FRAUD DETECTION THROUGH GRAPH-BASED USER BEHAVIOR MODELING

Alex Beutel
Leman Akoglu
Christos Faloutsos

Carnegie Mellon University

Stony Brook University

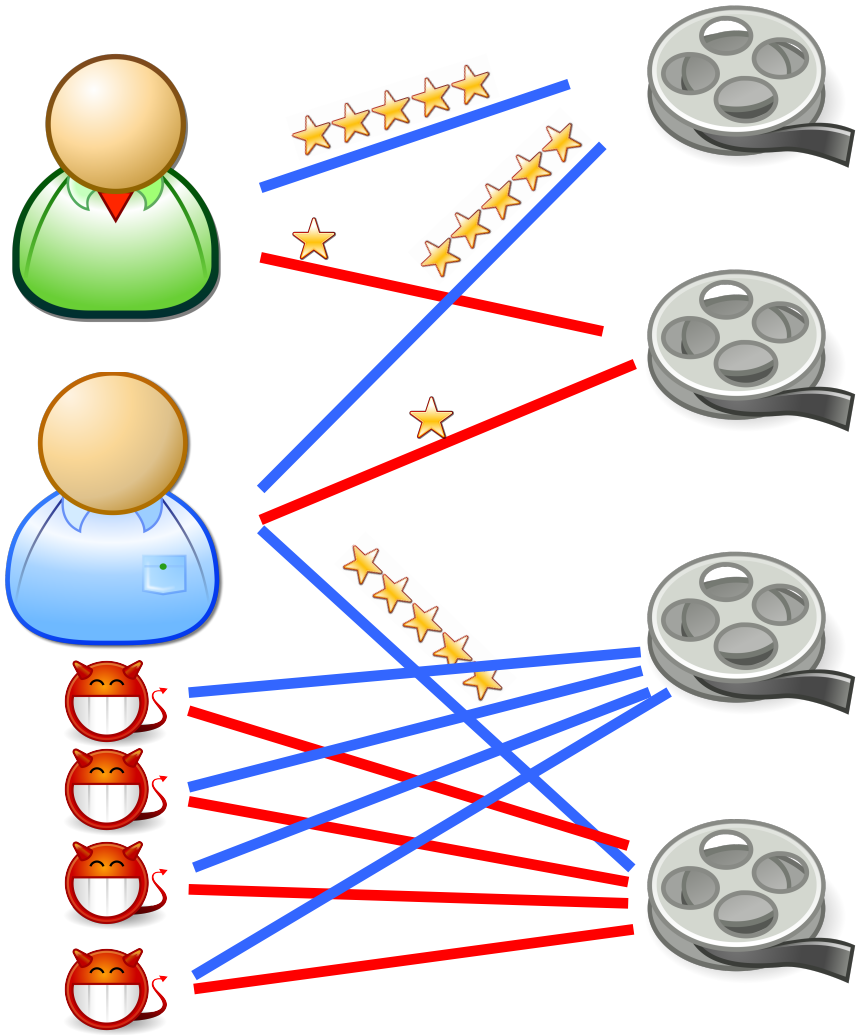
bit.ly/ccs2015_graphmodeling

CCS 2015 – October 13, 2015 – Denver, CO

Thanks to

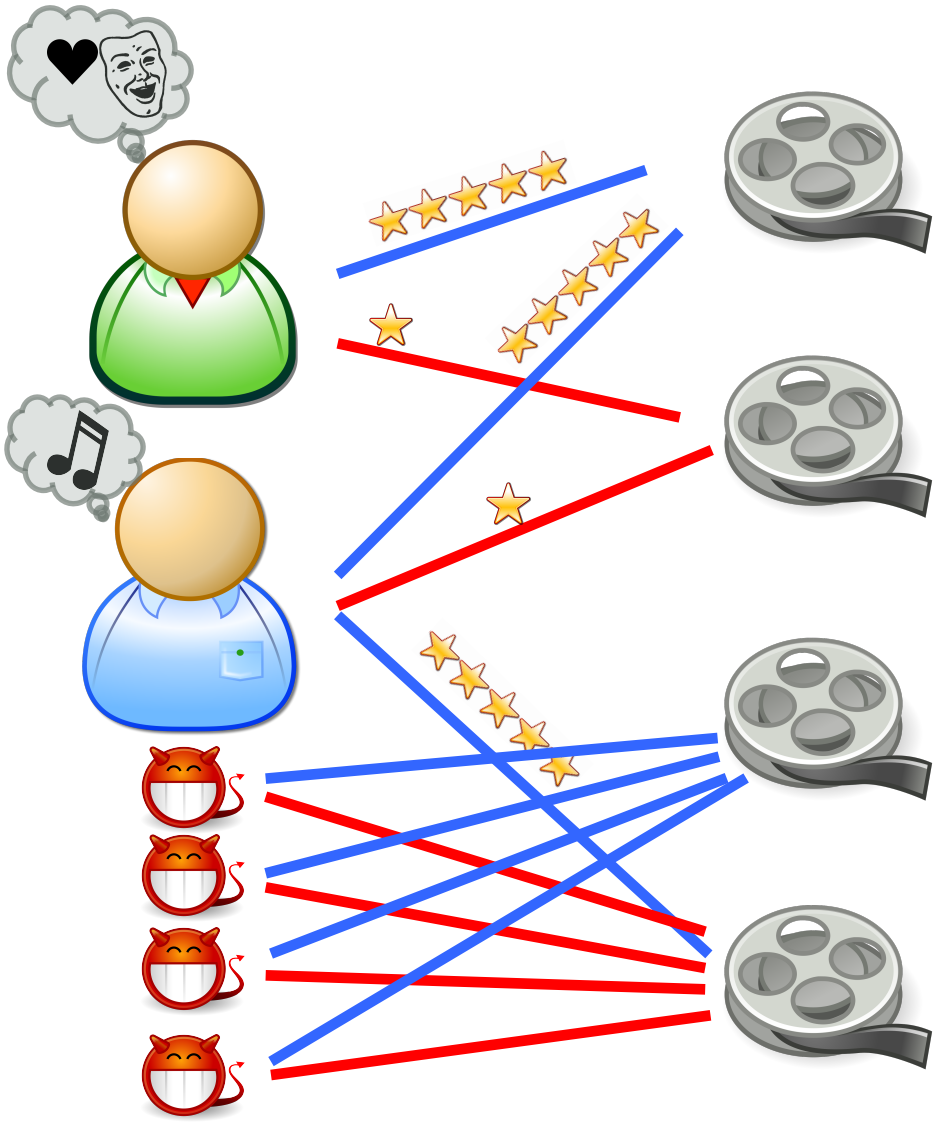
NSF Grant No. IIS-1408924, IIS-1408287,
CAREER 1452425, DGE-1252522, ...

