Incorporating Feedback into Tree-based Anomaly Detection

Shubhomoy Das, Weng-Keen Wong, Alan Fern,

Thomas G. Dietterich and **Md Amran Siddiqui**

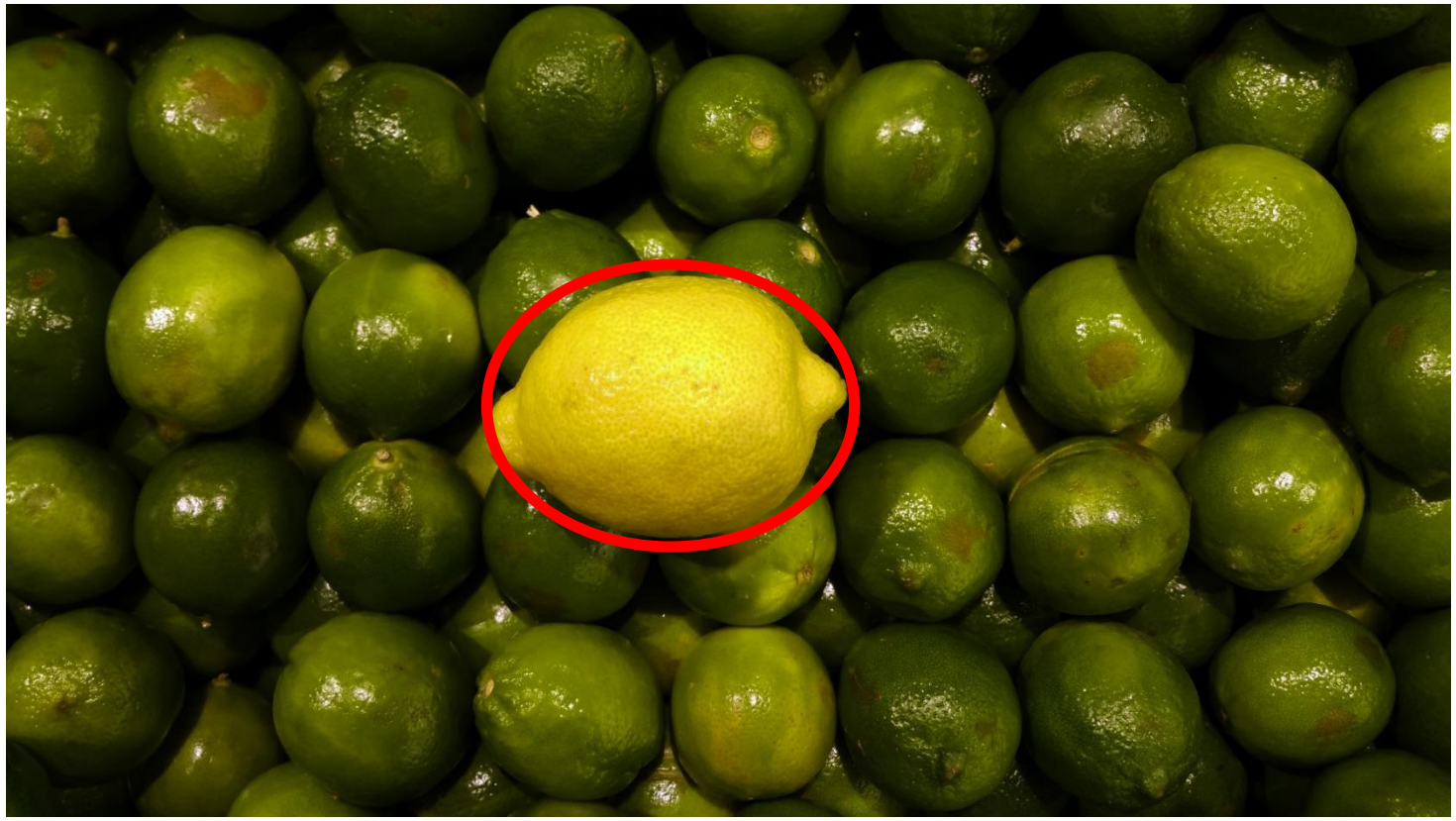
School of EECS

Anomaly Detection

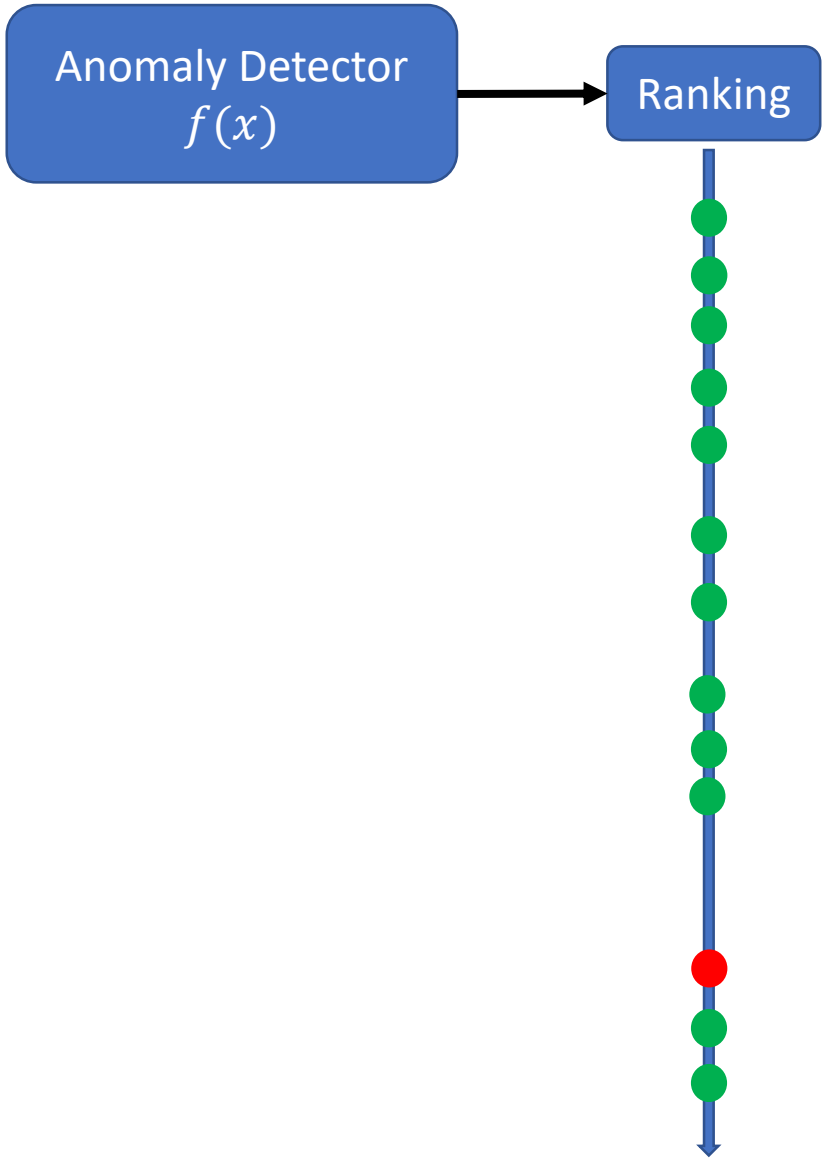
- **Goal:** Identify rare or strange objects

Anomaly Detection

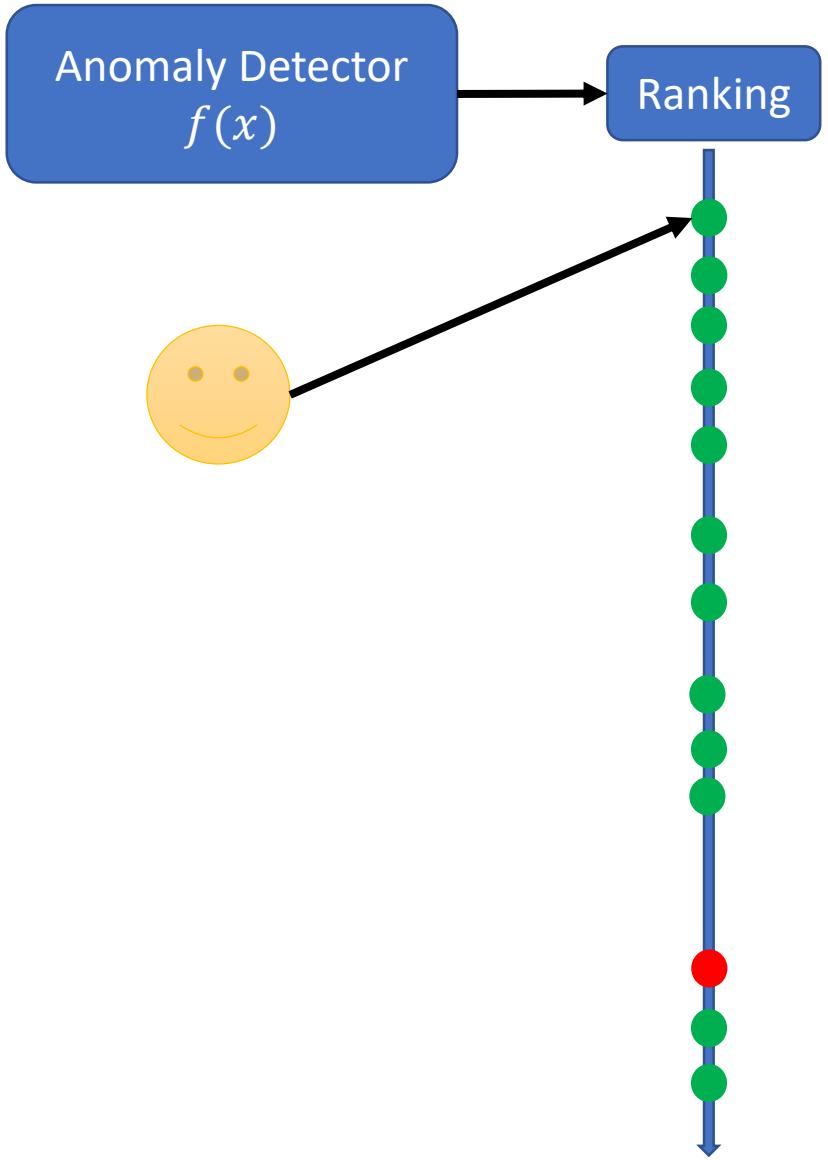
- **Goal:** Identify rare or strange objects



