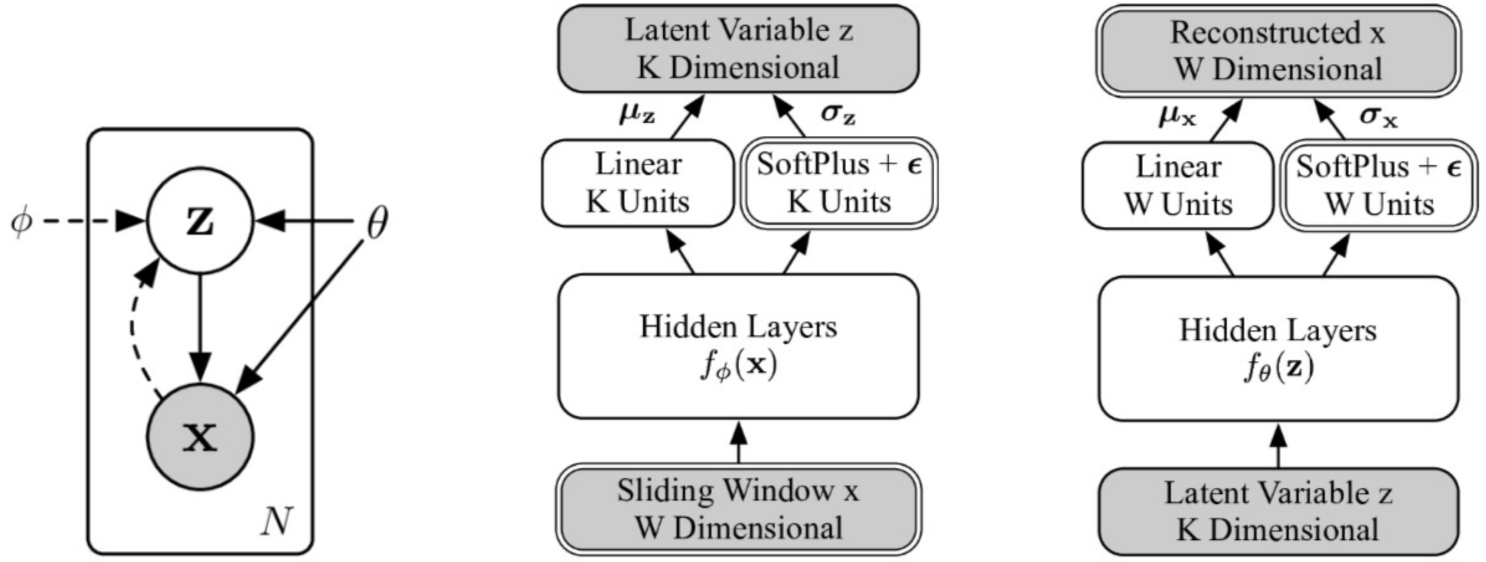
Frey Faces:



MNIST:



Network Structure



(a) VAE General Structure (b) $q_\phi(\mathbf{z}|\mathbf{x})$ of *Donut* (c) $p_\theta(\mathbf{x}|\mathbf{z})$ of *Donut*

- Variational net: $q_\phi(\mathbf{z}|\mathbf{x}) = \mathcal{N}(\boldsymbol{\mu}_\mathbf{z}, {\boldsymbol{\sigma}_\mathbf{z}}^2\mathbf{I})$.
- Generative net: $p_\theta(\mathbf{z}) = \mathcal{N}(\mathbf{0}, \mathbf{I})$, $p_\theta(\mathbf{x}|\mathbf{z}) = \mathcal{N}(\boldsymbol{\mu}_\mathbf{x}, {\boldsymbol{\sigma}_\mathbf{x}}^2\mathbf{I})$.
- SoftPlus Trick: $\boldsymbol{\sigma}_\mathbf{z} = \mathrm{SoftPlus}[\mathbf{W}_{\boldsymbol{\sigma}_\mathbf{z}}^\top f_\phi(\mathbf{x}) + \mathbf{b}_{\boldsymbol{\sigma}_\mathbf{z}}] + \boldsymbol{\epsilon}$, $\mathrm{SoftPlus}[a] = \log[\exp(a) + 1]$. Similar for $\boldsymbol{\sigma}_\mathbf{x}$. (otherwise, unbounded)

$$\mathcal{L}_{vae} = \mathbb{E}_{p(\mathbf{x})}\left[\mathbb{E}_{q_\phi(\mathbf{z}|\mathbf{x})}[\log p_\theta(\mathbf{x}|\mathbf{z})] - \mathrm{KL}\left[q_\phi(\mathbf{z}|\mathbf{x}) \,\|\, p_\theta(\mathbf{z})\right]\right]$$

