

Poisoning Attack Against CDA-AL

1. Attack Value Assessment


2. Estimation of Labeling Budget Consumption


5. Poisoned Sample Generation

4. Sample Uncertainty Attribution

3. Constraint Search Based on Uncertainty


Attacker


Step I. Submit test data \mathbf{D}_{te}^{t+1}
(including poisoned samples) to Inference


Victim Model f_{θ_t}

New Round of
Concept Drift Adaptation

Step II. Concept Drift
Sample Selection



**Performance
Degradation**



Step III. Model Retraining

based on \mathbf{D}_{tr}^{t+1}



Victim Model $f_{\theta_{t+1}}$

High Uncertainty Samples \mathbf{D}_{dr}^{t+1}



Model



Clean Data



Attack Module



Poisoned Data