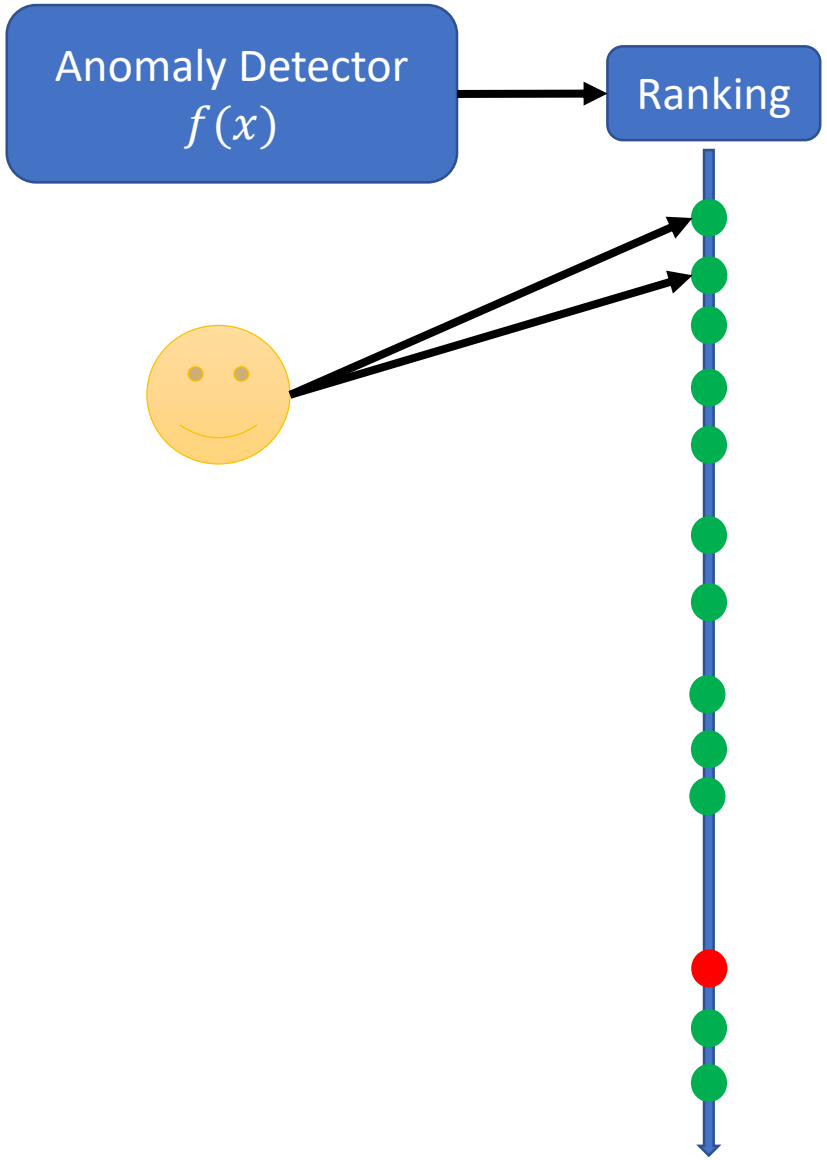
Typical Investigation



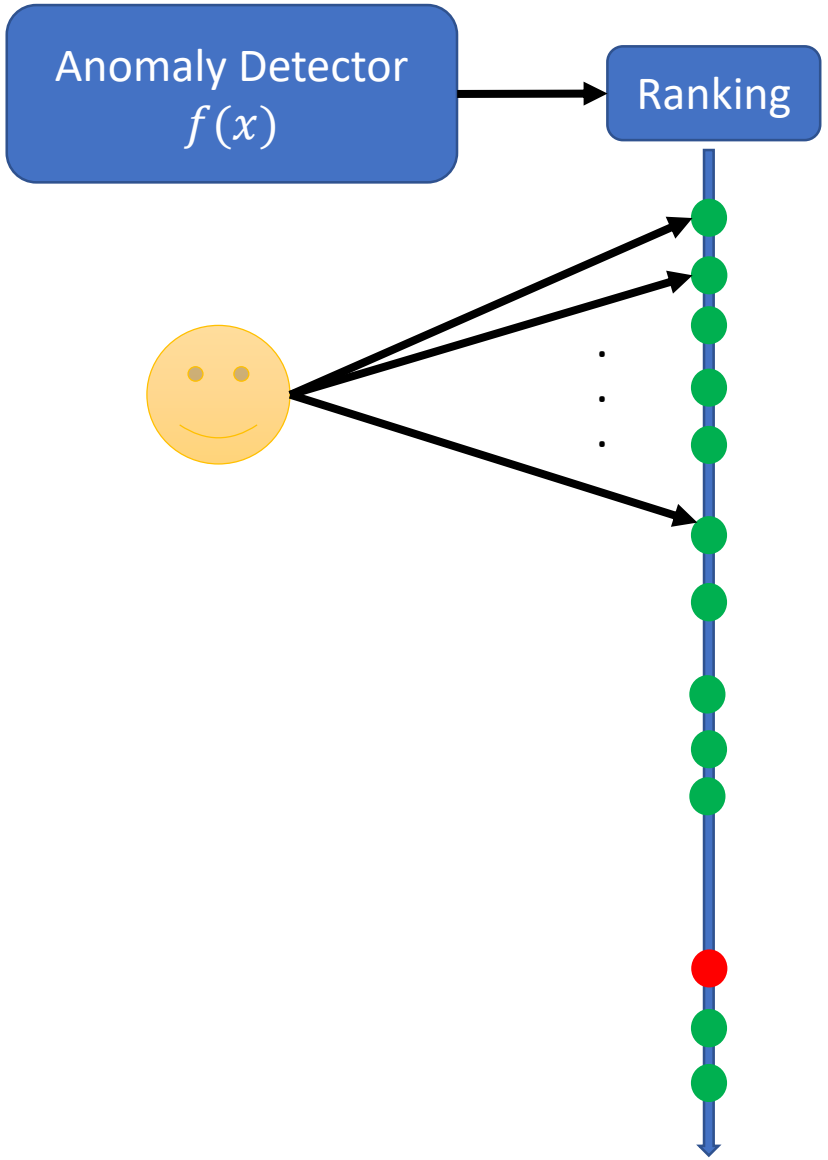
Typical Investigation



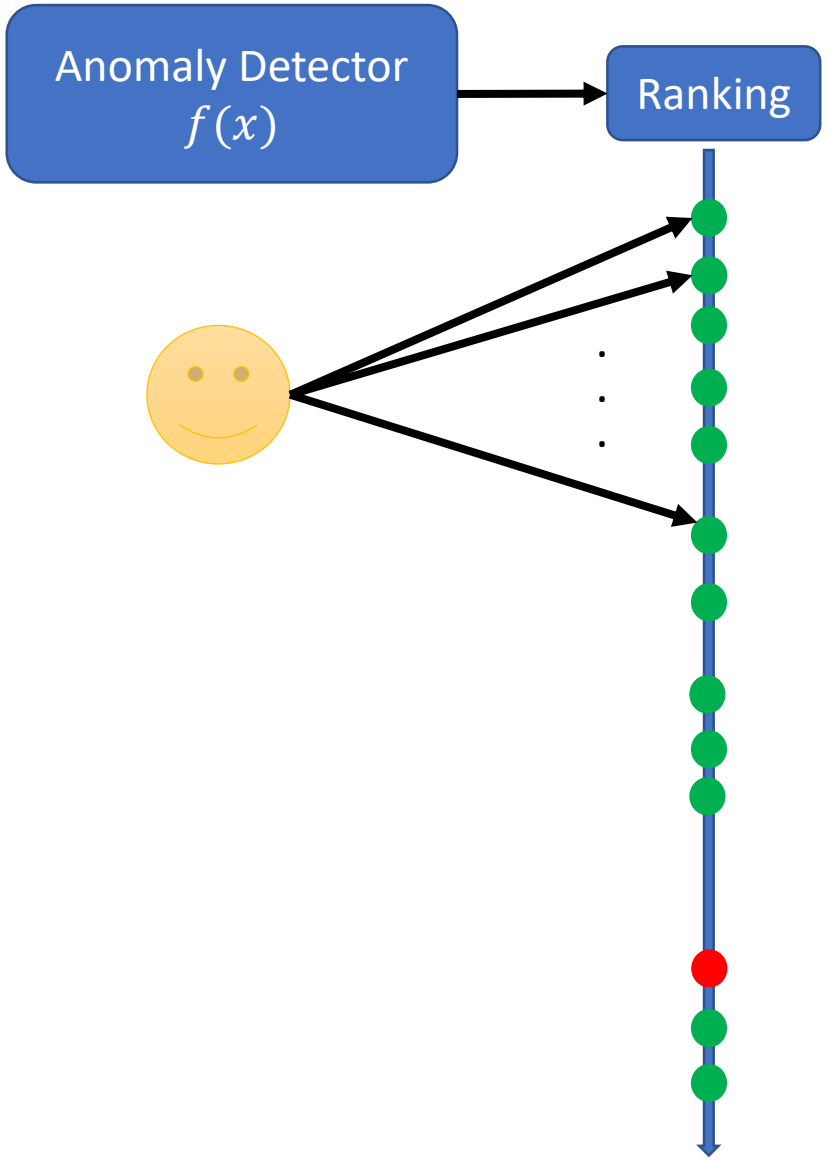
Typical Investigation



Typical Investigation

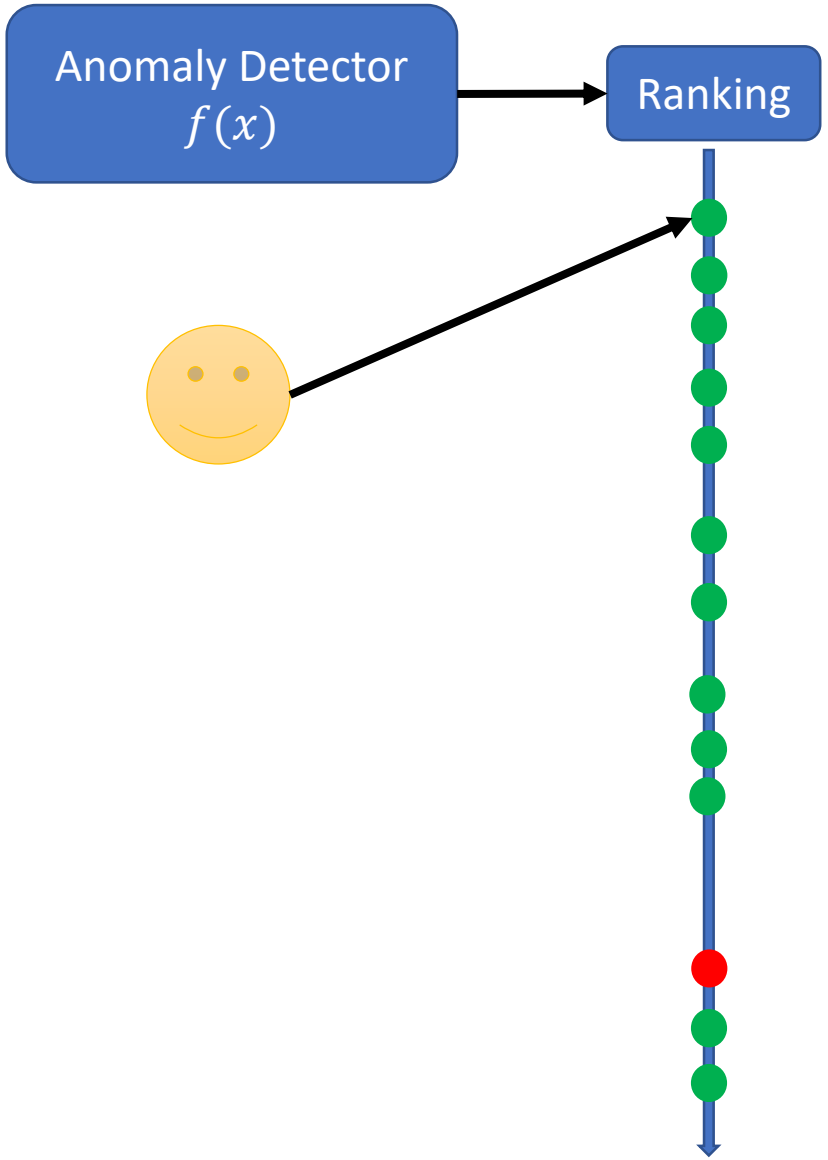


Typical Investigation

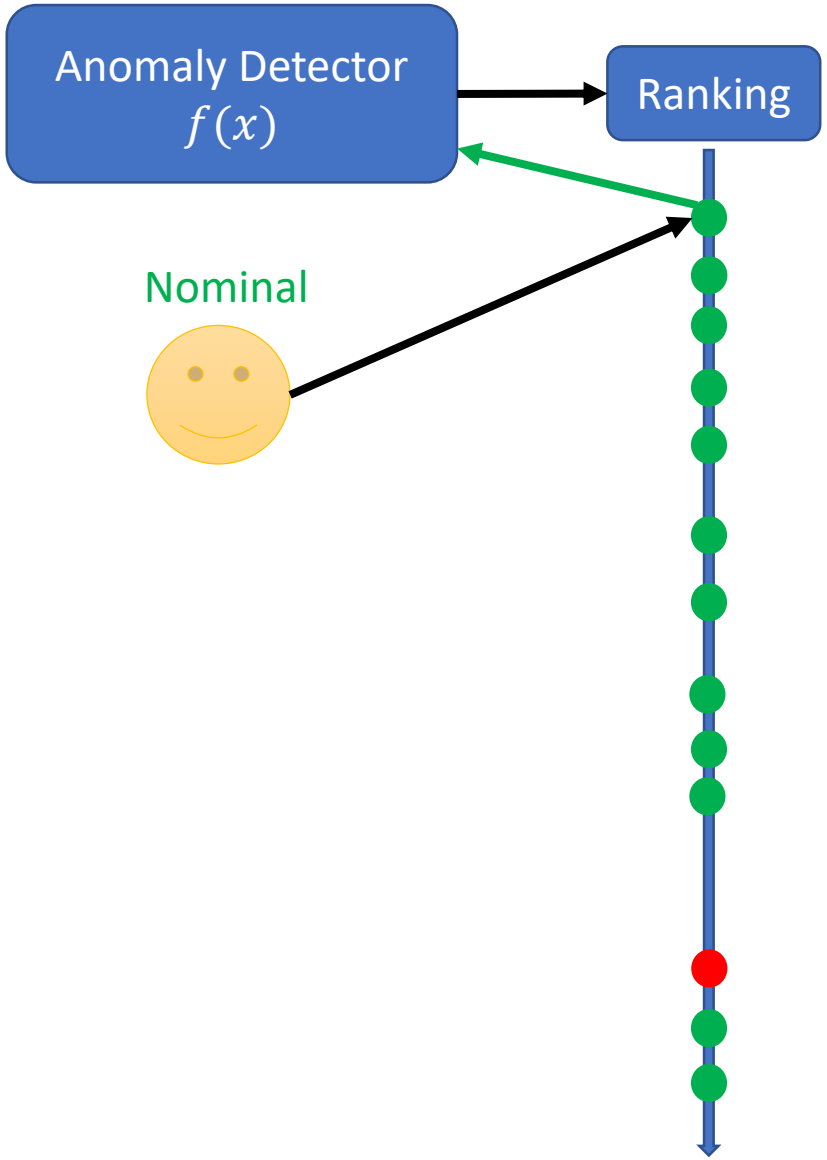


- **Major problem:** Statistical anomalies don't necessarily correspond to semantic anomalies
- Need to deal with large number of false positives

