Anomaly Detection in Social Networks

Anahitta Davoudi*, University of Central Florida

As social network systems grow, they get affected by huge number of fake user profiles. Particularly, social recommender systems are vulnerable to profile injection attacks where malicious profiles are injected into the rating system to affect users opinion. The objective of attackers is to inject a large set of biased profiles that provide favorable or unfavorable recommendations for a product. We propose a classification approach for detection of attackers. First, we define attributes that provide the likelihood of a user having a profile of that of an attacker. Using user-item rating matrix and user-connection matrix, we find if the ratings are abnormal and if there are random connections in the network. Then, we use k-means clustering to categorize users into authentic users and attackers. To evaluate our framework, we use Epinions dataset and inject intelligent push and nuke attacks. For performance evaluation, we use precision and recall to show that k-means clustering can identify the attackers with high accuracy and low false positives.

Keywords: Recommender Systems, Social Networks, Anomaly Detection