User Behavior Challenges



NETFLIX

User Behavior Challenges

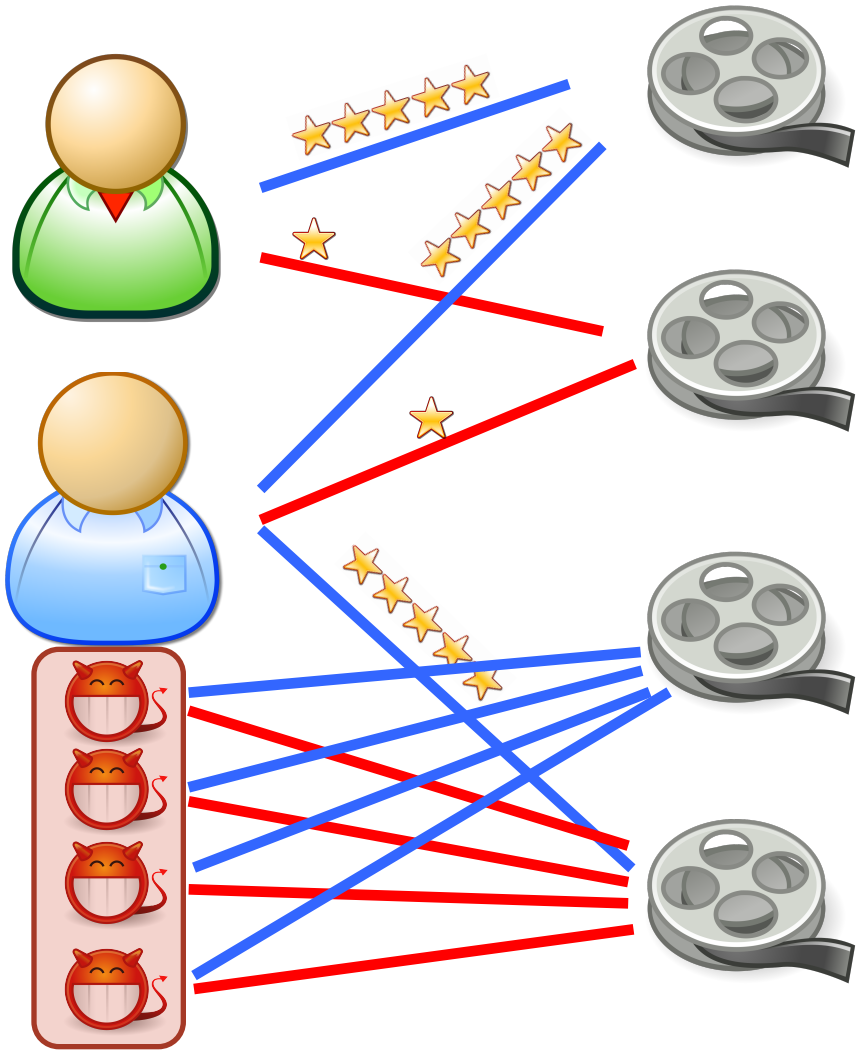


Three Main Questions:

1. How can we understand typical/normal user behavior in a graph?

NETFLIX

User Behavior Challenges

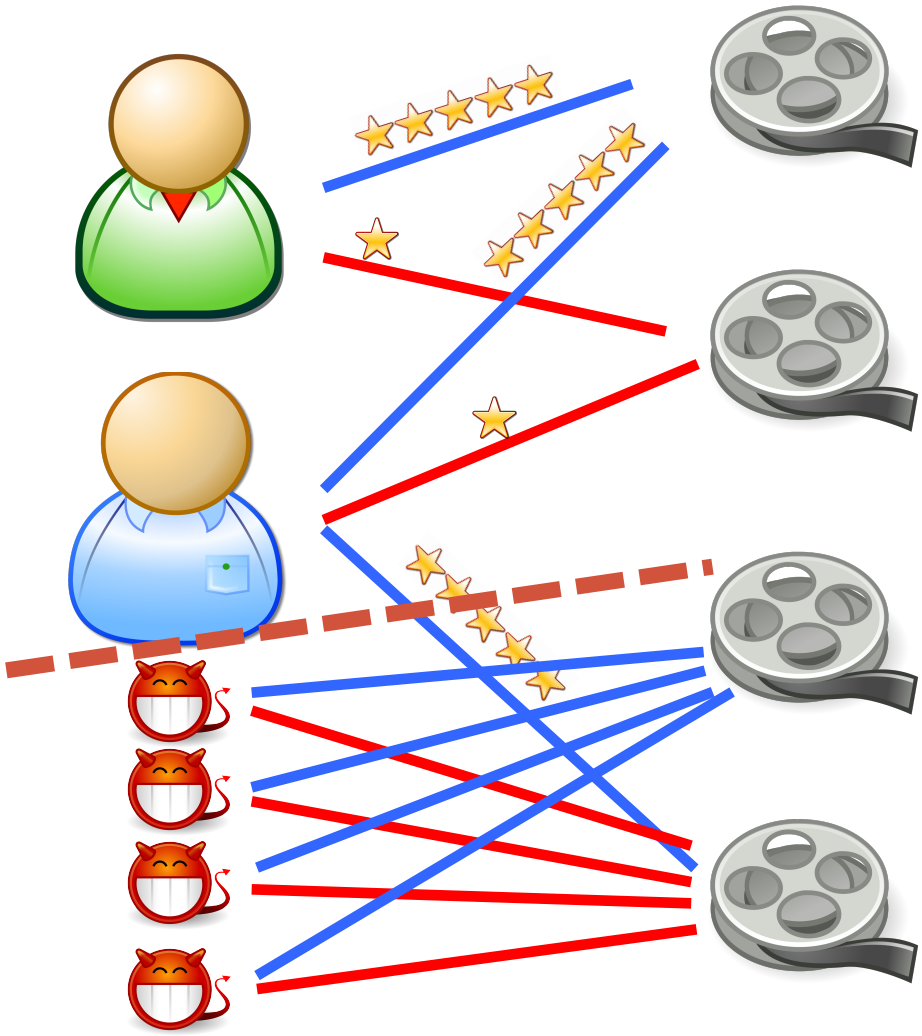


Three Main Questions:

1. How can we understand typical/normal user behavior in a graph?
2. How can we find suspicious user behavior?

NETFLIX

User Behavior Challenges

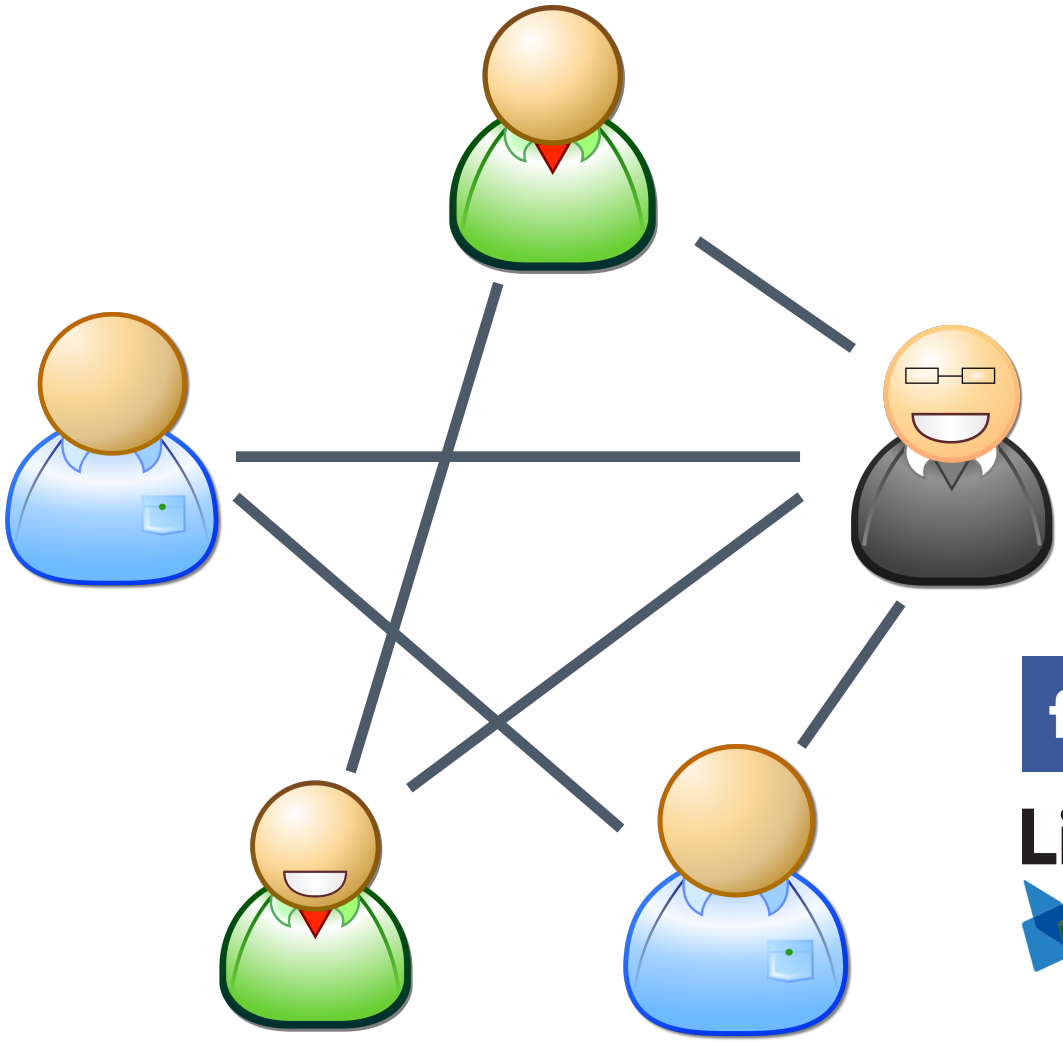


Three Main Questions:

1. How can we understand typical/normal user behavior in a graph?
2. How can we find suspicious user behavior?
3. How can we distinguish the two?