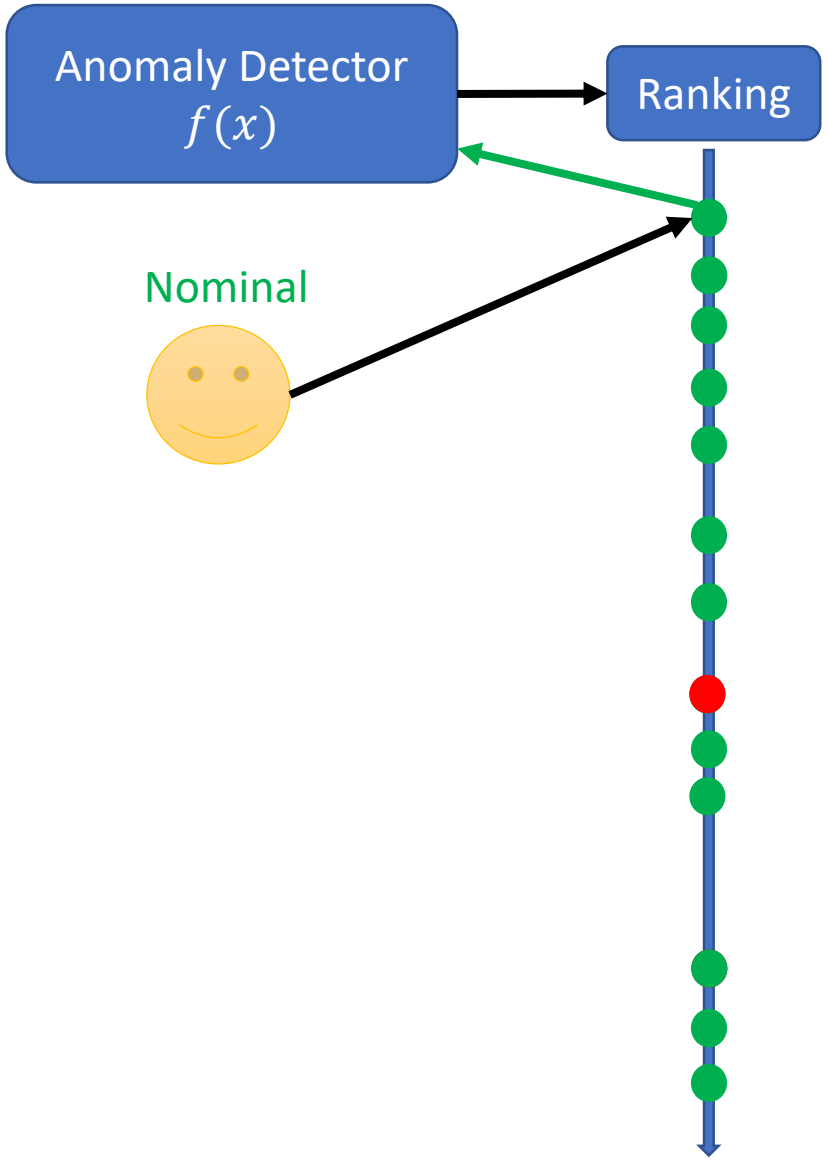
Investigation with Feedback



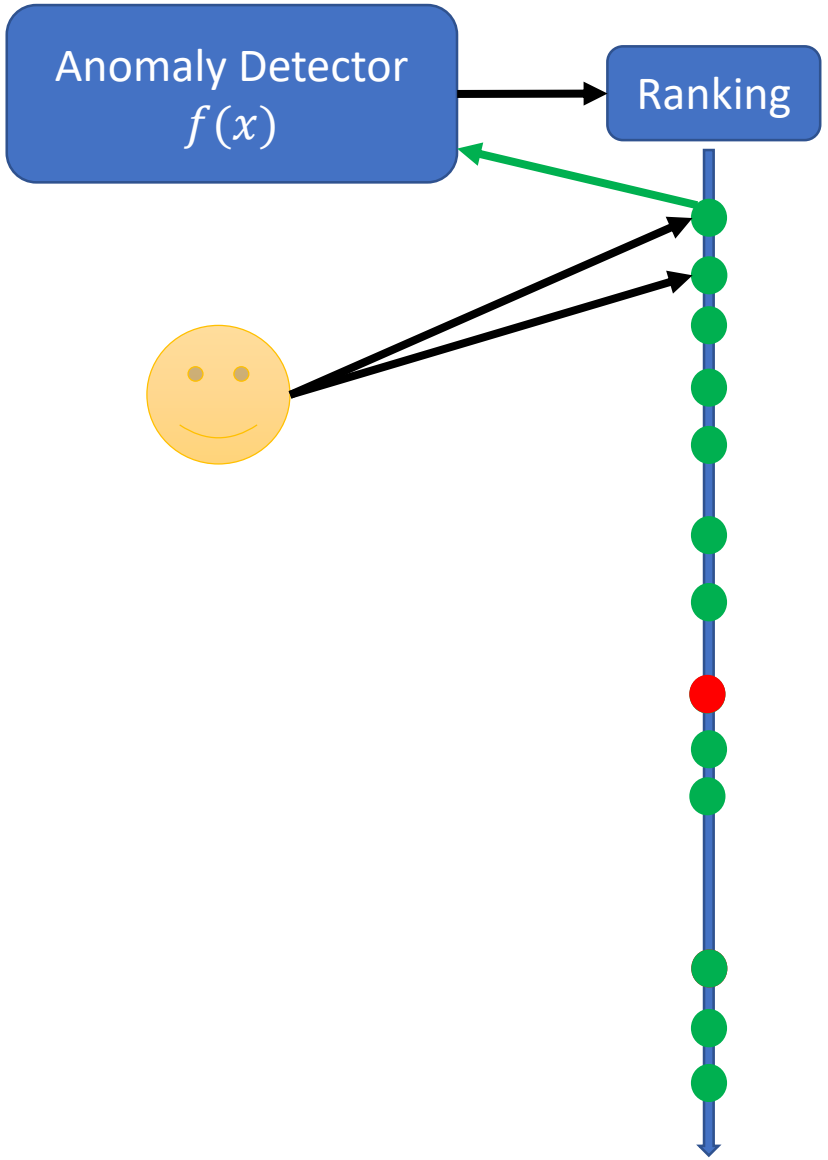
Investigation with Feedback



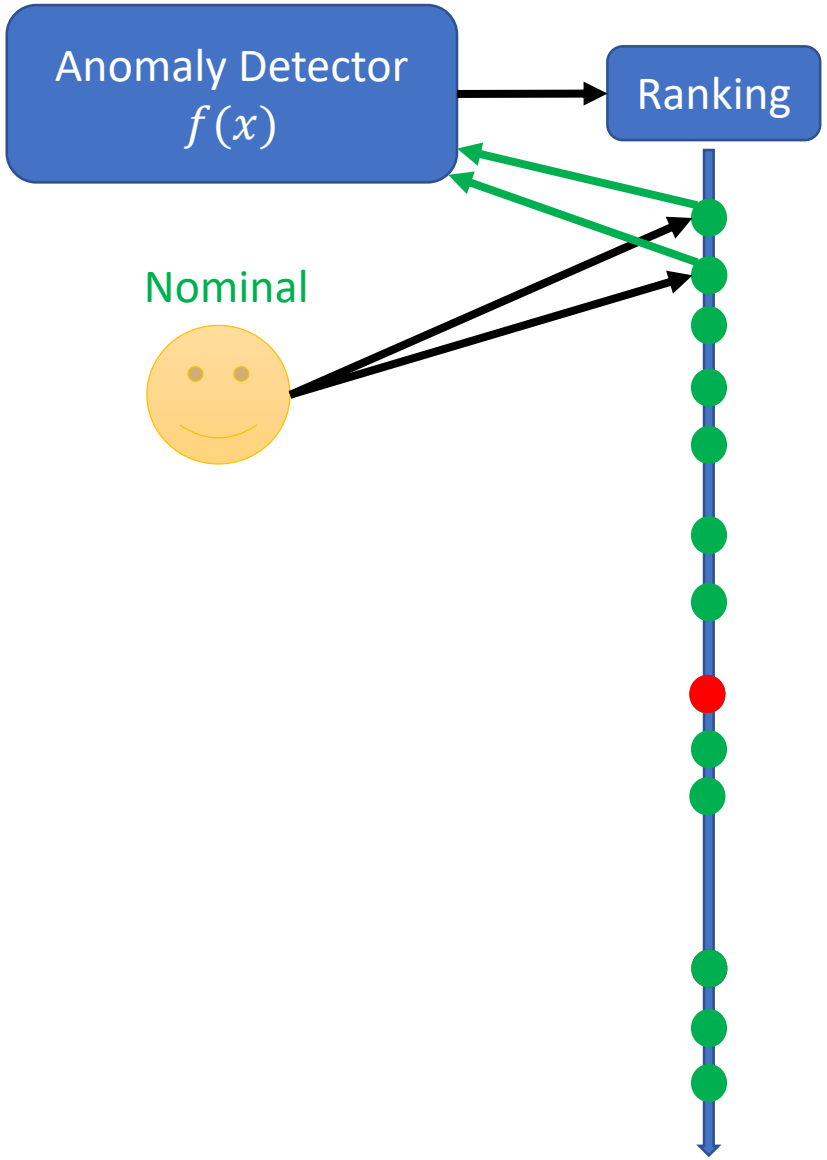
Investigation with Feedback



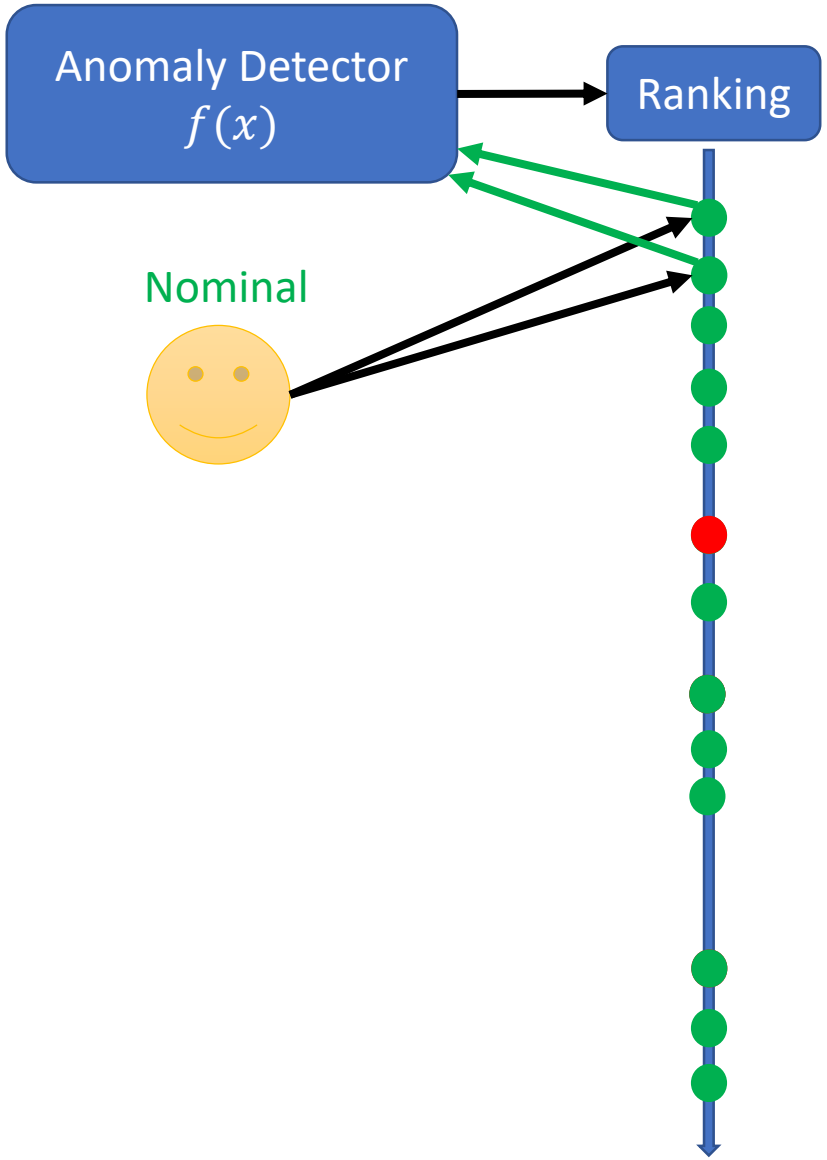
Investigation with Feedback



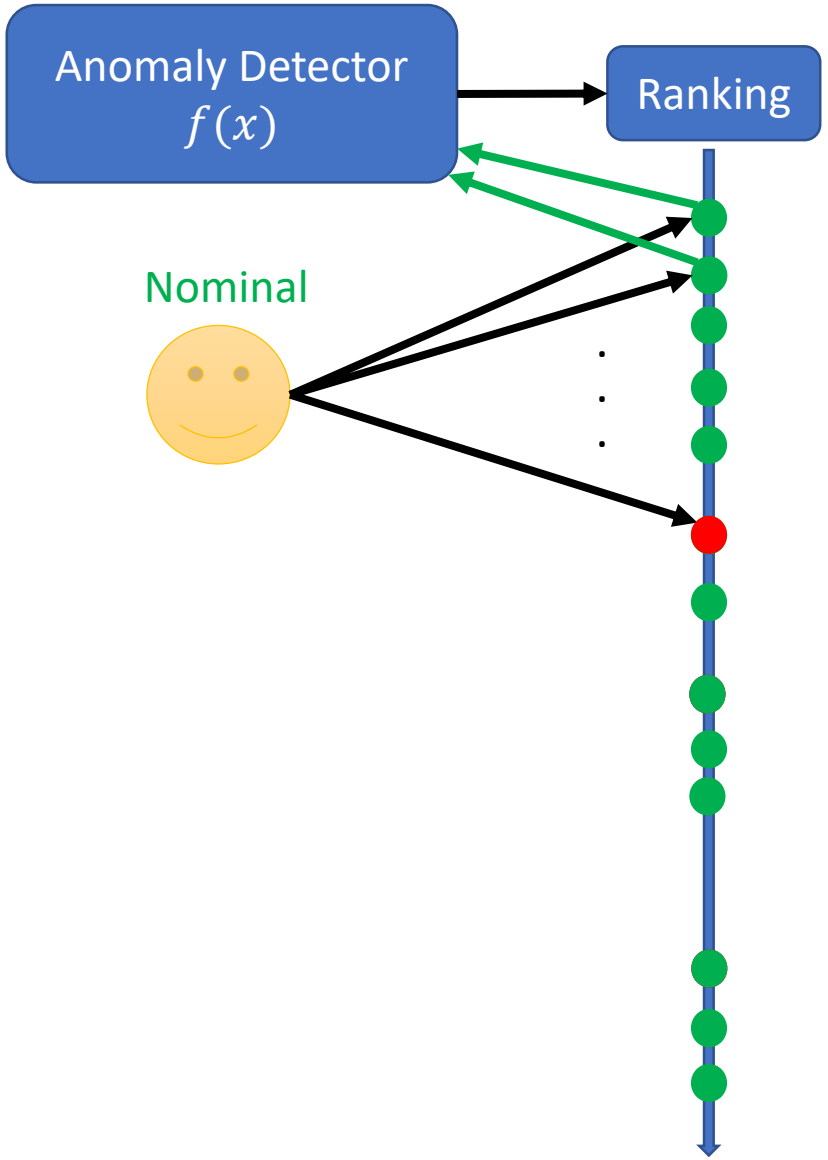
Investigation with Feedback



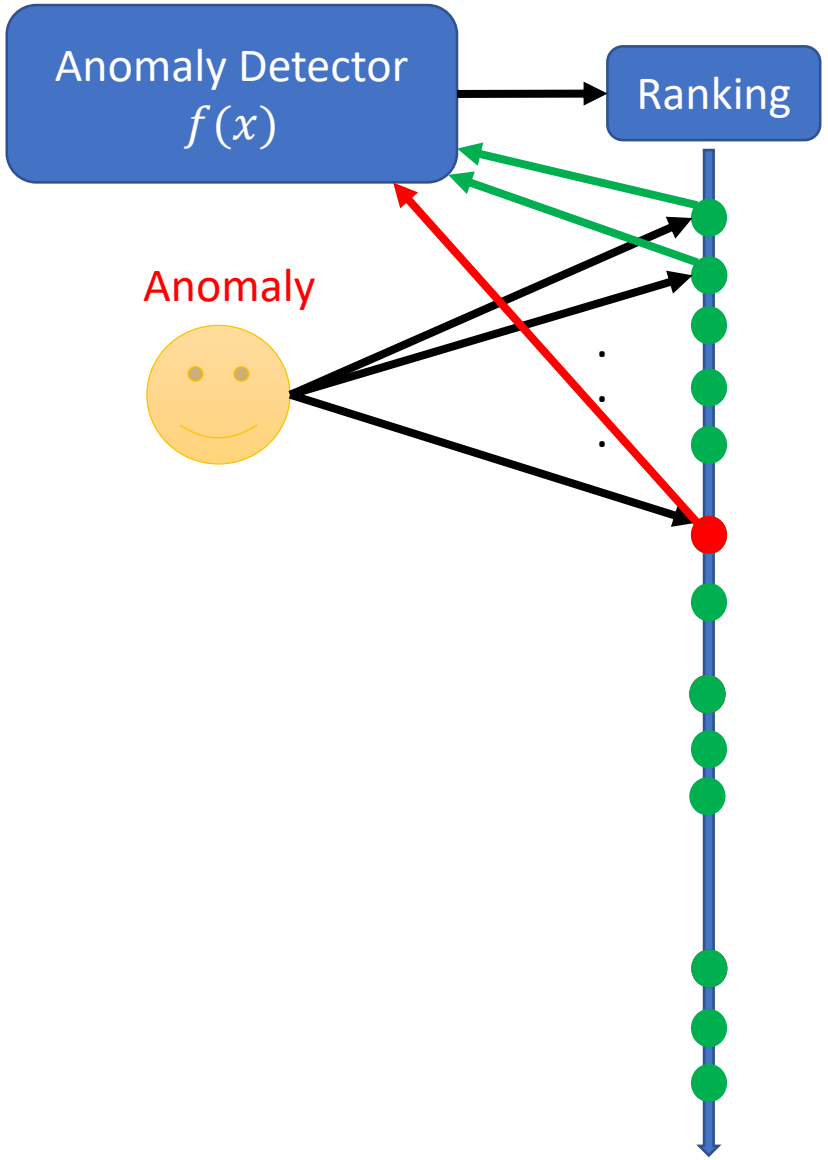
Investigation with Feedback



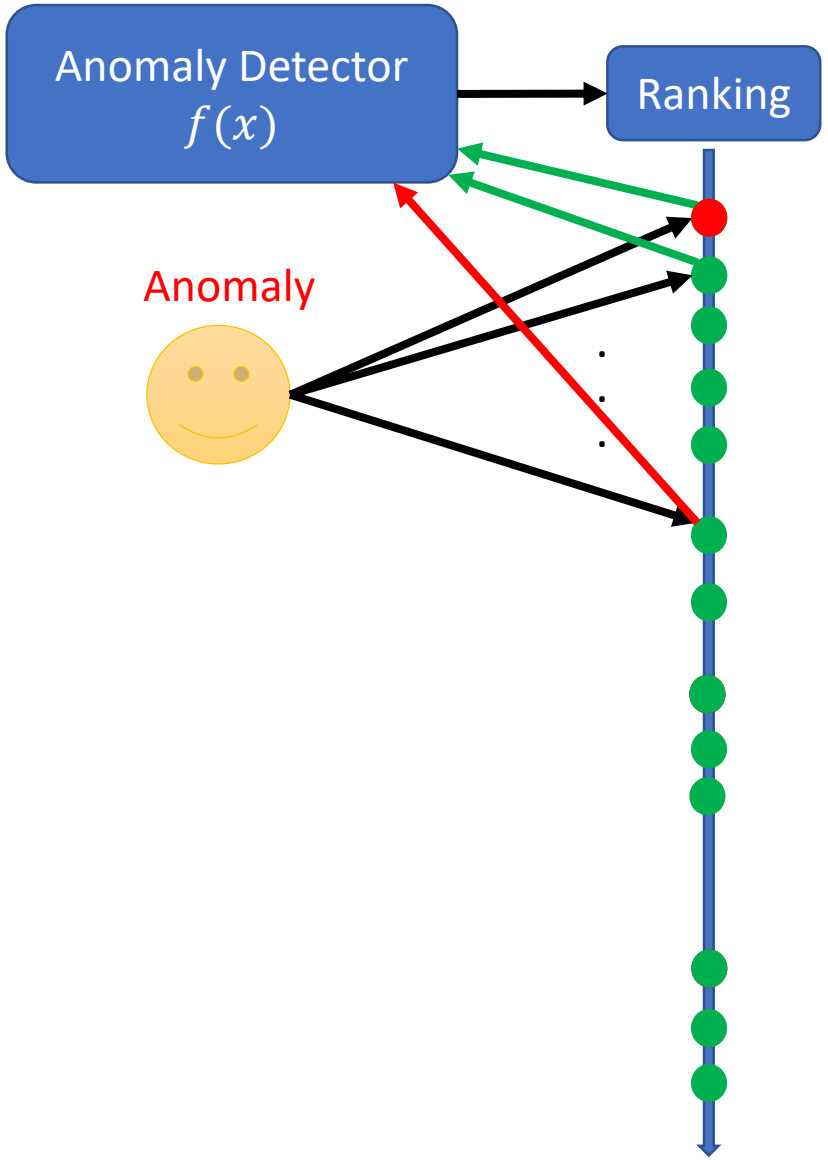
Investigation with Feedback



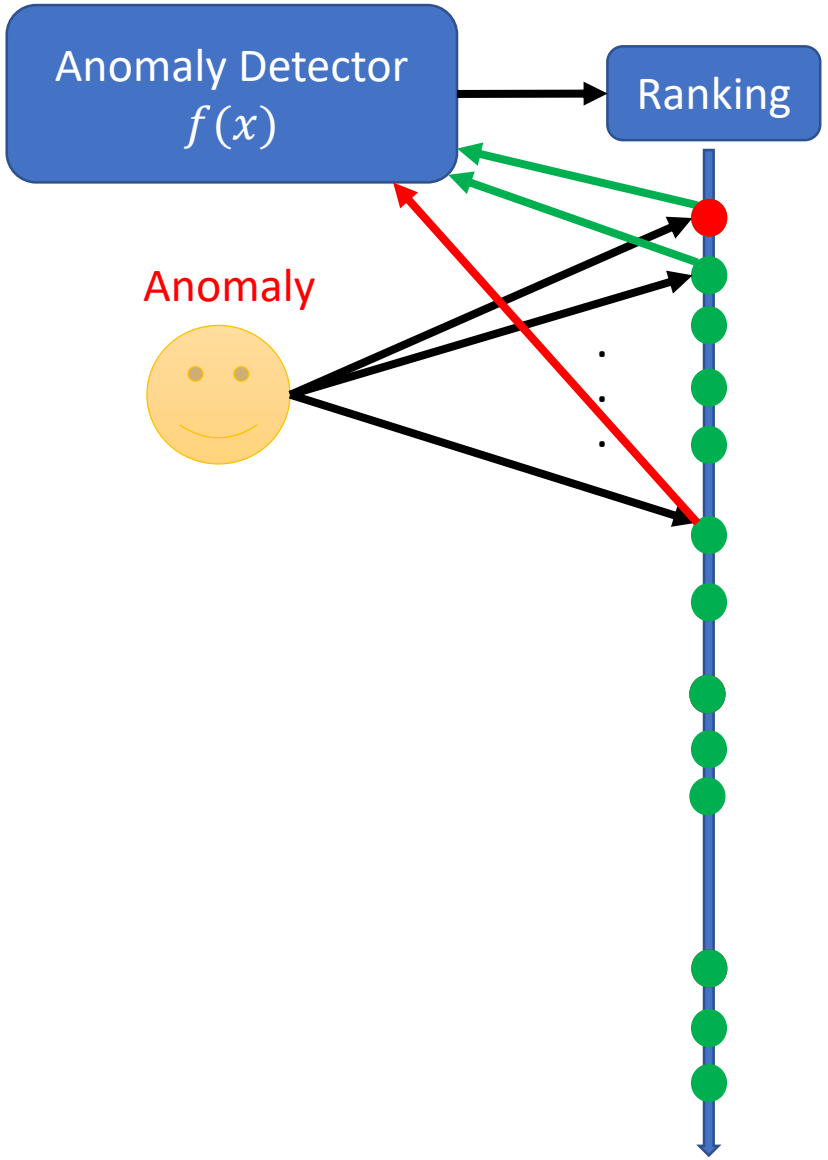
Investigation with Feedback



Investigation with Feedback



Investigation with Feedback

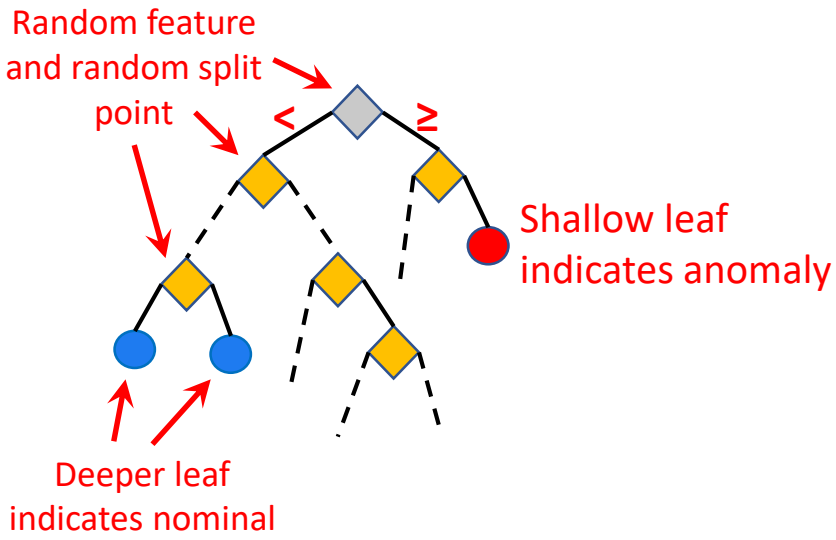


- Ranking is adaptive
- Reduces false positive

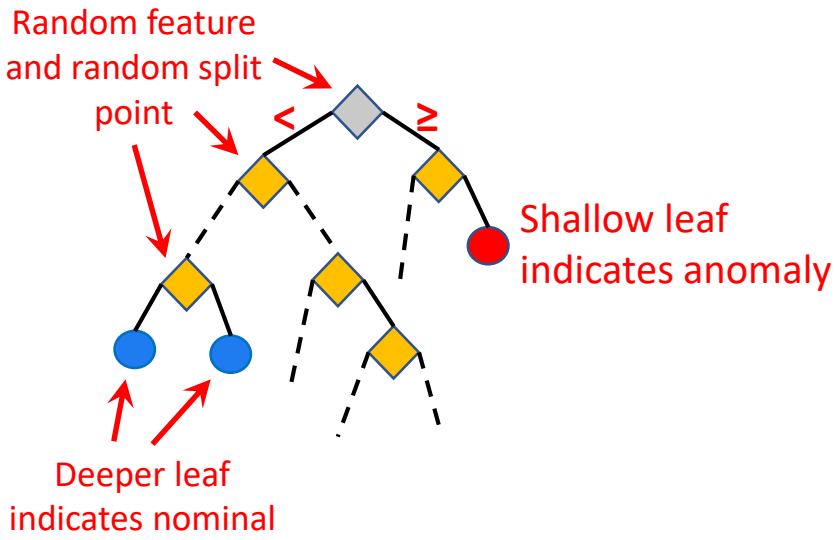
Tree-based Anomaly Detection

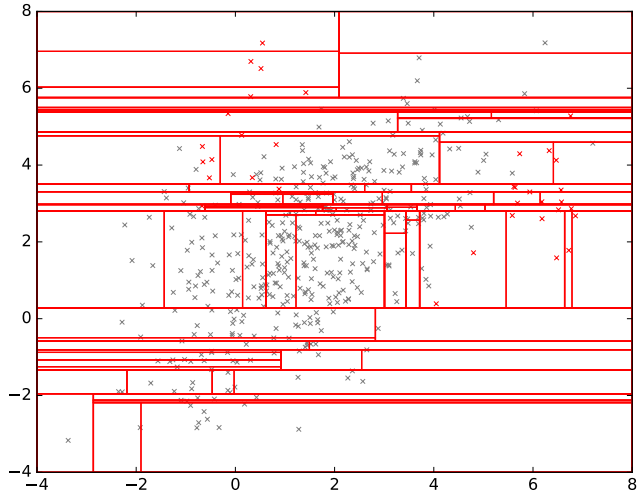
- Isolation Forest
- HS-Trees
- RS-Forest
- RPAD
- Random Projection Forest
- …