3D Visualization of the Latent Space

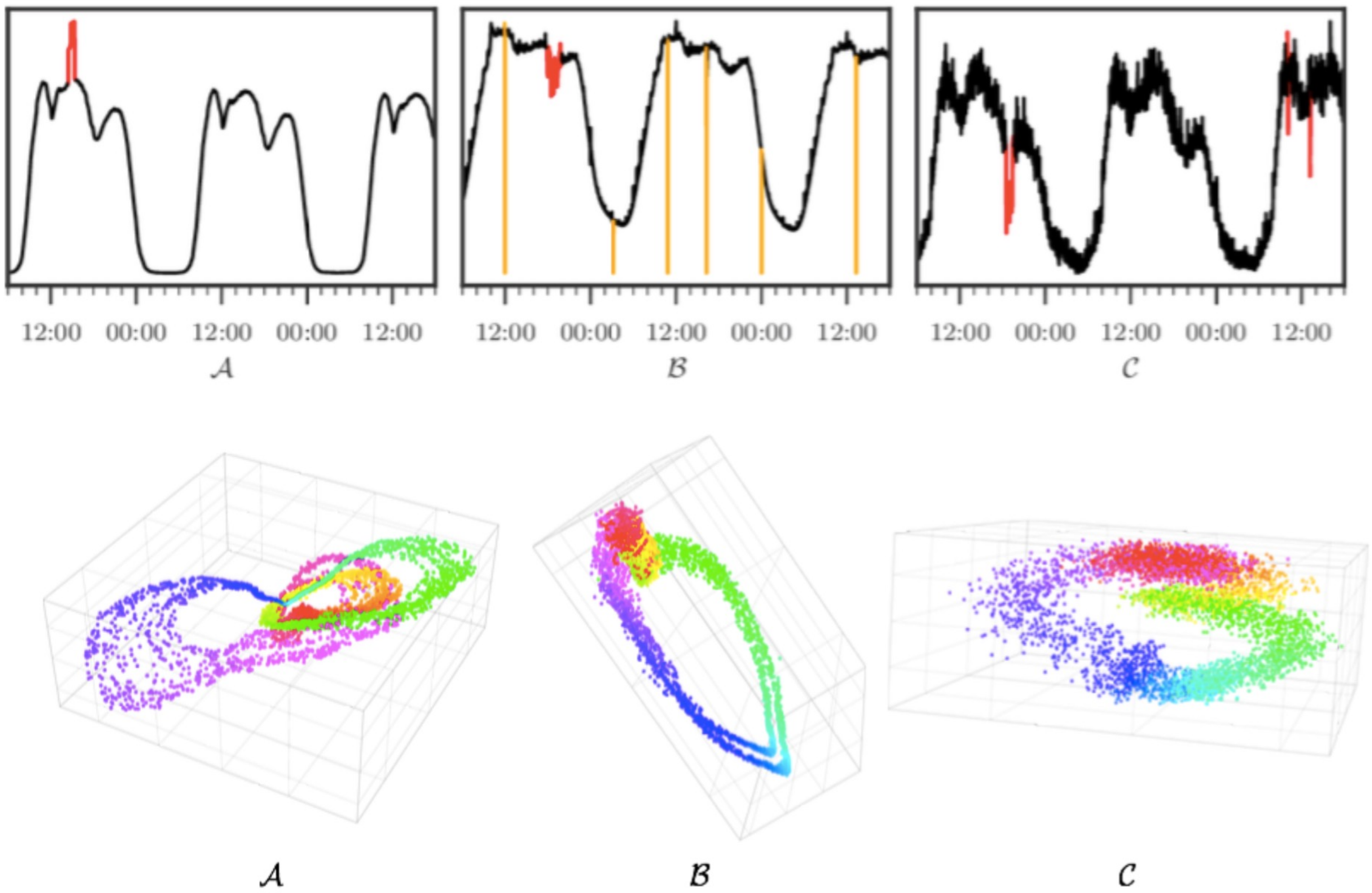