NETFLIX

Graphs of User Behavior



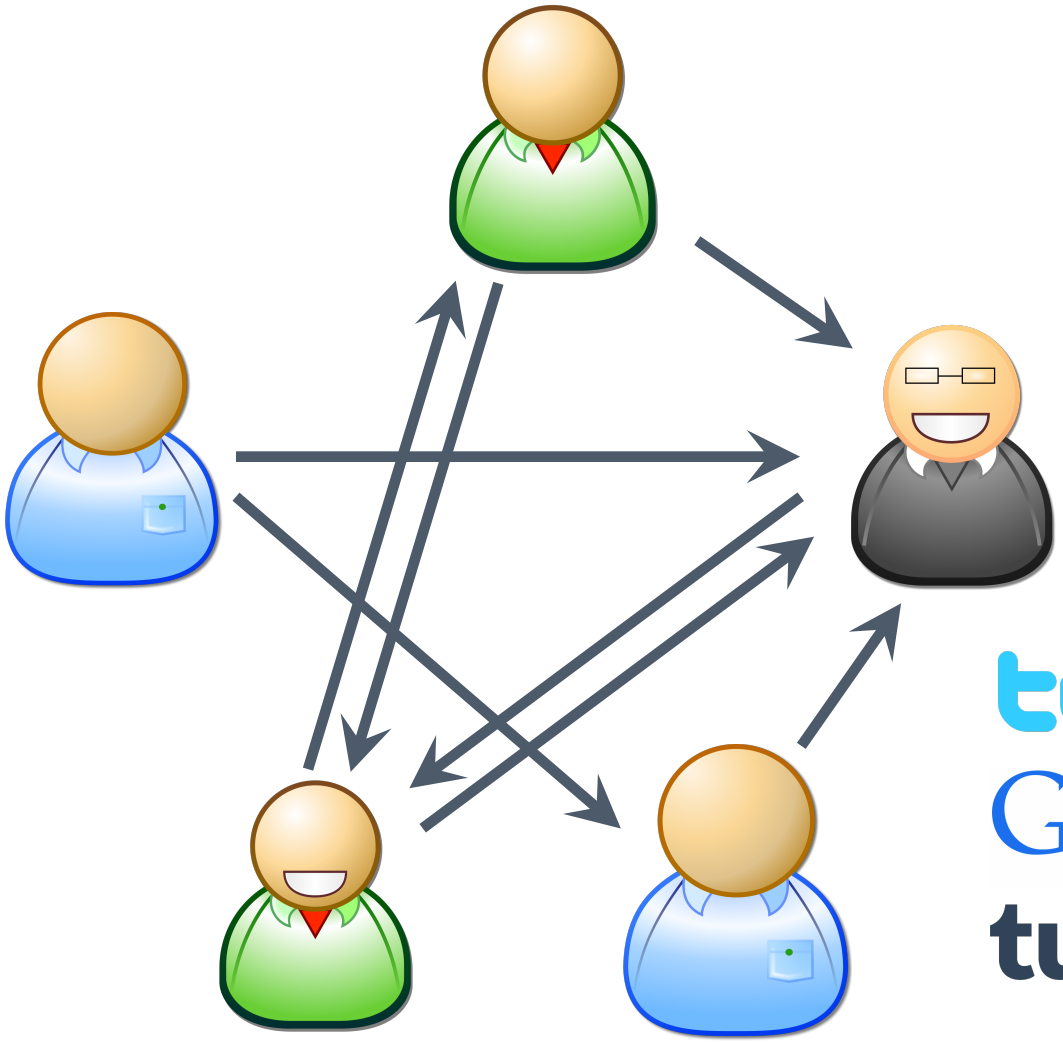
- Undirected graphs

facebook

LinkedIn

dblp
computer science bibliography

Graphs of User Behavior