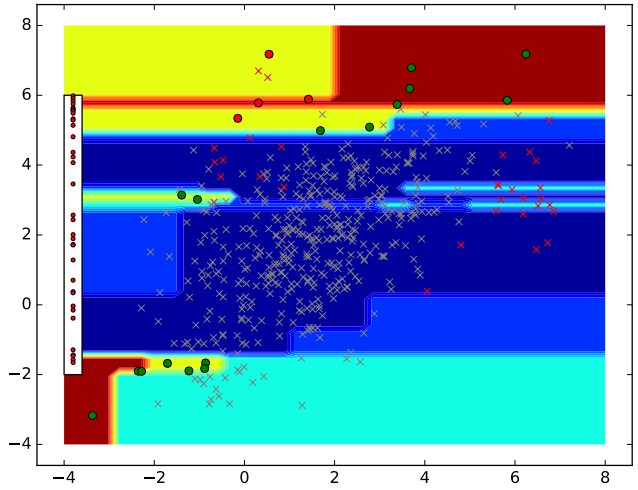
Isolation Forest



Isolation Forest



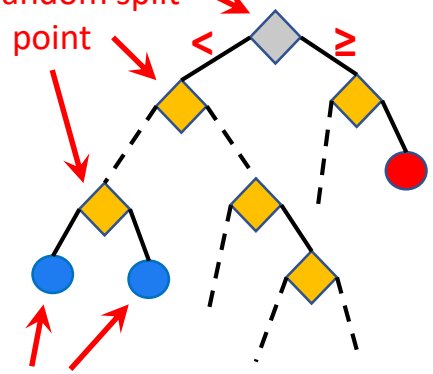




Oregon State University

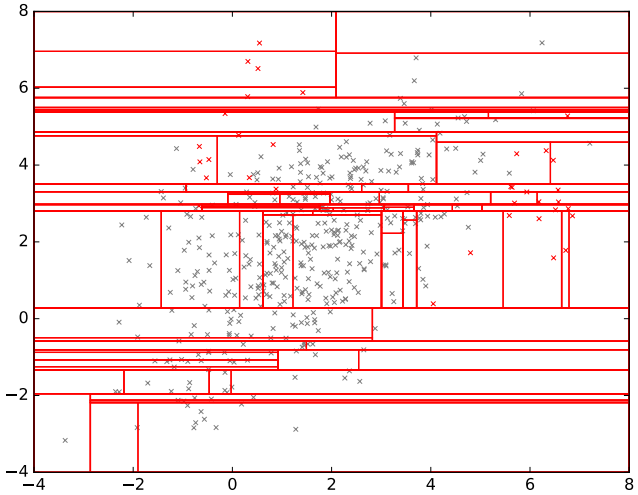
Isolation Forest

Random feature and random split point

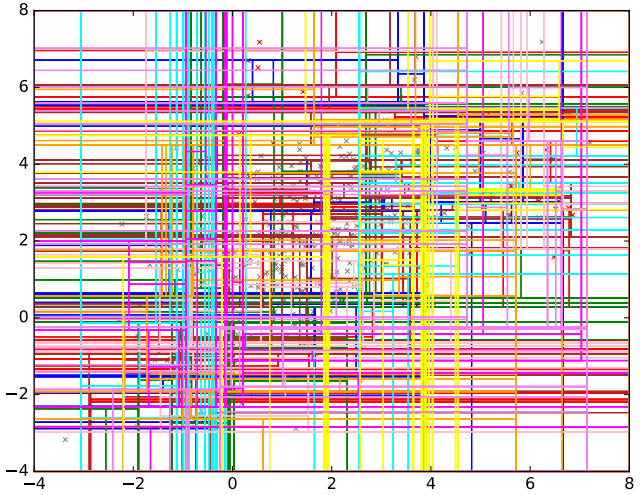


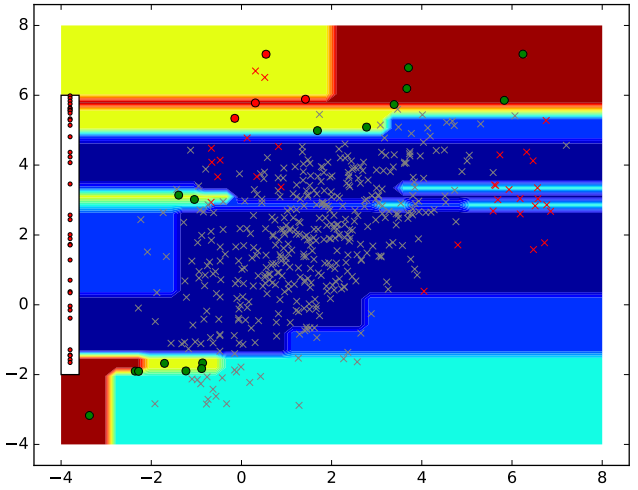
Shallow leaf indicates anomaly

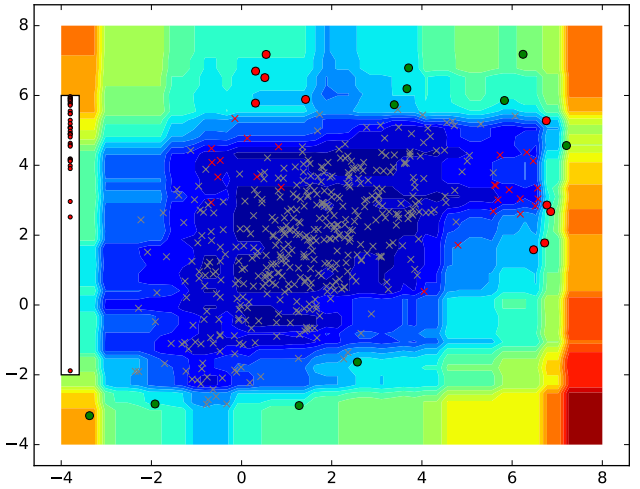
Deeper leaf indicates nominal



Typically 100 trees in practice





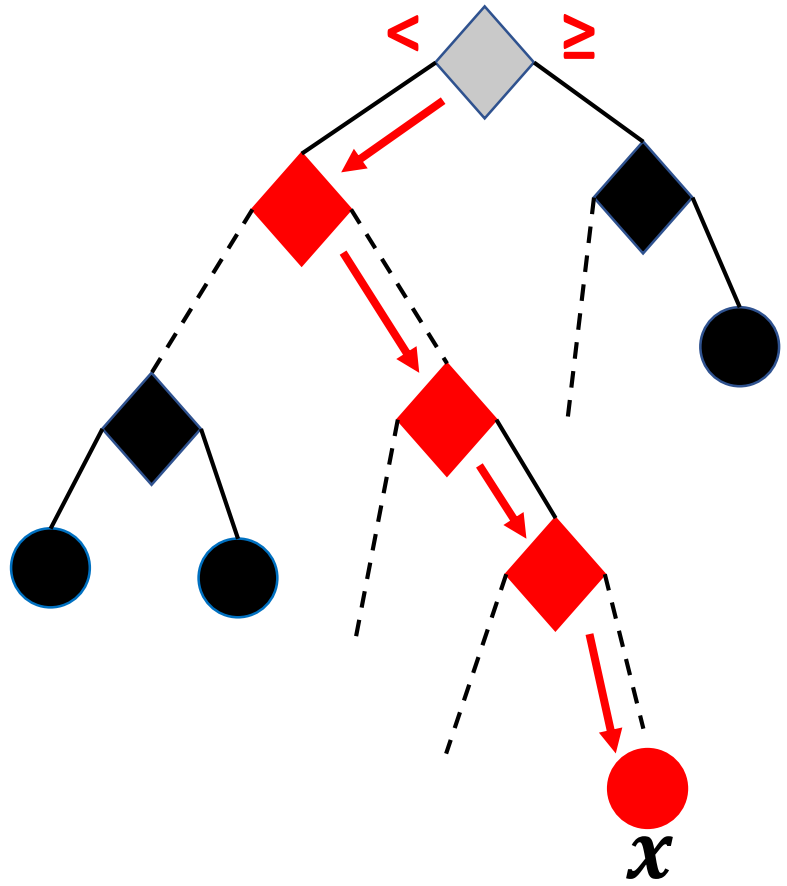


Oregon State University

Weighted Representation of Trees

$$z(x) = [-1, 0, 0, -1, 0, 0, 0, -1, -1, \dots]^T$$

(extremely sparse)



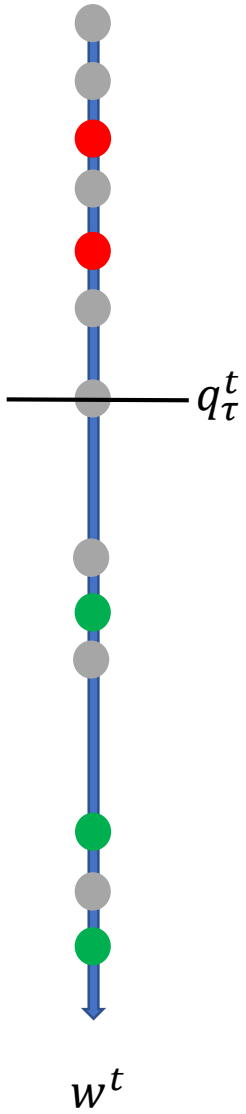
- Weights for isolation forest:

$$w = [1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1,\ 1, \dots]^T$$

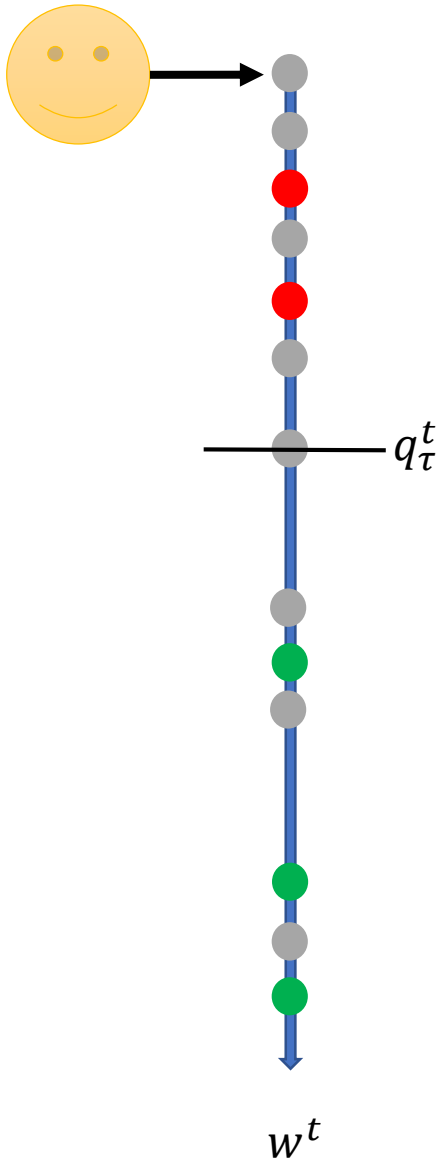
- Different set of weights will result other tree based detectors

