Unsupervised Continual Shallow Learning Techniques

- Shambu Kavir & Taha Adeel Mohammed

Introduction

- For Network Intrusion Detection Systems(NID), labelling the training data is an expensive task, and the testing data would have concept drift over time, and the attack data is very sparse.
- Furthermore, the model ideally should be light (deployable on edge devices) and have explainability.
- Hence shallow unsupervised anomaly detection models without catastrophic forgetting would be ideal for our scenario.

Techniques

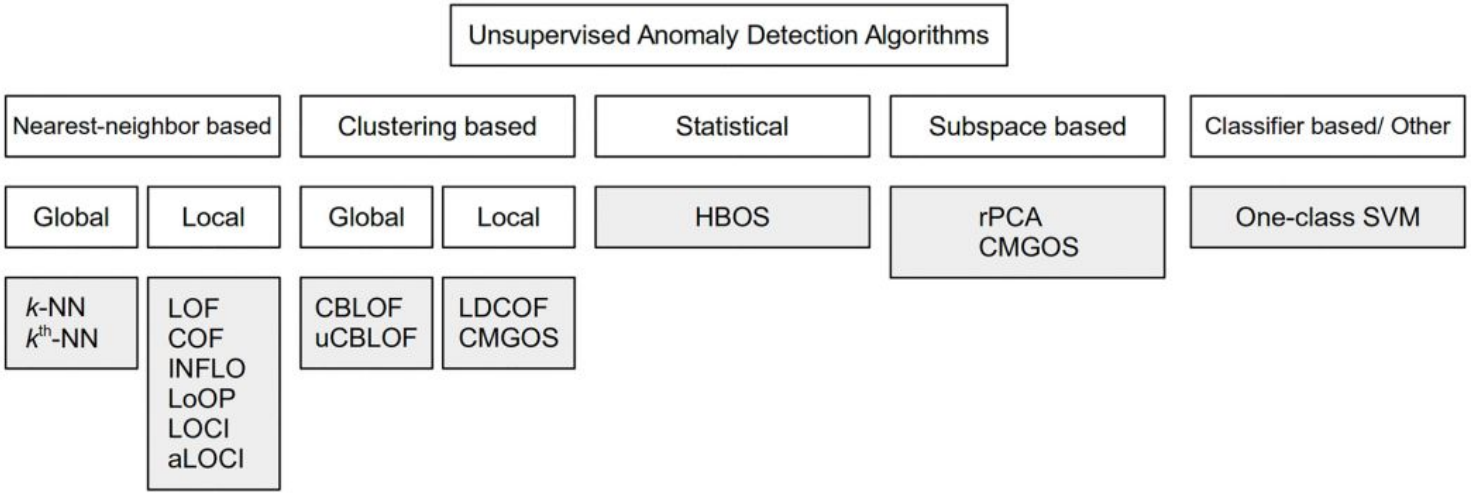


Fig 3. A taxonomy of unsupervised anomaly detection algorithms comprising of four main groups. Note that CMGOS can be categorized in two groups: It is a clustering-based algorithm as well as estimating a subspace of each cluster.

Unsupervised Decision Trees

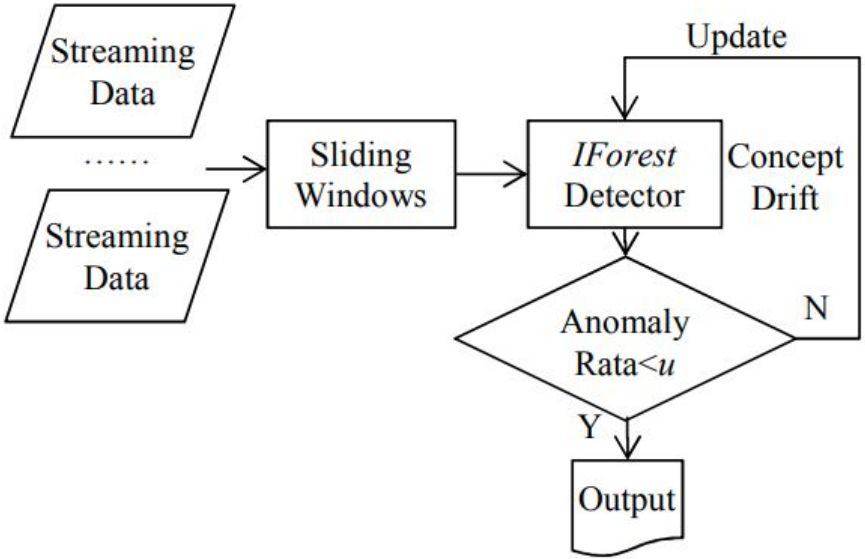
- You basically run a clustering algorithm on your data (say k-nn algorithm) and get labels.
- Then build decision tree using these labels. (Can be maybe extended to use Hoeffding Trees instead of normal decision trees.)
- Ensemble multiple trees to get Random Forest.

Isolation Forests

- Unsupervised decision trees
- Work for anomaly detection, i.e when the attack class data is very sparse.
- The decision tree keeps splitting the data until each leaf has only one value. The anomalies would be classified at an earlier depth compared to the benign data.
- Hence it is able to classify the data.

Streaming Isolation Forests

- Uses sliding buffer memory window



$$S(x, N) = 2^{-\frac{E(h(x))}{c(N)}}$$

$$E(h(x)) = \frac{1}{L}\sum_{i=1}^{L} h_i(x)$$

LifeLong Spectral Clustering

Knowledge Library:-

1) orthogonal basis library: capturing latent cluster centers
2) feature embedding library: embedding the feature manifold information shared among multiple related tasks

As a new task arrives, knowledge from the orthogonal library and feature embedding library is used to obtain the encoding matrix, and this is further used to redefine the libraries.

Continual Learning in Unsupervised Setting

- **INSOMNIA:**
  - Semi-supervised intrusion detector with active learning
  - Nearest Centroid Neighbor classifier (NC) for labels
  - Tries explaining concept drift over time
- **OWAD (**Open World Anomaly Detection**):**
  - Talks about normality shift challenges for zero-positive anomaly detection.
  - Proposes general distribution-level framework to tackle it

Continual Learning in Unsupervised Setting

- **CURL** (Continual Unsupervised Representation Learning)**:**
  - Learns task-specific representations and deals with task ambiguity by performing task inference within the model
  - Deep learning model
- **UDA** (Unsupervised Domain Adaptation)**:**
  - Source Domain and Target Domain differ.
  - Source free method based on episodic memory replay with buffer management

Other Techniques

- Unsupervised Interior Clustering Tree (For unsupervised, not CL)
- Generative Replay Methods
- Latent/Orthogonal Representations
- Buffer Memory
- Clustering trees
- Generative random forests