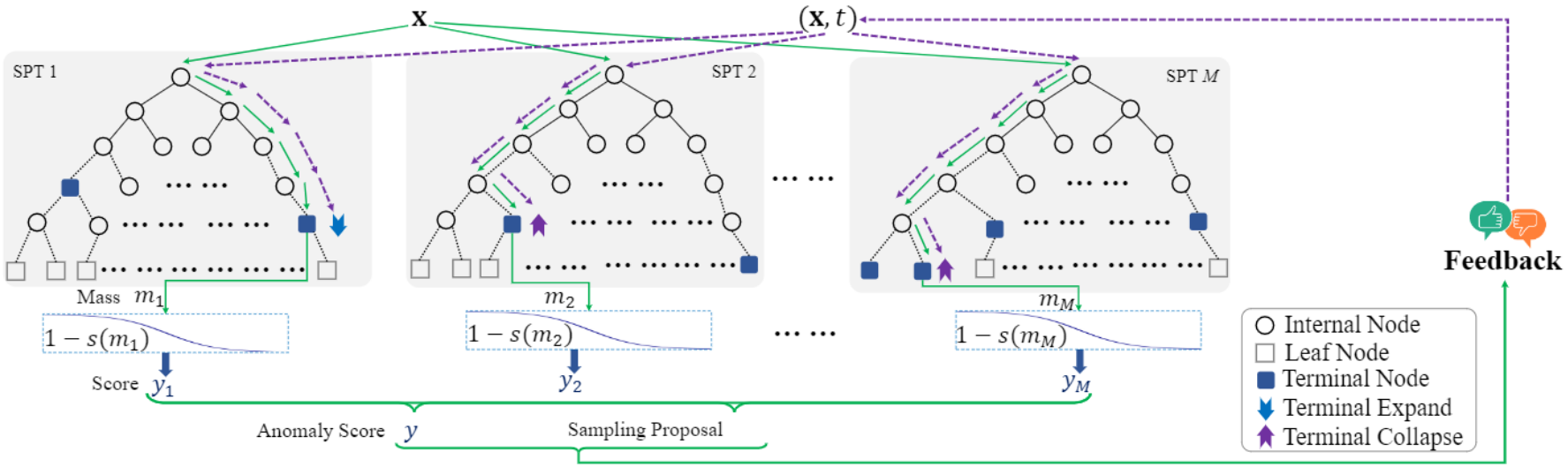
Human-Machine Interactive Streaming Anomaly Detection by Self-Adaptive Forest

Qingyang LI, Zhiwen YU, Huang XU, Bin GUO

Frontiers of Computer Science, DOI: 10.1007/s11704-022-1270-y

Problems & Ideas

- Problems of static streaming anomaly detection methods:
  - Static anomaly detectors have difficulty of adapting to distribution change in streaming anomaly detection.
  - The detection results of are often imprecise because of staic model structures and the unavailability of ground truth .
- Ideas: An online self-adaptive model that updates structures and anomaly scores under the guidance of human feedback .



The workflow of the proposed anomaly detector. The detector reports an anomaly score y when an instance x is fed to the system. The corresponding feedback t is given by a human expert, which is used to update the calculation of anomaly scores and structure of the model for the detector.

Main Contributions

- Contributions:
  - A human-machine interactive anomaly detection model is proposed. The anomaly detector is improved incrementally under the guidance of human feedback.
  - An instance sampling method for acquiring feedback from a human is designed. The amount of feedback is changeable according to the extent of the improvement of the detector.
  - A post tuning algorithm is designed for deciding an optimal update strategy in each iteration. The original model is adjusted from the perspectives of structures and the anomaly score calculation.

Dataset	iForest	HS-Trees	RS-Forest	LDOF	Loda	SA	MStream	AI^2	IF-AAD	ISPForest
Smtp	0.8831	0.8751	0.8823	0.8769	0.9945	0.9974	0.9315	0.9962	0.9936	**0.9983**
Http	**1.0000**	0.9964	0.9991	0.9854	0.9982	0.9775	0.9832	0.9994	0.9982	0.9999
Smtp+Http	0.9972	0.9965	0.9982	0.9396	0.9927	0.9891	0.9623	0.9944	0.9943	**0.9993**
Shuttle	**1.0000**	0.9394	0.9980	0.9388	0.9925	0.9922	0.9868	0.9986	0.9995	0.9999
Breastw	0.9905	0.9924	0.9857	0.9983	0.9880	0.9914	0.9803	0.9988	0.9974	**0.9992**
Annthyroid	0.8233	0.7121	0.7327	0.7264	0.7592	0.8052	0.8197	0.8081	0.8224	**0.8435**
Cardio	0.8656	0.8417	0.7474	0.6983	0.7008	0.8112	0.8419	0.8331	0.8684	**0.8982**

Performance comparison of different methods on all benchmark datasets. AUC score is measured. Bold and underline results respectively indicate the best and second-best methods on each dataset.