$$score(x) = w^T . z(x)$$

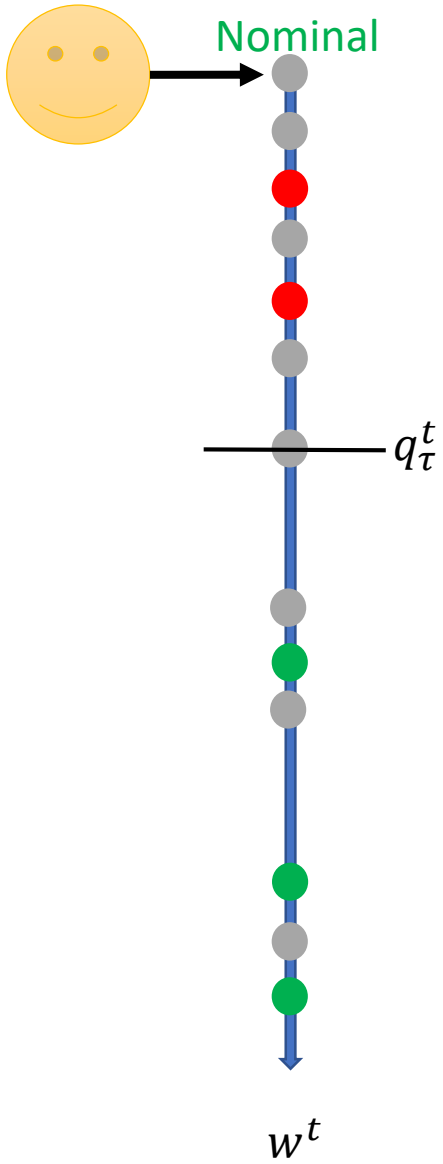
Active Anomaly Discovery



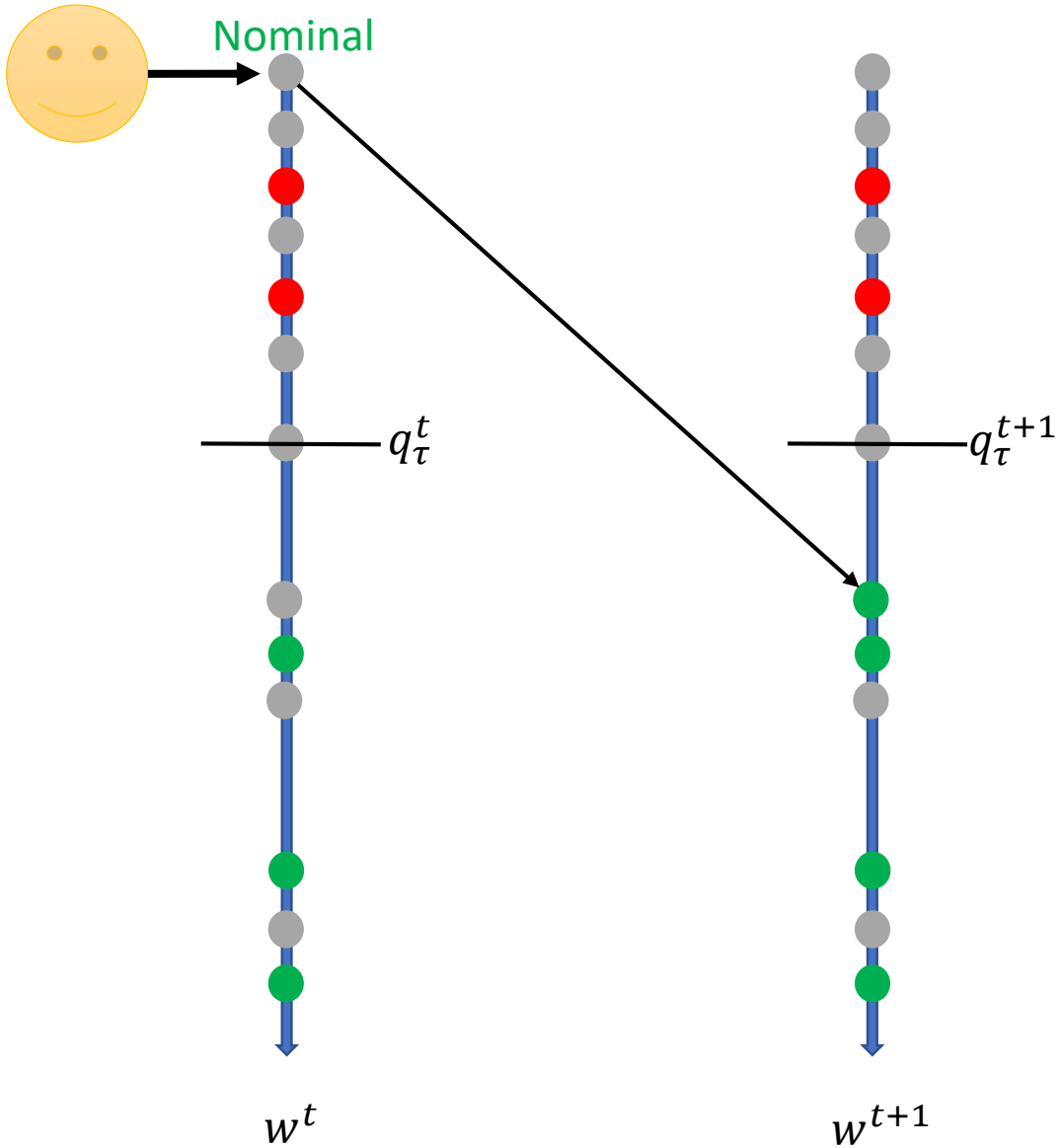
Active Anomaly Discovery



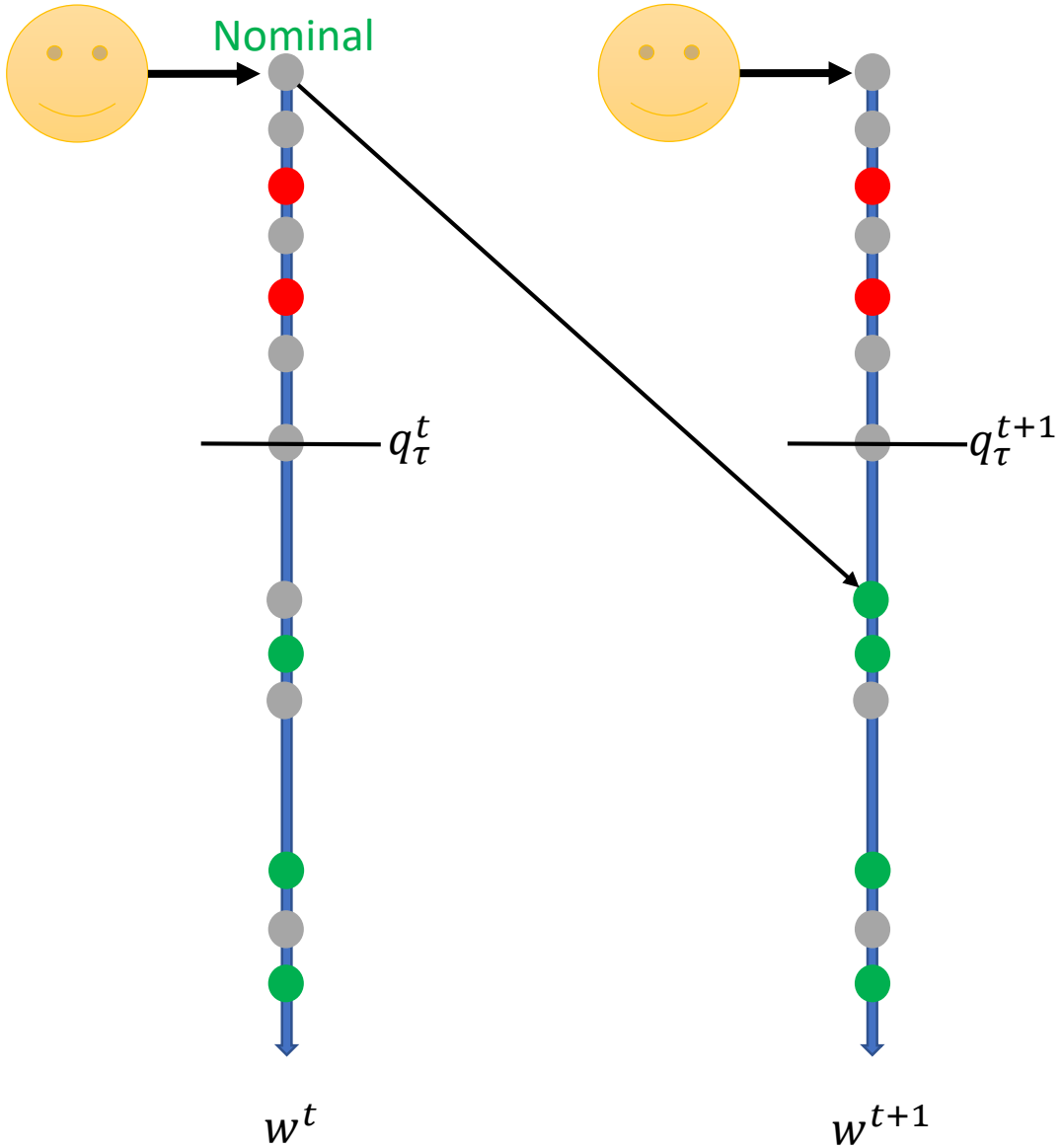
Active Anomaly Discovery



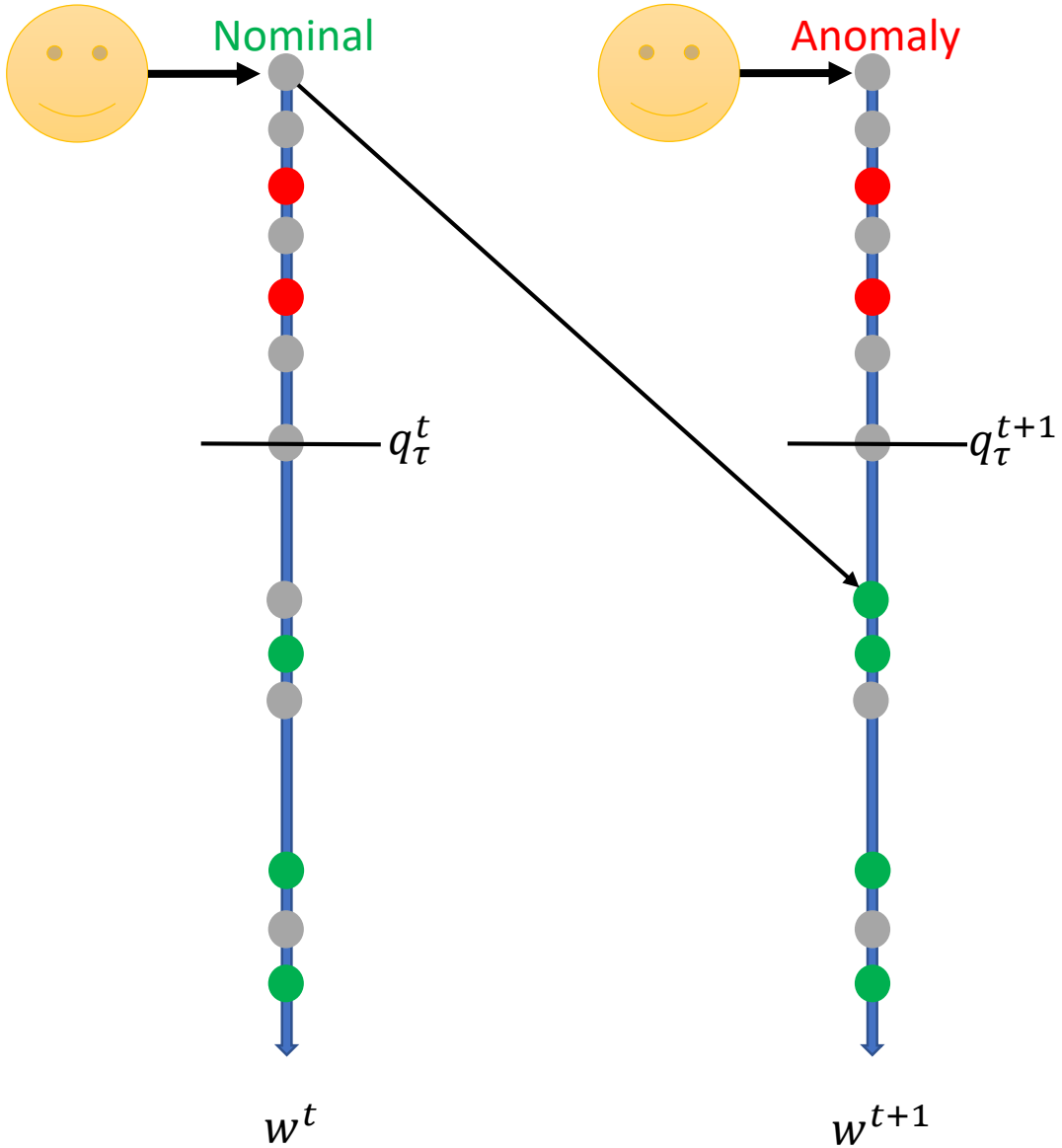
Active Anomaly Discovery



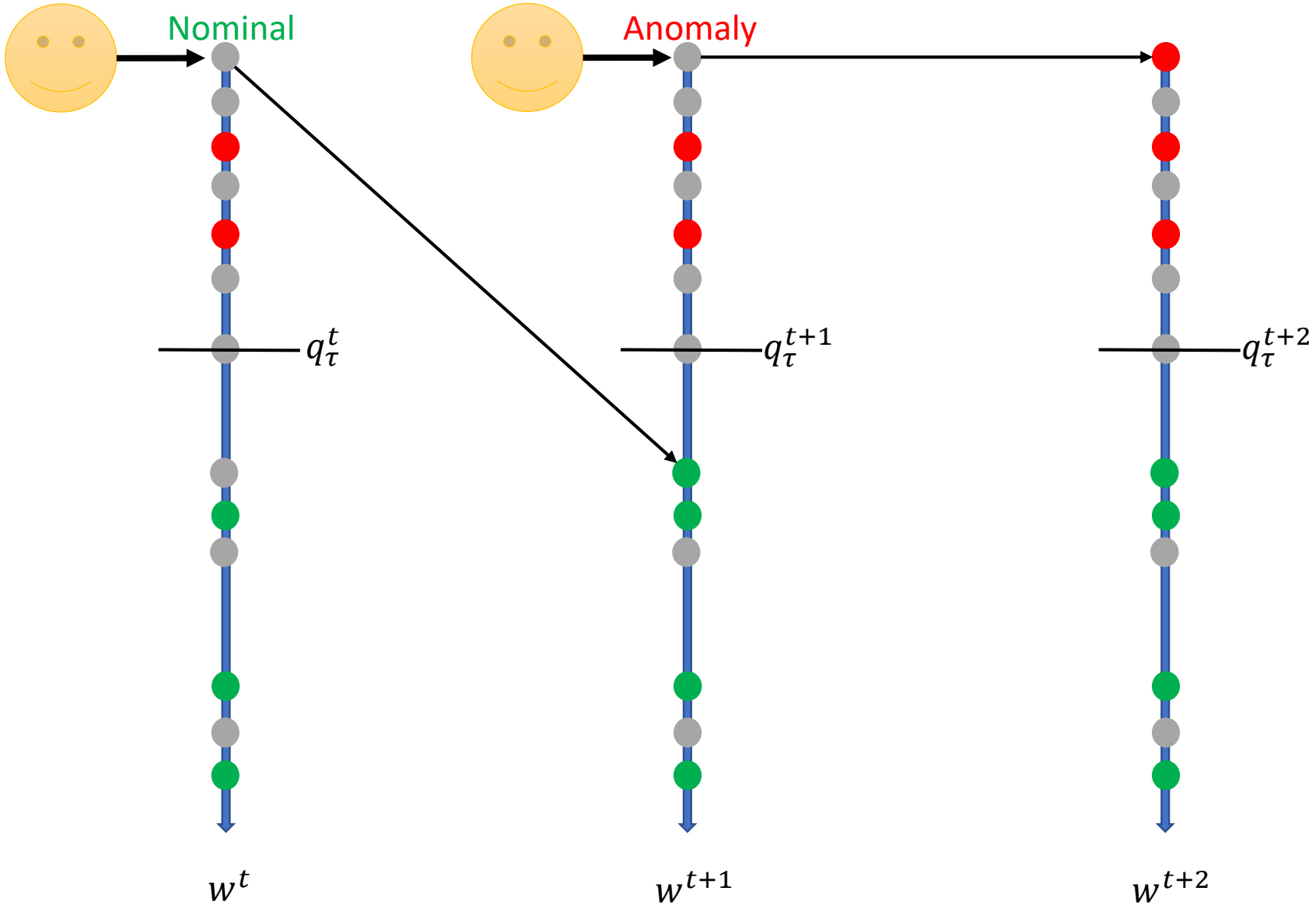
Active Anomaly Discovery



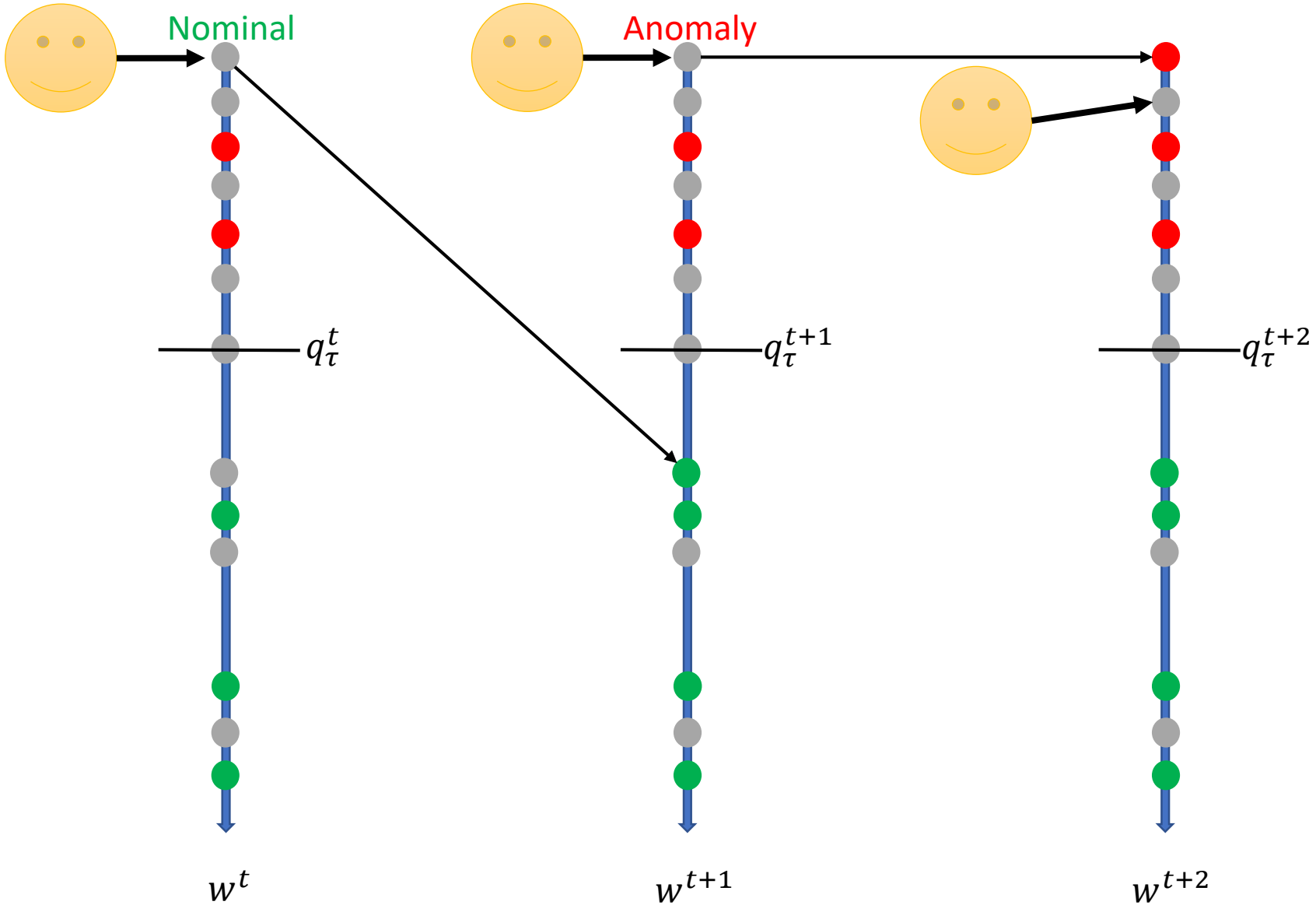
Active Anomaly Discovery



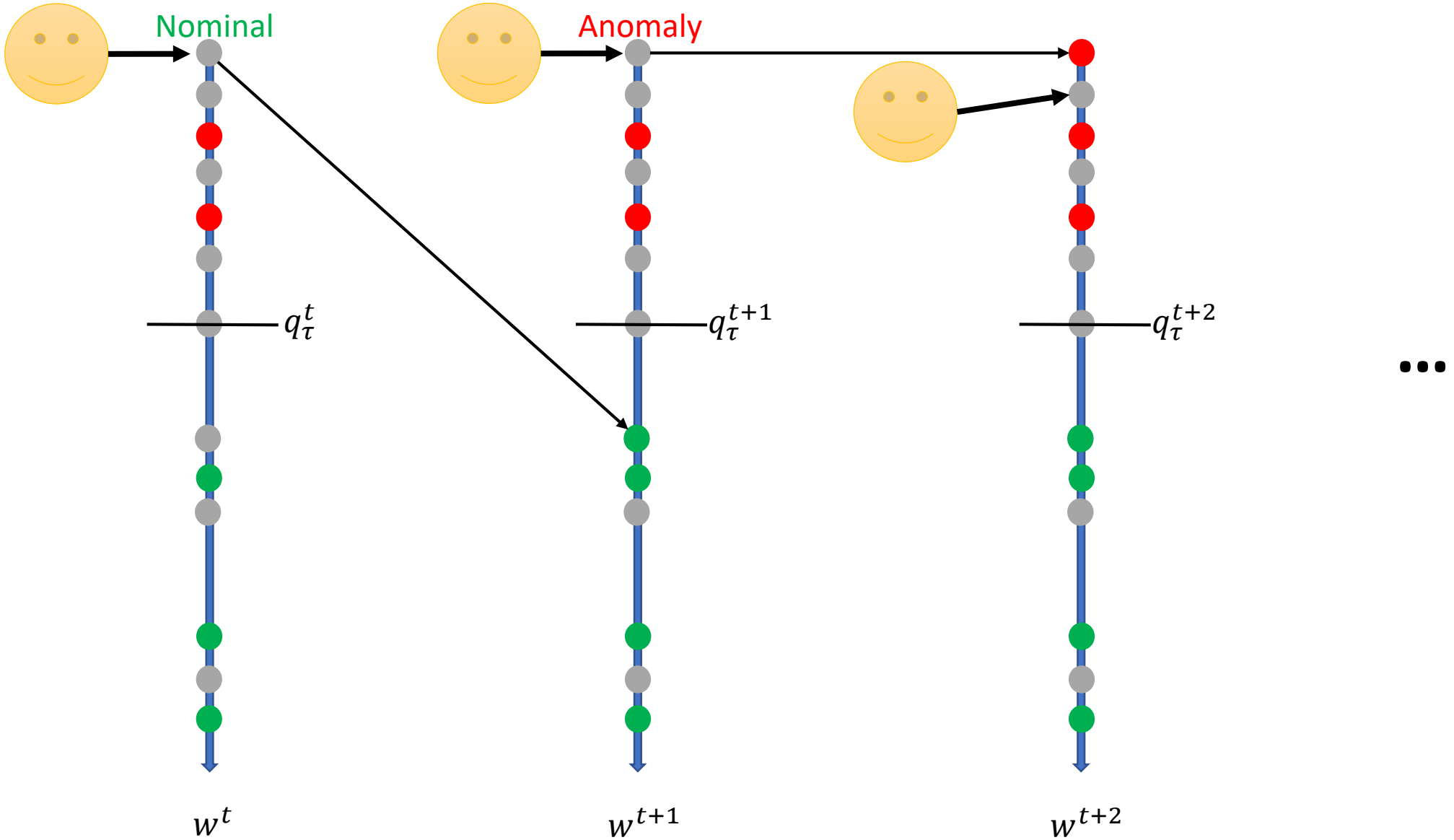
Active Anomaly Discovery



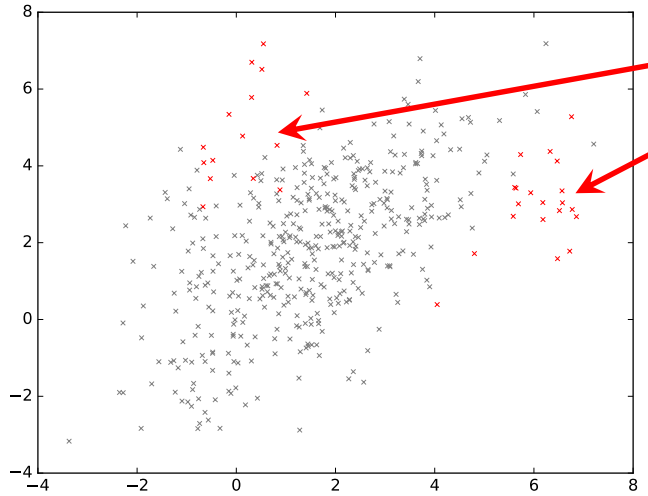
Active Anomaly Discovery



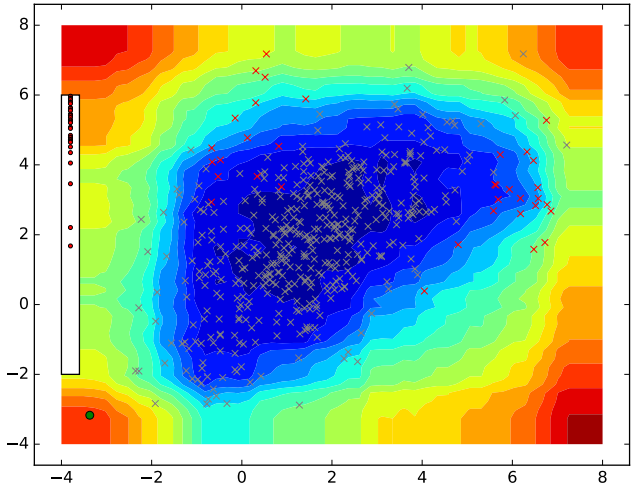
Active Anomaly Discovery



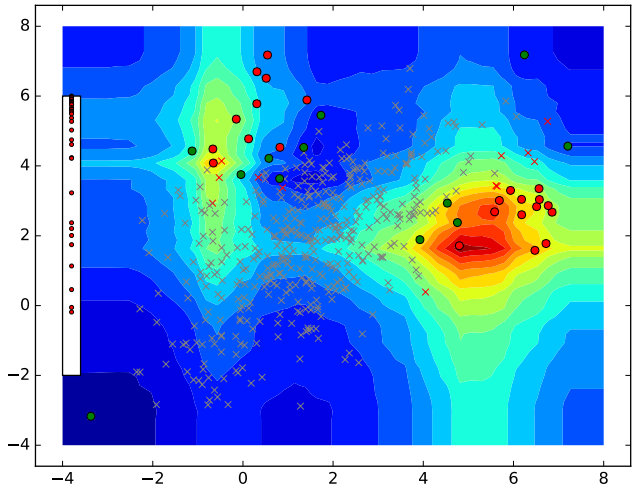
Result



Synthetic Dataset



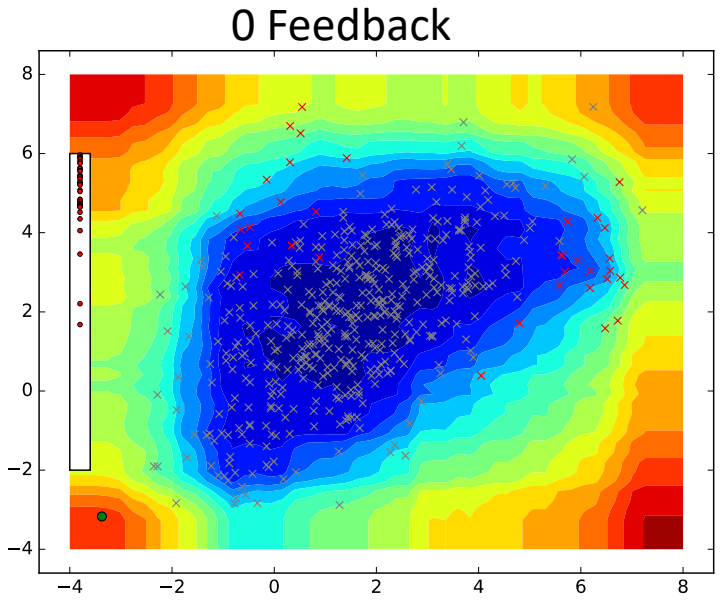
Baseline discovers **12** anomalies in 35 iterations



