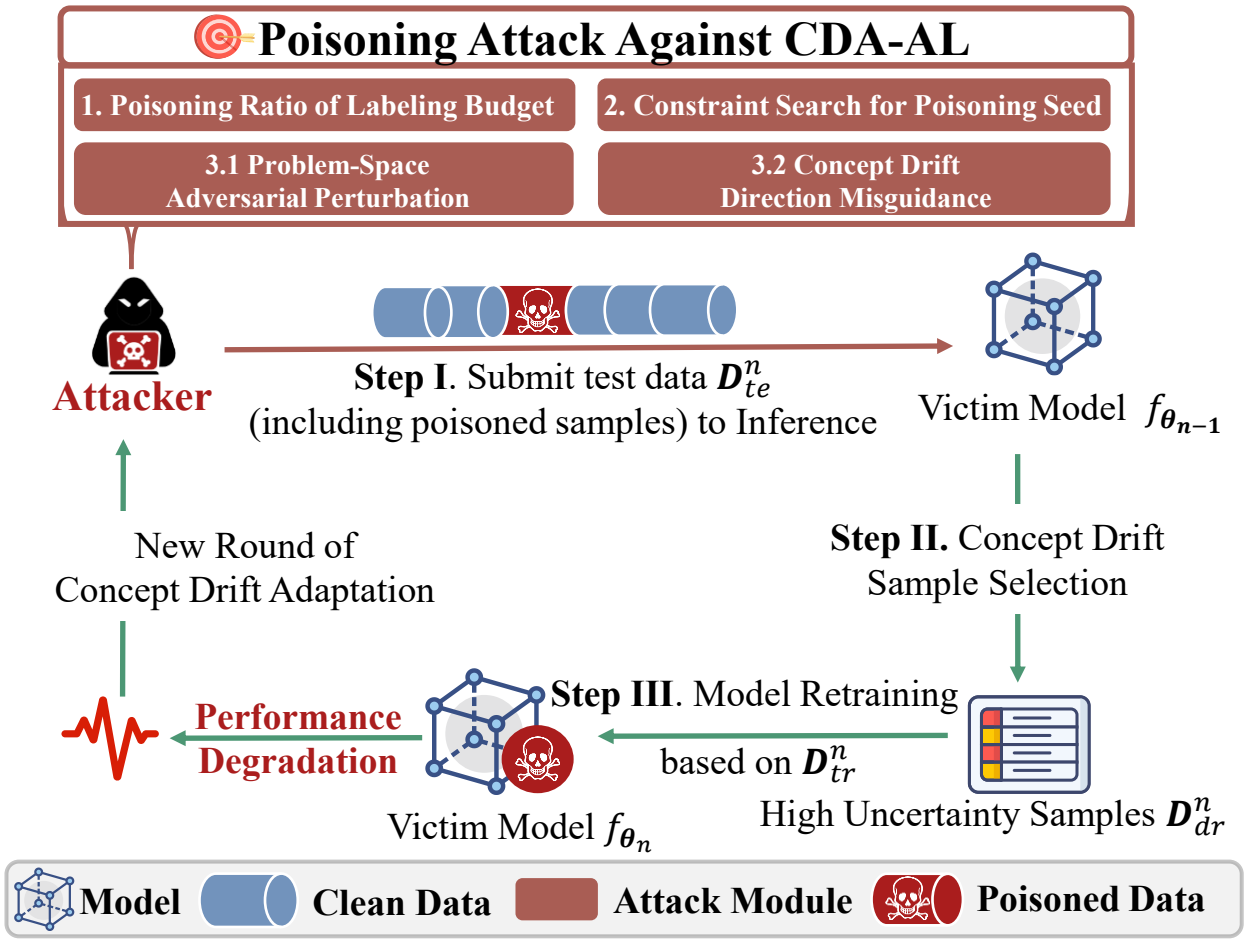
Poisoning Attack Against CDA-AL
1. Poisoning Ratio of Labeling Budget
2. Constraint Search for Poisoning Seed
3.1 Problem-Space Adversarial Perturbation
3.2 Concept Drift Direction Misguidance
Attacker
Step I. Submit test data D_{te}^{n} (including poisoned samples) to Inference
Victim Model $f_{\theta_{n-1}}$
Step II. Concept Drift Sample Selection
High Uncertainty Samples D_{dr}^{n}
Step III. Model Retraining based on D_{tr}^{n}
Victim Model f_{θ_n}
Performance Degradation
New Round of Concept Drift Adaptation
Model
Clean Data
Attack Module
Poisoned Data