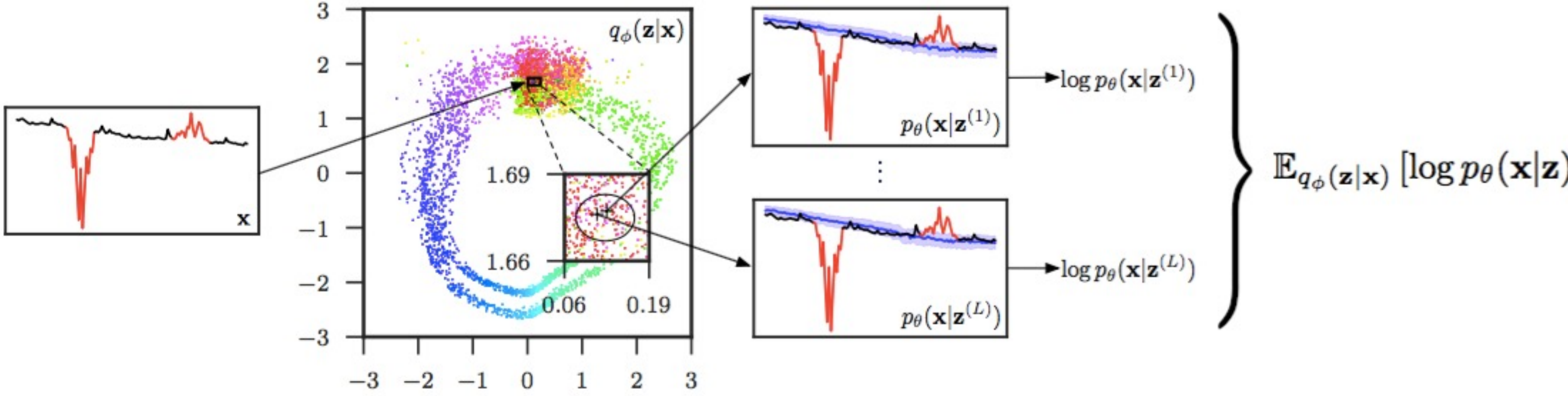
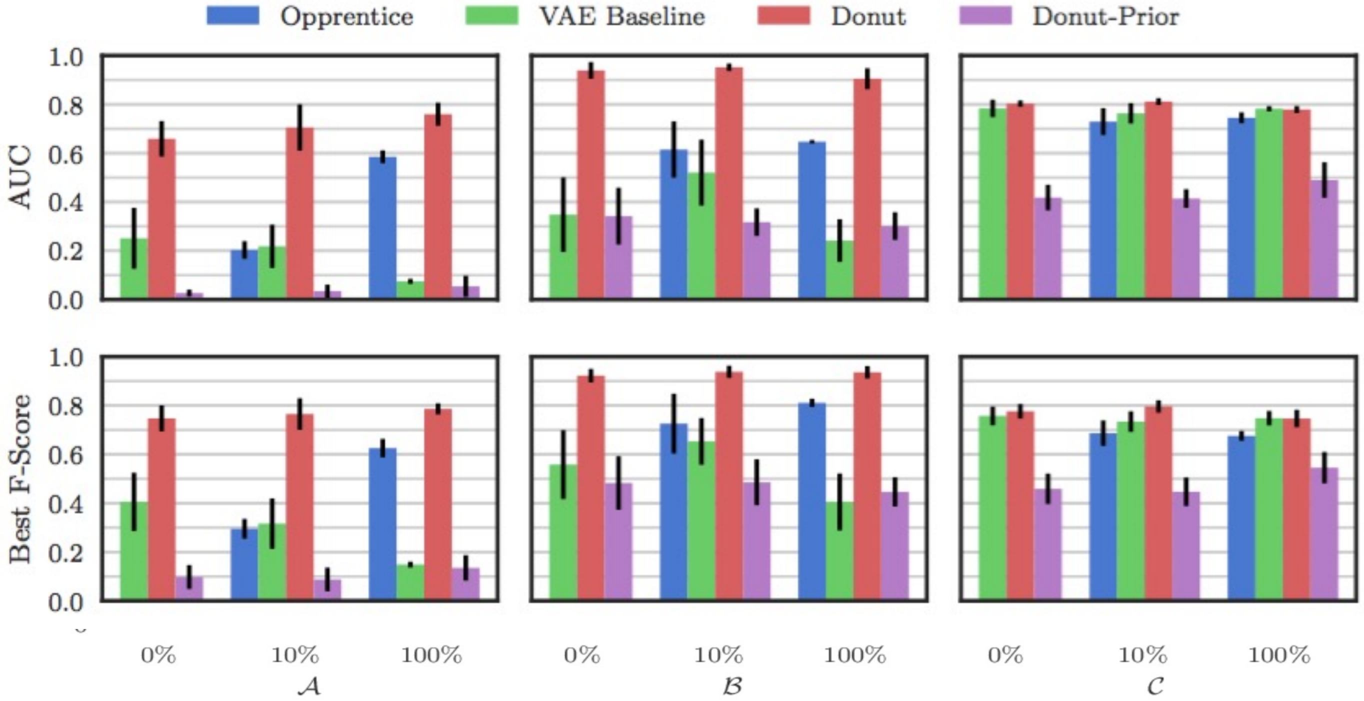