AAD discovers **23** anomalies in 35 iterations

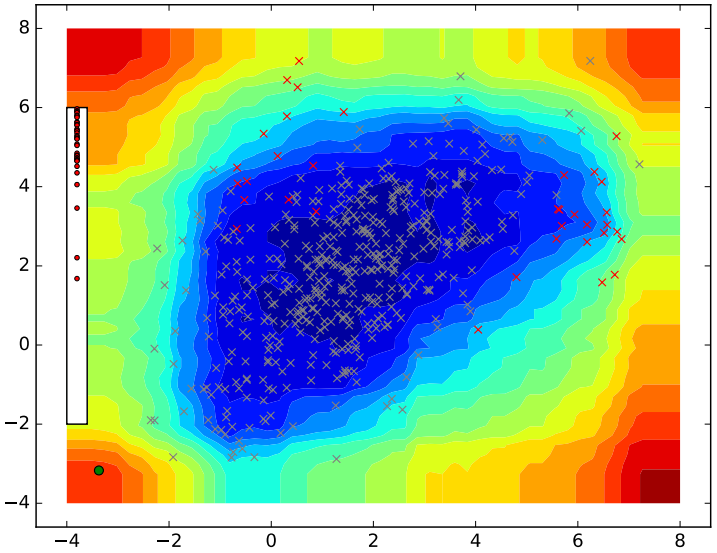
Oregon State University

Result

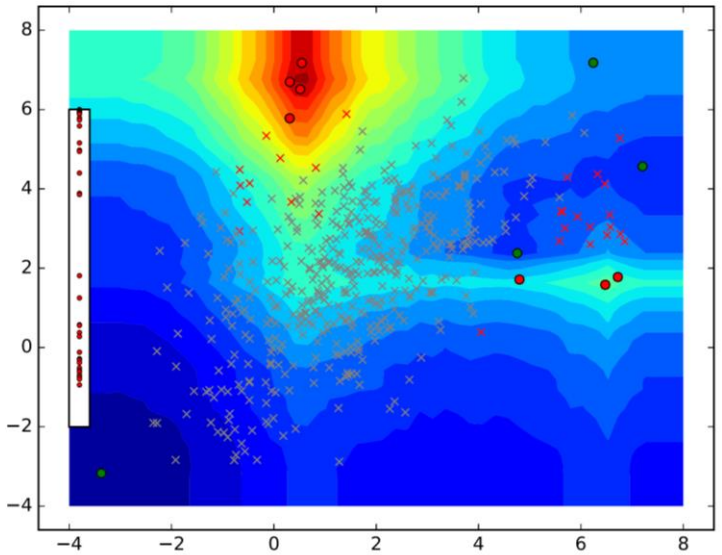


Result

0 Feedback

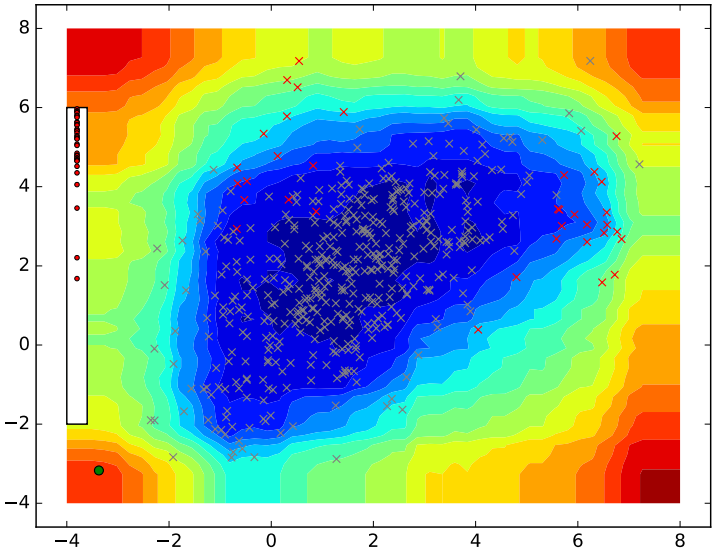


10 Feedback

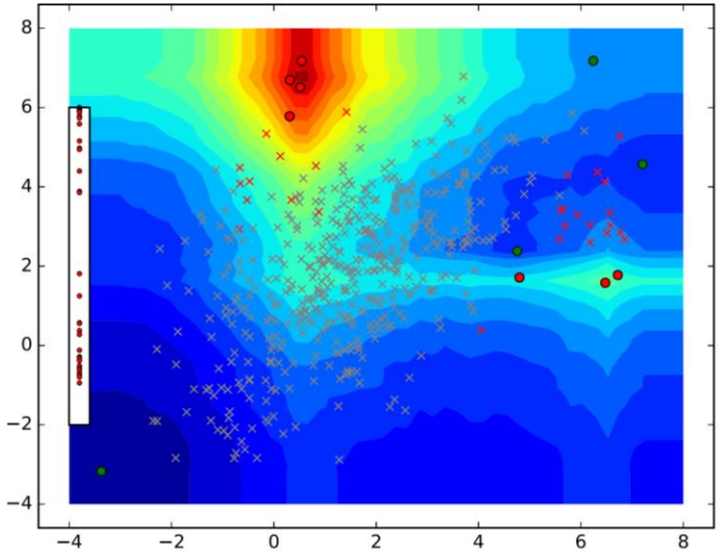


Result

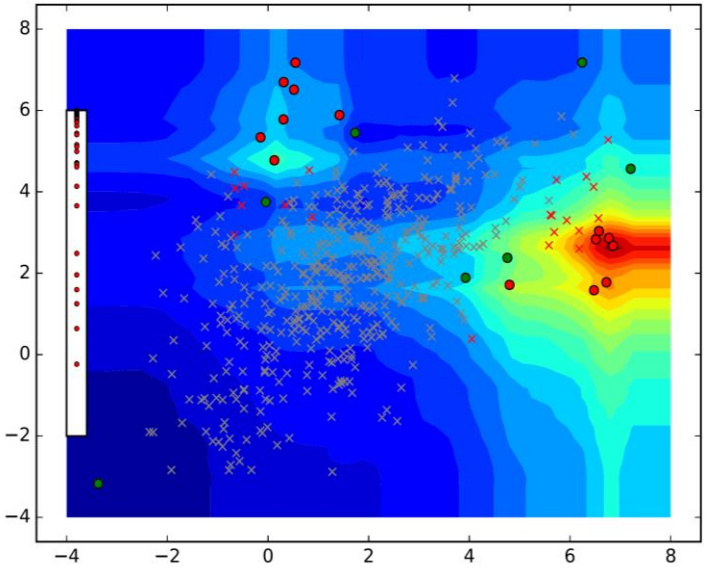
0 Feedback



10 Feedback



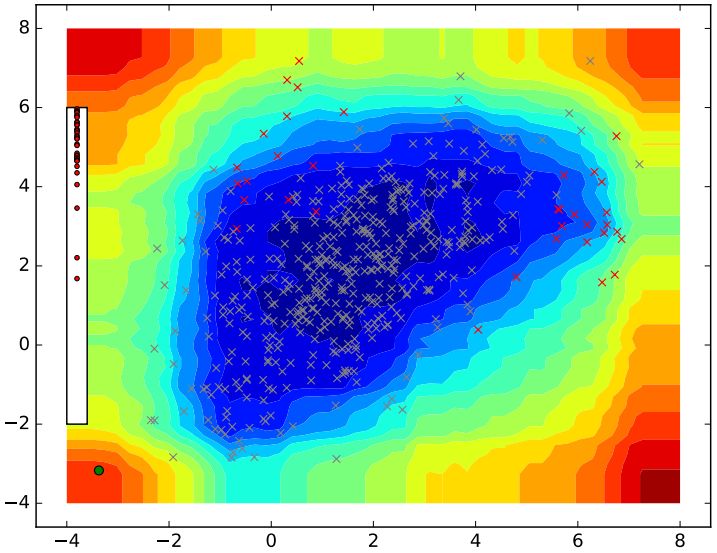
20 Feedback



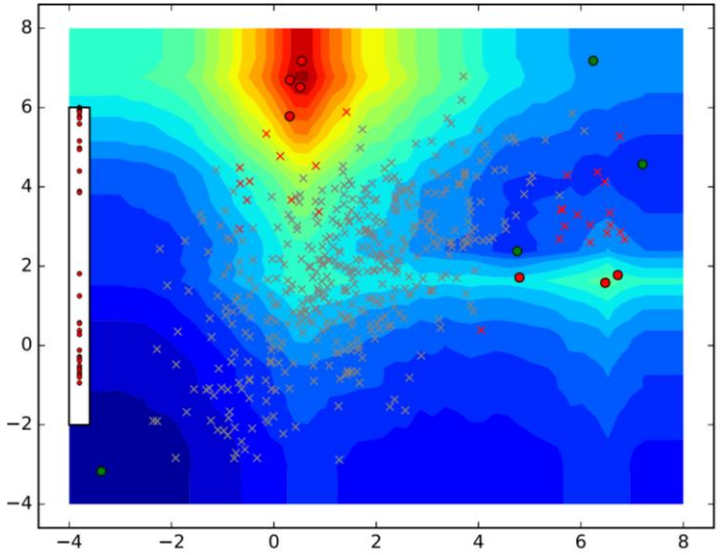
Oregon State University

Result

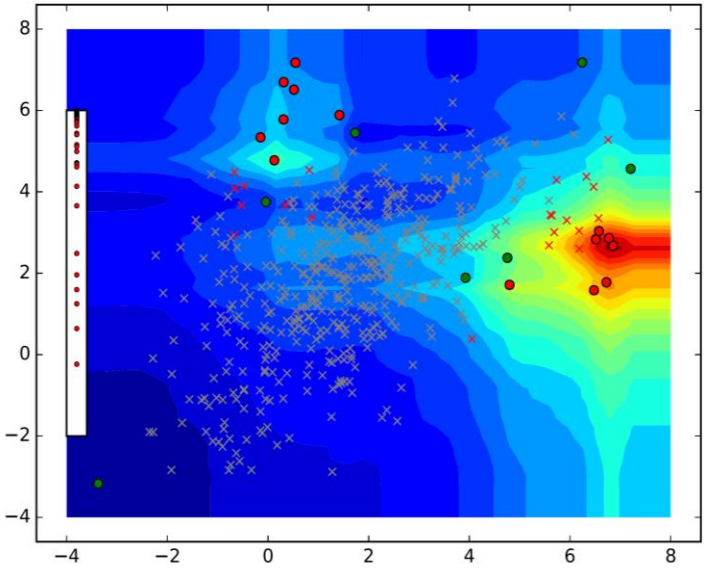
0 Feedback



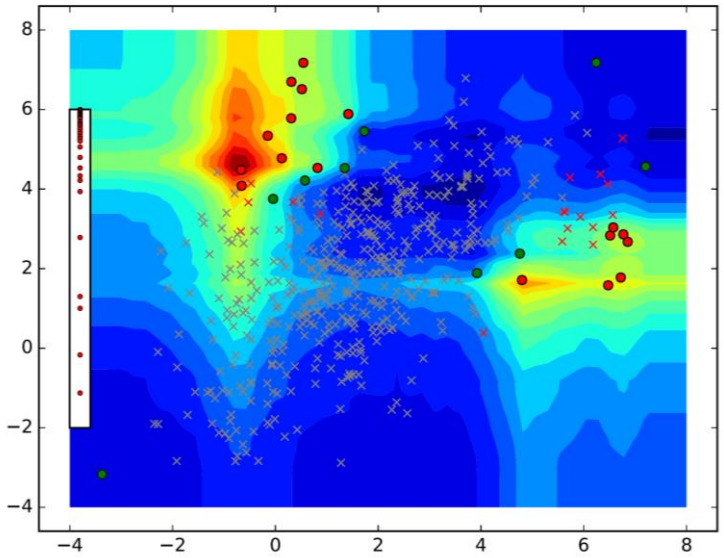
10 Feedback



20 Feedback

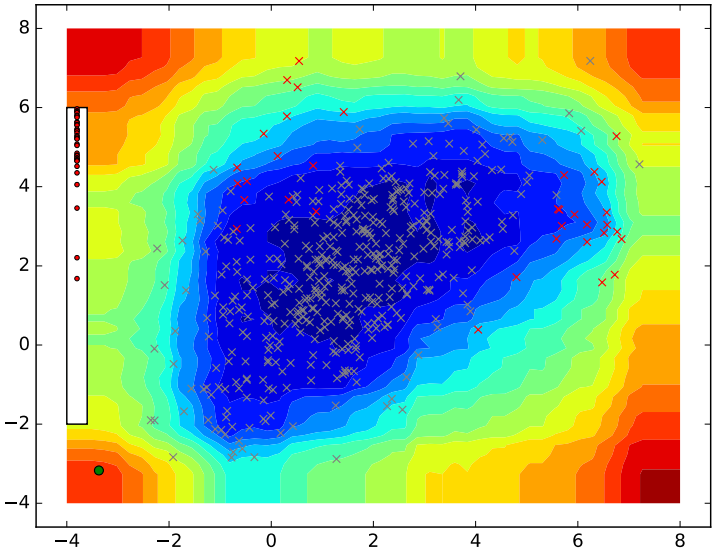


25 Feedback

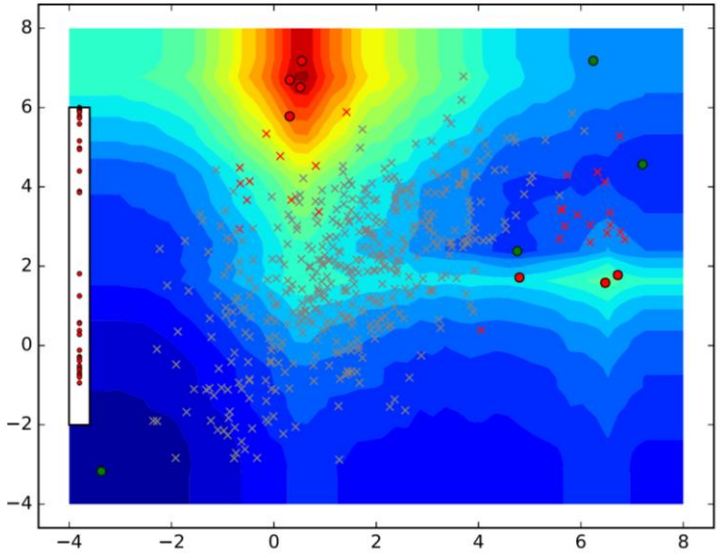


Result

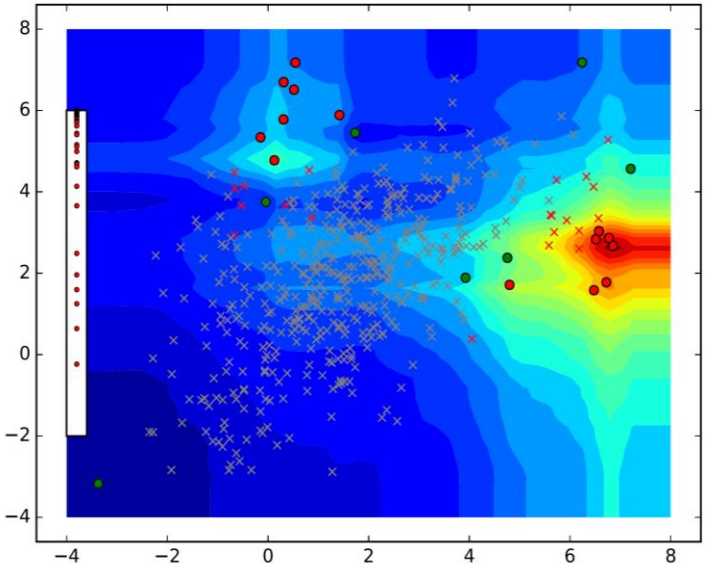
0 Feedback



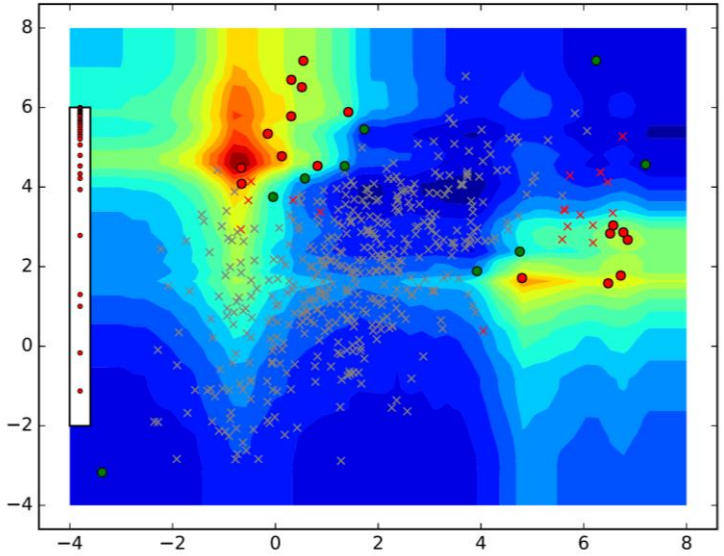
10 Feedback



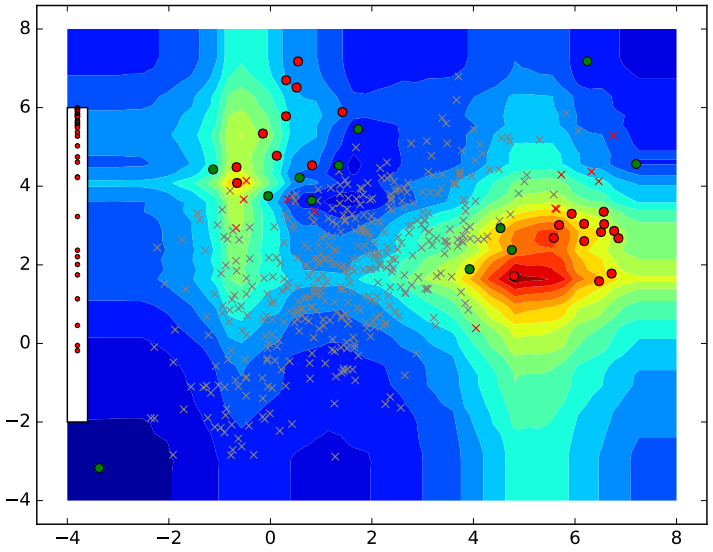
20 Feedback



25 Feedback



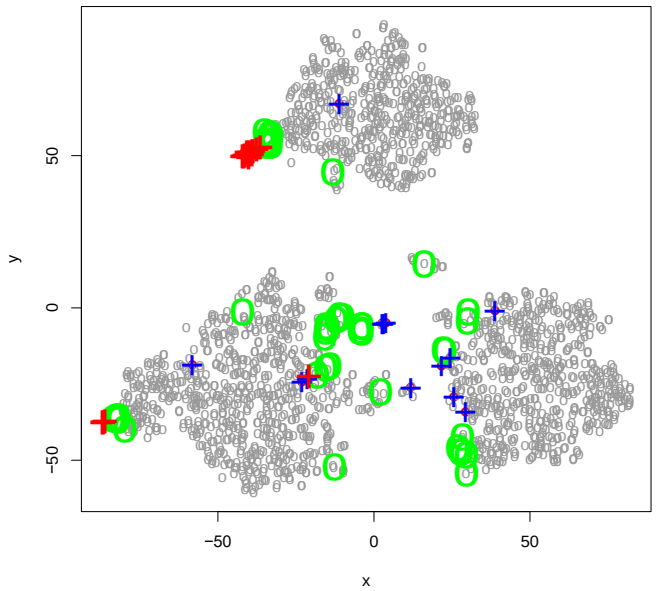
35 Feedback



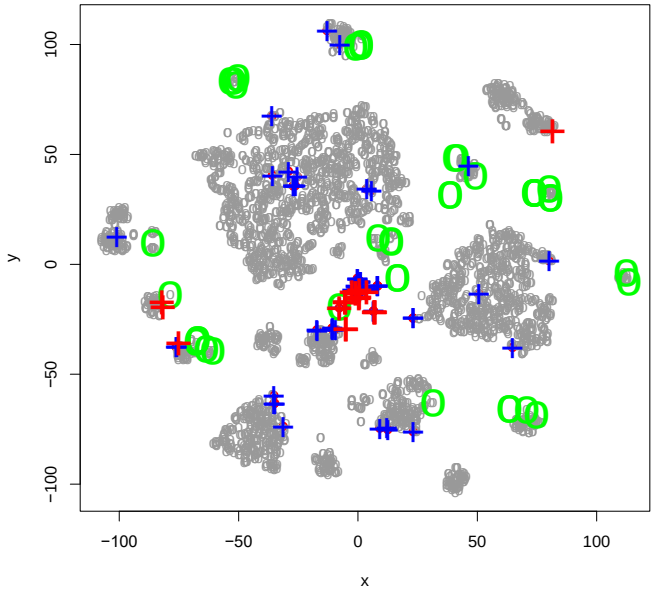
A closer look at the data with t-SNE

A closer look at the data with t-SNE

Abalone Baseline



ANN Thyroid 1v3 Baseline



o False Positive

