A SNA Approach to Detecting Suspicious Online Financial Activities

Lei Tang, Geoffrey Barbier, Huan Liu
Computer Science and Engineering, Arizona State University, USA
{l.tang, gbarbier,huan.liu}@asu.edu

Challenges & Motivations
- Challenges:
  - A fine line between legal and illegal financial transactions
  - Huge number of noisy network transactions
  - Activities across time
  - Criminal activities demonstrate interesting structures.
- Social Network Analysis (SNA) can help:
  - Exploit tips: confirm or reject the legitimacy of tips and follow the lead to find potential associates
  - Understand roles: capture various roles of actors such as sink, intermediary, distributor and the relationships between actors for subject-based data mining
  - Discover interesting patterns: most actors with similar statistics perform some routine tasks.
- Empirical Study:
  - Access to financial data is limited
  - Resort to Enron Email corpus

Introduction
- Financial institutions submit Suspicious Activity Reports (SARs) to the Financial Crimes Enforcement Network (FinCEN). Among 53,590 cases in 2007-2008, 45% were wire transfer fraud. Many eye-opening cases:
  - A bankrupt defendant made over 1,000 deposits at several different bank locations, totaling more than $500,000. These transactions took place at several different locations in amounts less than $10,000 and, in one instance, five transactions occurring in one business day. The defendant was making cash deposits totaling up to $30,000 monthly and writing numerous $2,000 checks to himself and family members.
  - Stealing from numerous accounts relatively small amounts of money via computer intrusion, credit card fraud, debit card fraud, and wire transfer fraud shows an unusually large number of inlinks to the defendant’s node.
  - “Victims would send money to him, mostly through wire transfers and personal checks that he deposited in various accounts, and he would withdraw the money in structured transactions. With cash in hand, he would purchase money orders to send to the principals.”

Case Studies of SNA
- Suspicious Activity Detection based on Pattern Difference: $\text{difference} = \text{distance}(a, a_i)
  - Pete Davis’s removal results in a sharp pattern change: 3 spikes $\rightarrow$ 1 spike
    - Most of Peter’s email are garbage: real-time transaction reminders generated by machines every hour.
- Community Pattern Discovery and Key Actors
  - Use depth-first search to find all maximal cliques
  - Merge cliques with overlap $> \epsilon$ into one cluster
  - Actors connecting two cliques are key actors

Data Mining and Machine Learning Lab

Conclusion
As financial crimes continue to increase, SNA techniques may be a useful tool to guide investigators to suspects, and aid administrators in detecting unlawful activities.

This work is, in part, supported by AFOSR.

Key actors plays a key role in reality as well.
Jeff Steffs is the vice president in Enron for government affairs.