Figure 12: 3-d latent space of all three datasets.



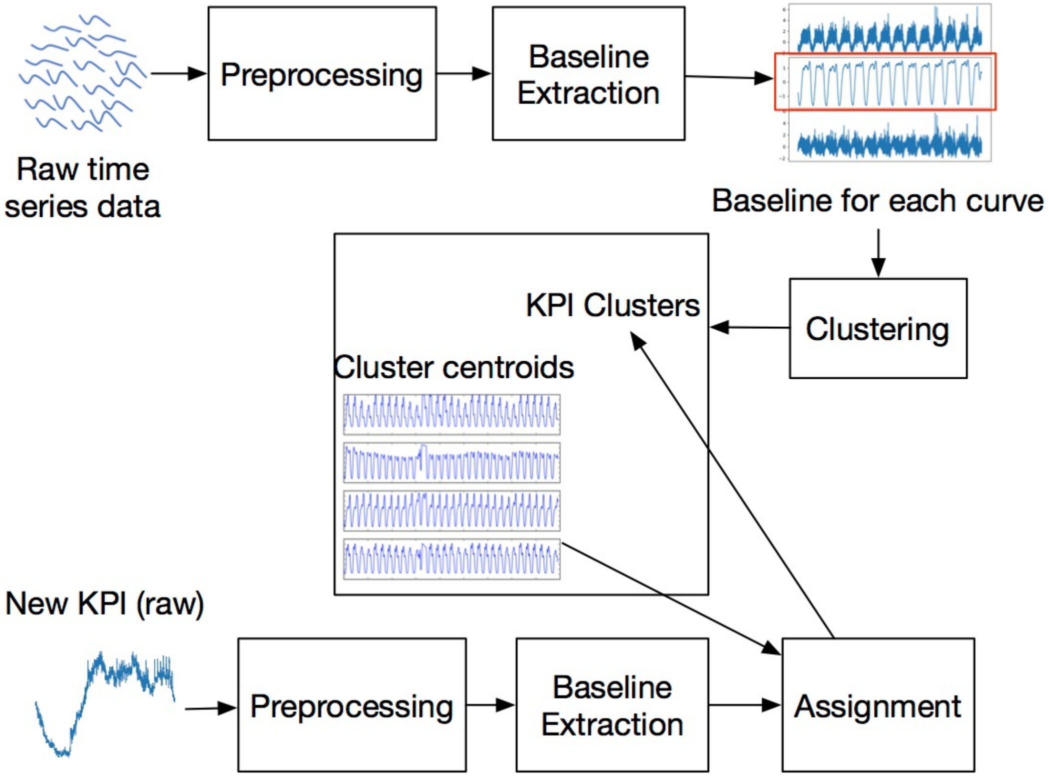


"Unsupervised KPI Anomaly Detection Through Variational Auto-Encoder"

Joint work with Alibaba, published in WWW 2018

Accuracy of 0.8~0.9，even better than supervised approach.

Clustering + Transfer Learning to reduce training overhead



IWQoS 2018

	Original DONUT [WWW2018]	ROCKA+DONUT+KPI-specific threshold
Avg. F-score	0.89	0.88
Total training time (s)	51621	5145

Thanks！

清華大學 | NetMan Tsinghua