\+ False Negative

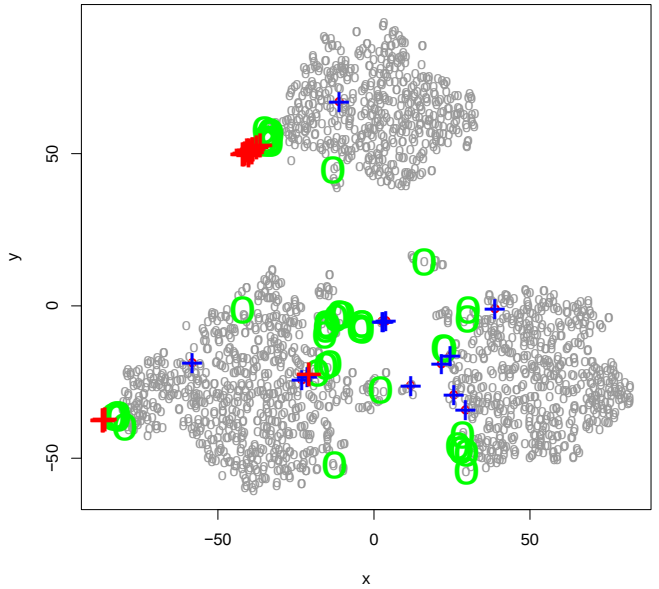
\+ True Positive

o True Negative

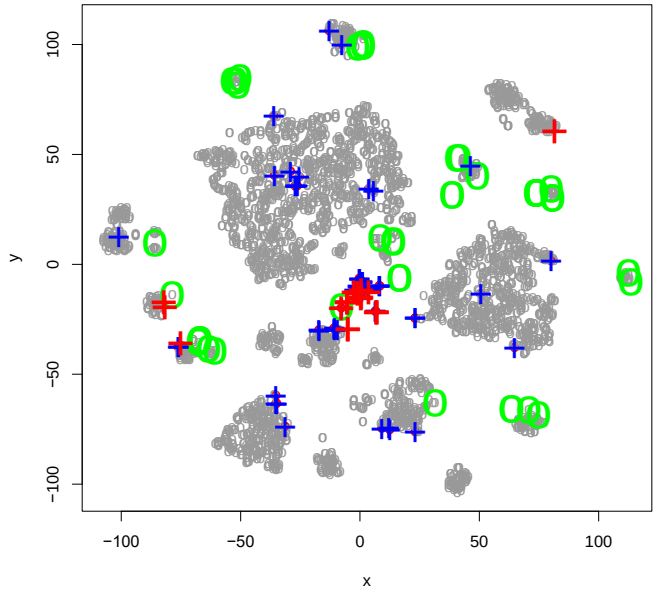
Oregon State University

A closer look at the data with t-SNE

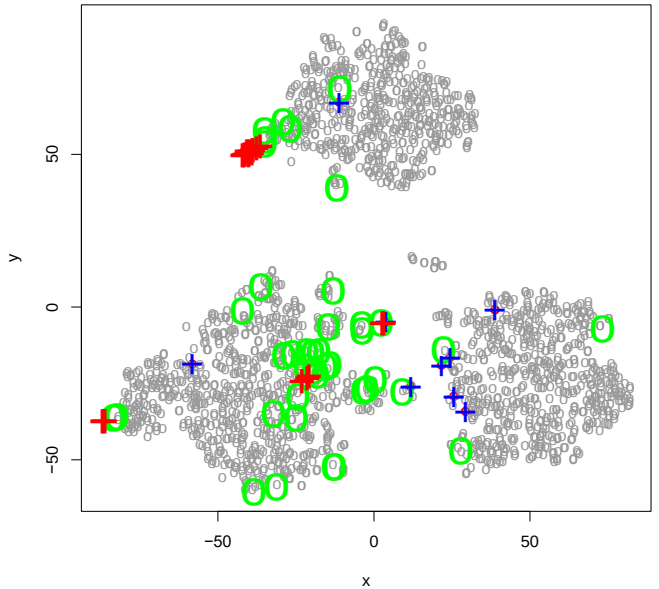
Abalone Baseline



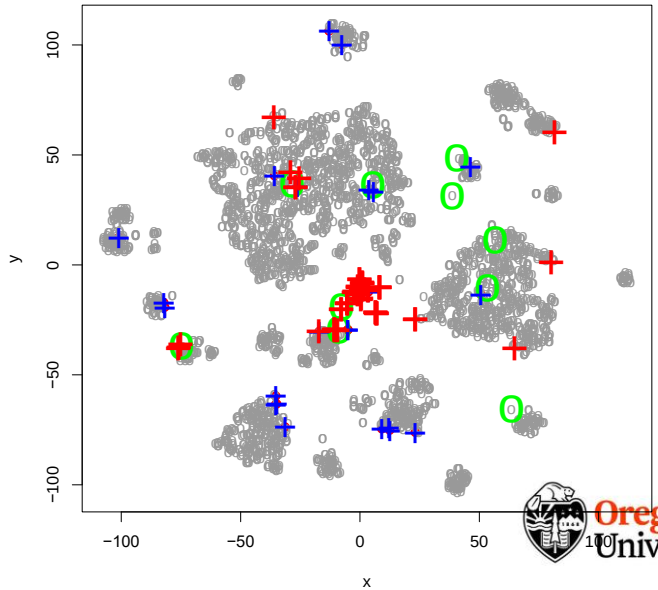
ANN Thyroid 1v3 Baseline



Abalone IF-AAD



ANN Thyroid 1v3 IF-AAD



o False Positive

\+ False Negative

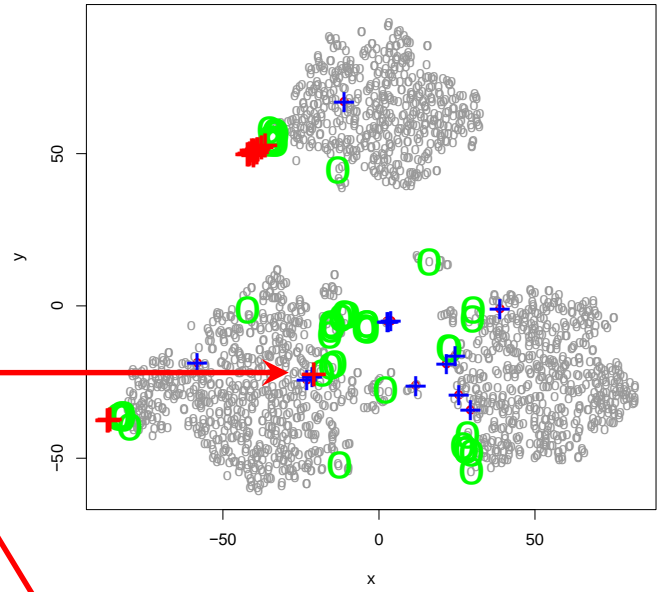
\+ True Positive

o True Negative

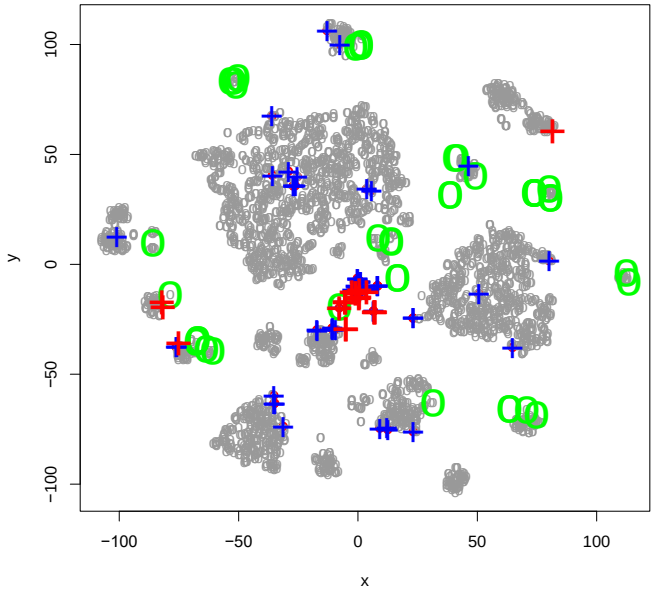
A closer look at the data with t-SNE

- Effect of feedback
  - Increase focus where anomalies have been discovered previously

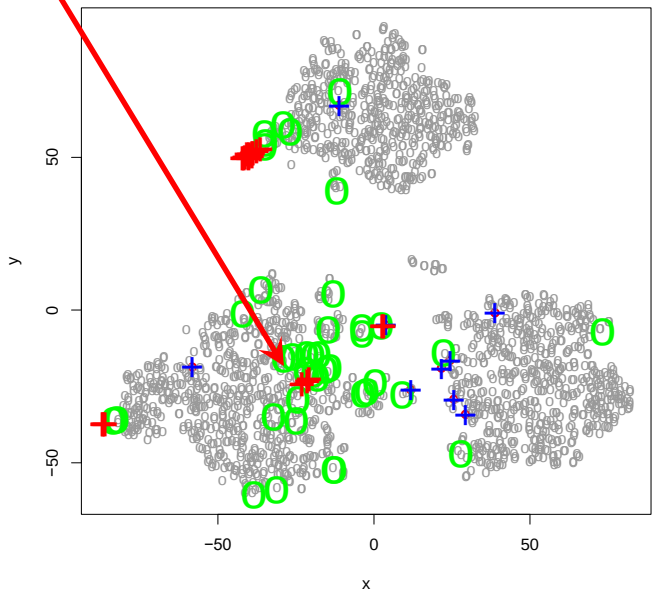
Abalone Baseline



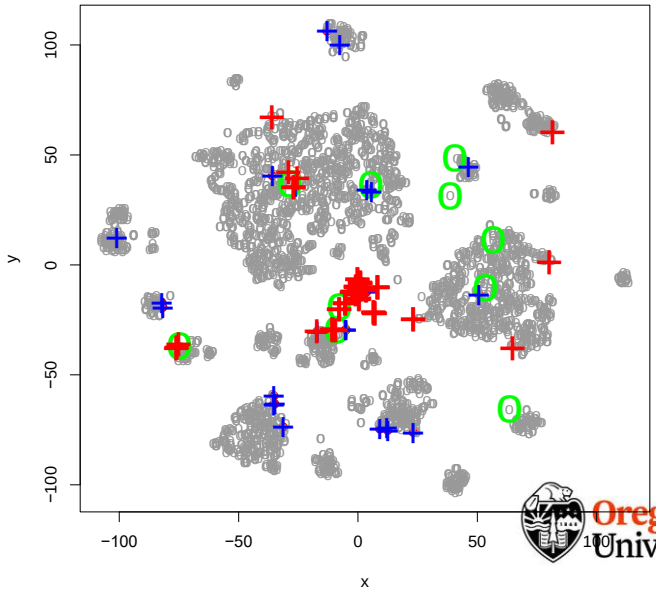
ANN Thyroid 1v3 Baseline



Abalone IF-AAD



ANN Thyroid 1v3 IF-AAD



o False Positive

\+ False Negative

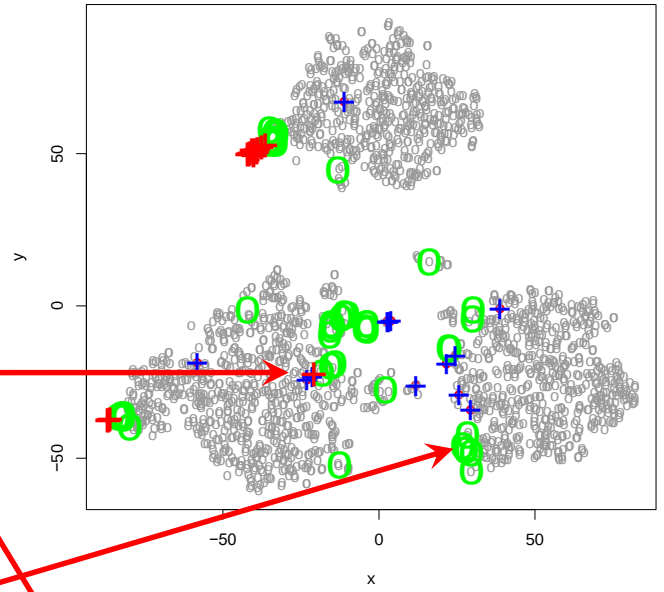
\+ True Positive

o True Negative

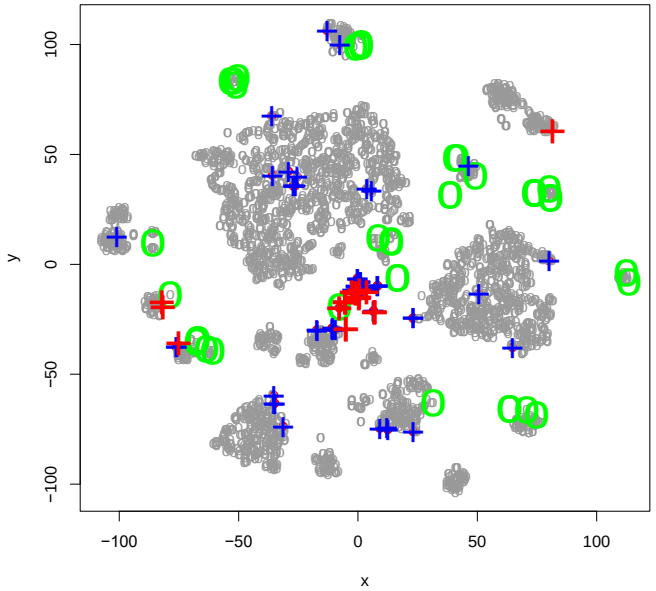
A closer look at the data with t-SNE

- Effect of feedback
  - Increase focus where anomalies have been discovered previously
  - Remove focus from unpromising regions

