Theme: Machine Learning

Topic: Fraud/crawler detection using user behavior sequence

Background

Modern e-market systems are confronted with many cyber security issues, such as web crawler, promotion abuse, spam comments.

There has been a number of mechanisms that help detect crawler or fraud users in current systems. For example, expert systems, rule-based methods, traditional machine learning approaches. However, those approaches are heavily depended on expert experience and feature engineering.

Deep learning is proven to be effective end-to-end approach for sequence classification and time series classification. We are hoping to develop a cutting-edge model that using attributed user behavior sequence for crawler/fraud detection.

This task has many challenges. First, the labeled instance is far less than the whole data set. Few-shot learning or deep transfer learning methods could be involved. The action in sequence is attributed with both numerical and categorical features. New network architecture is required for utilizing the numerical and categorical attributes simultaneously.

Target

- A methodical model based on our production system. A deep learning based methodology is preferred.

Related Research Topics

- Traditional methods about fraud detection.
- Sequence classification with deep learning approaches.
- Few-shot learning in fraud detection applications.

Suggested Collaboration Method

AIR (Alibaba Innovative Research), one-year collaboration project.