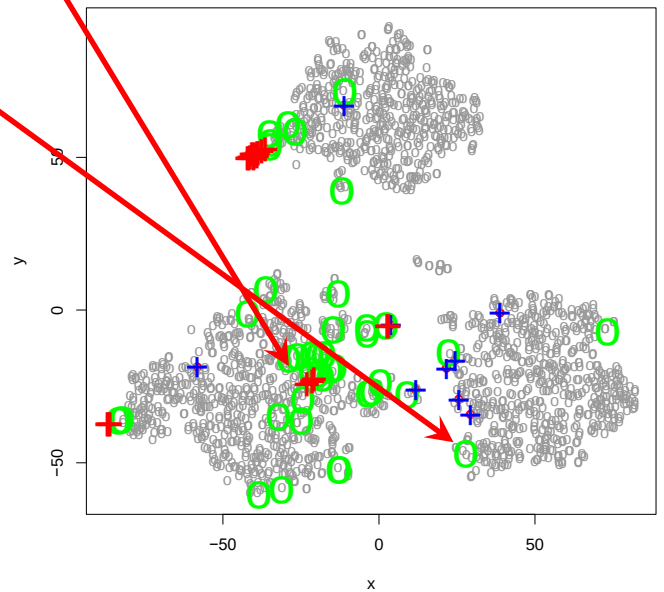
Abalone Baseline



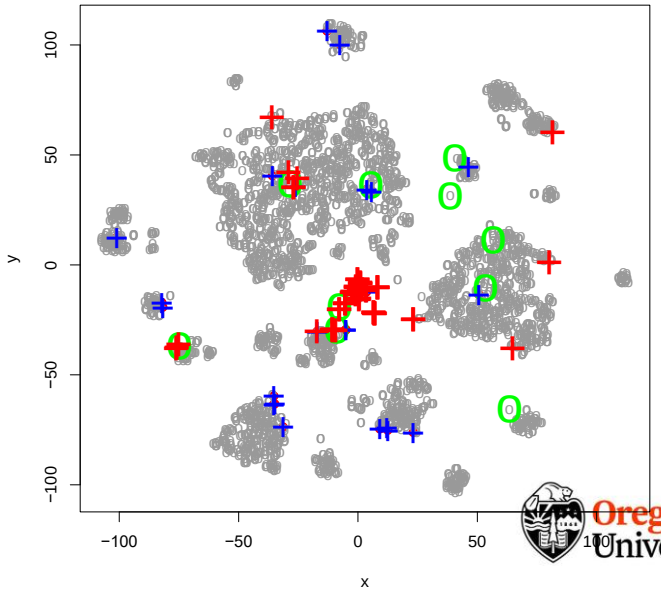
ANN Thyroid 1v3 Baseline



Abalone IF-AAD

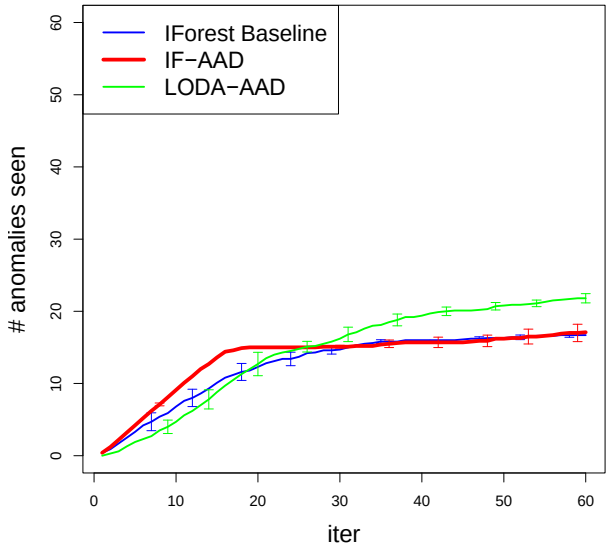


ANN Thyroid 1v3 IF-AAD

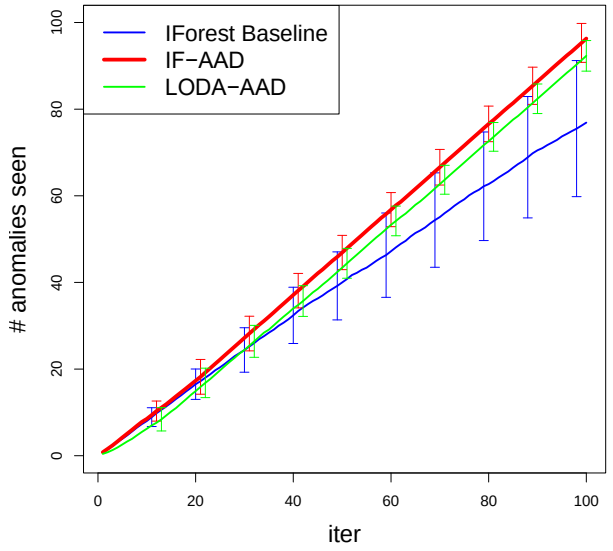


o False Positive
\+ False Negative
\+ True Positive
o True Negative

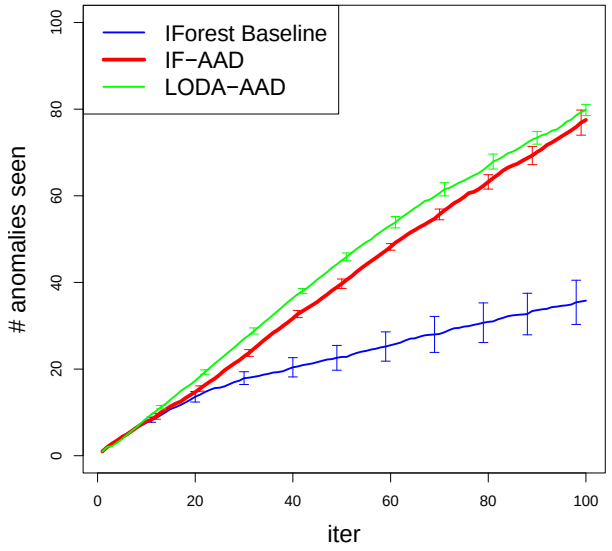
Abalone



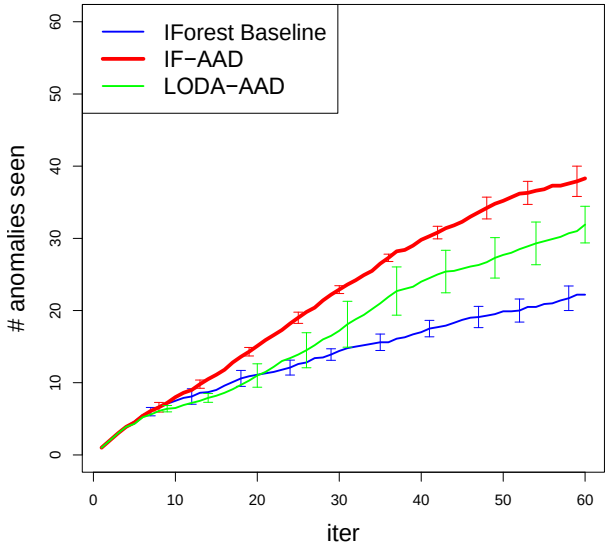
Covtype



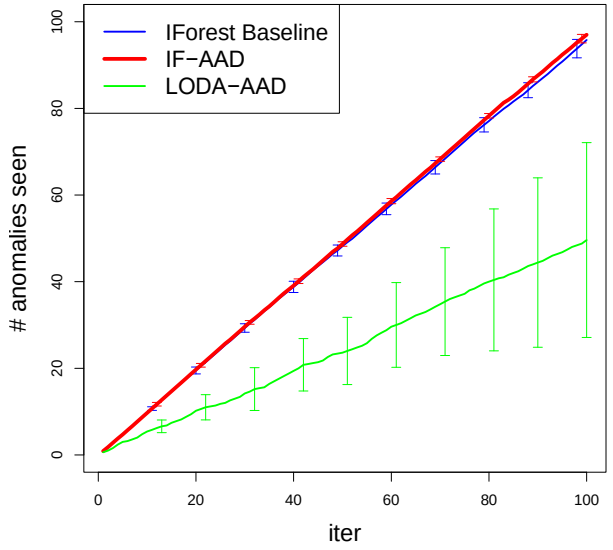
Mammography



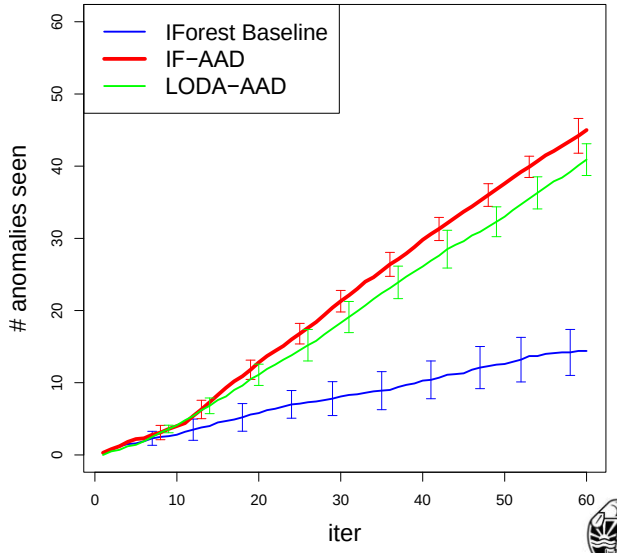
Cardiotocography



KDDCup99



ANN Thyroid 1v3



Conclusion & Future Work

- Human feedback is essential and improves the unsupervised learner ☺

Conclusion & Future Work

- Human feedback is essential and improves the unsupervised learner ☺
- Extend to other types of anomaly detectors

Conclusion & Future Work

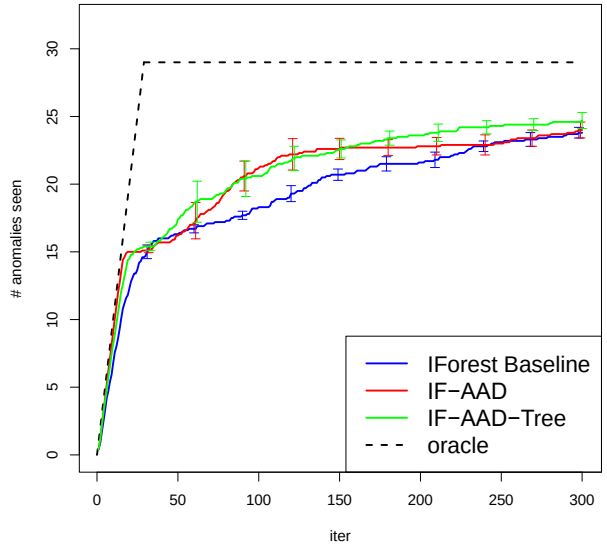
- Human feedback is essential and improves the unsupervised learner ☺
- Extend to other types of anomaly detectors
- Explanation based feedback

Questions?

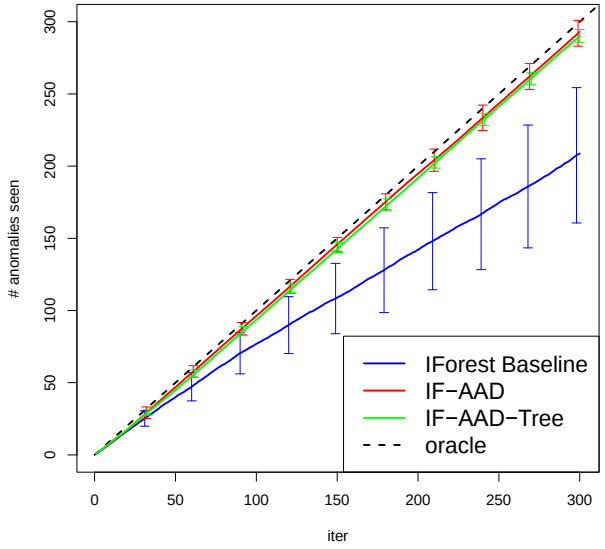
Extra Slides

Results (adjusting tree weights instead of node-weights)

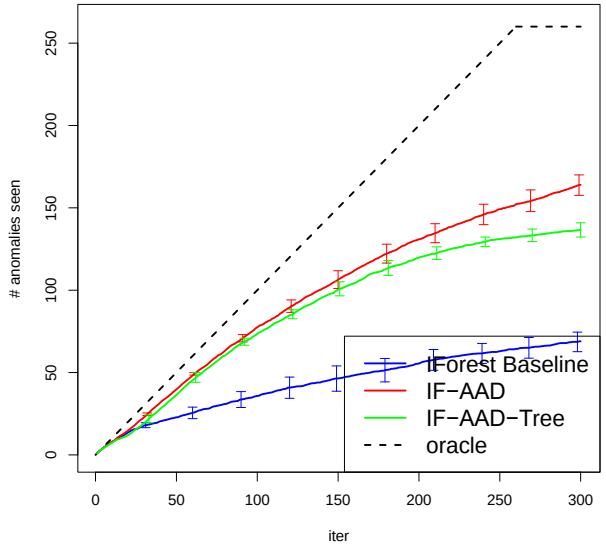
Abalone



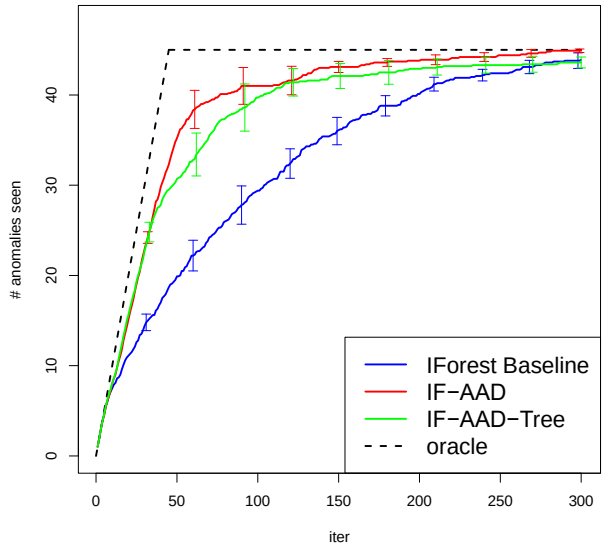
Covtype



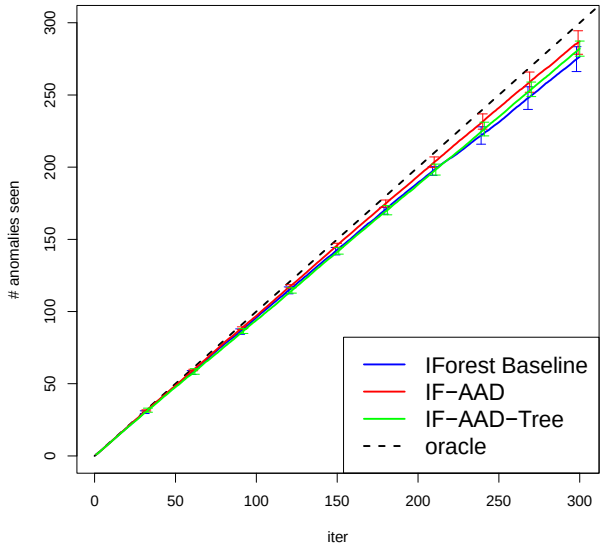
Mammography



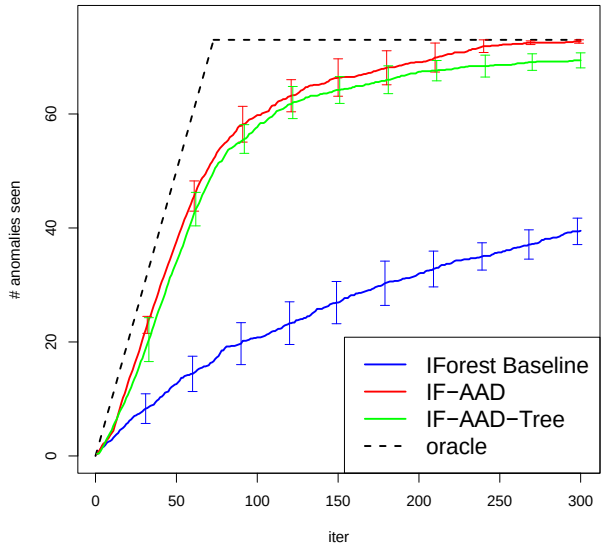
Cardiotocography



KDDCup99

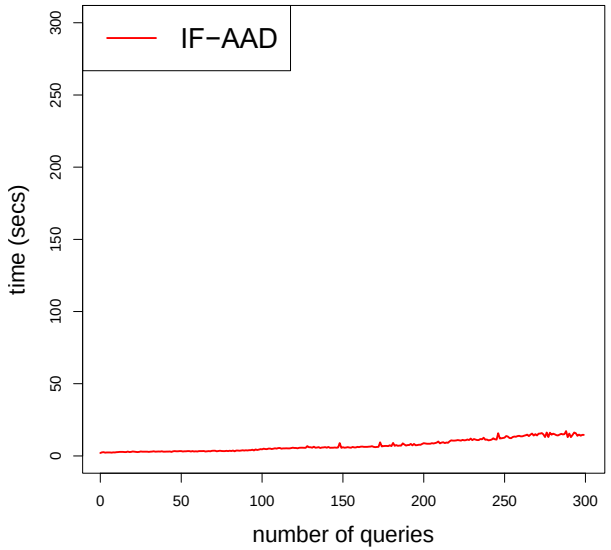


ANN Thyroid 1v3

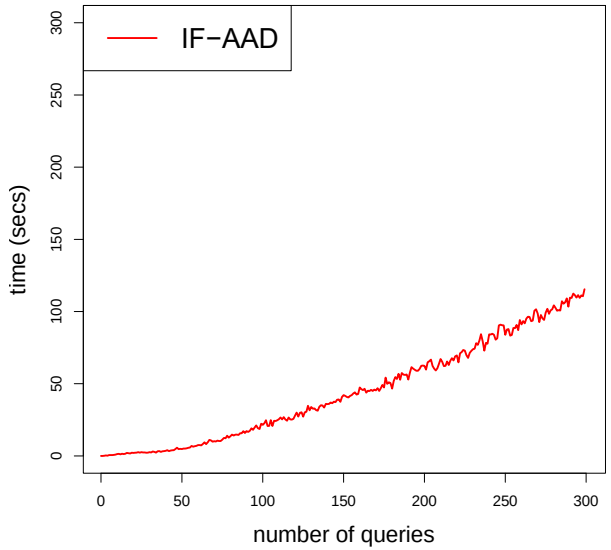


Oregon State University

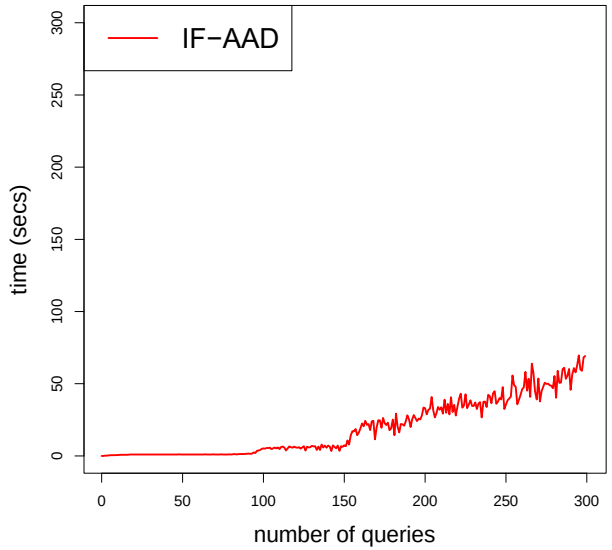
Timing Plots



Covtype



Mammography



Shuttle