- Undirected graphs
- Directed graphs

twitter

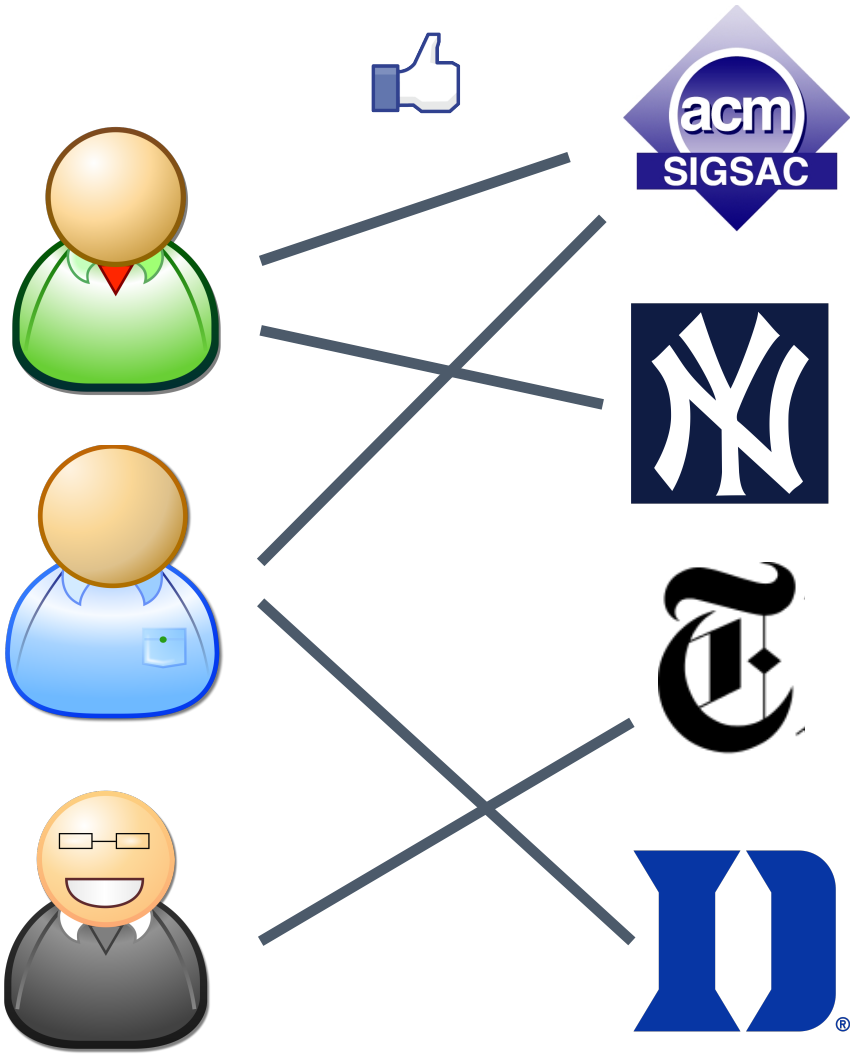
Google+

tumblr.

Instagram
Fast beautiful photo sharing

腾讯微博 测试版
t.qq.com

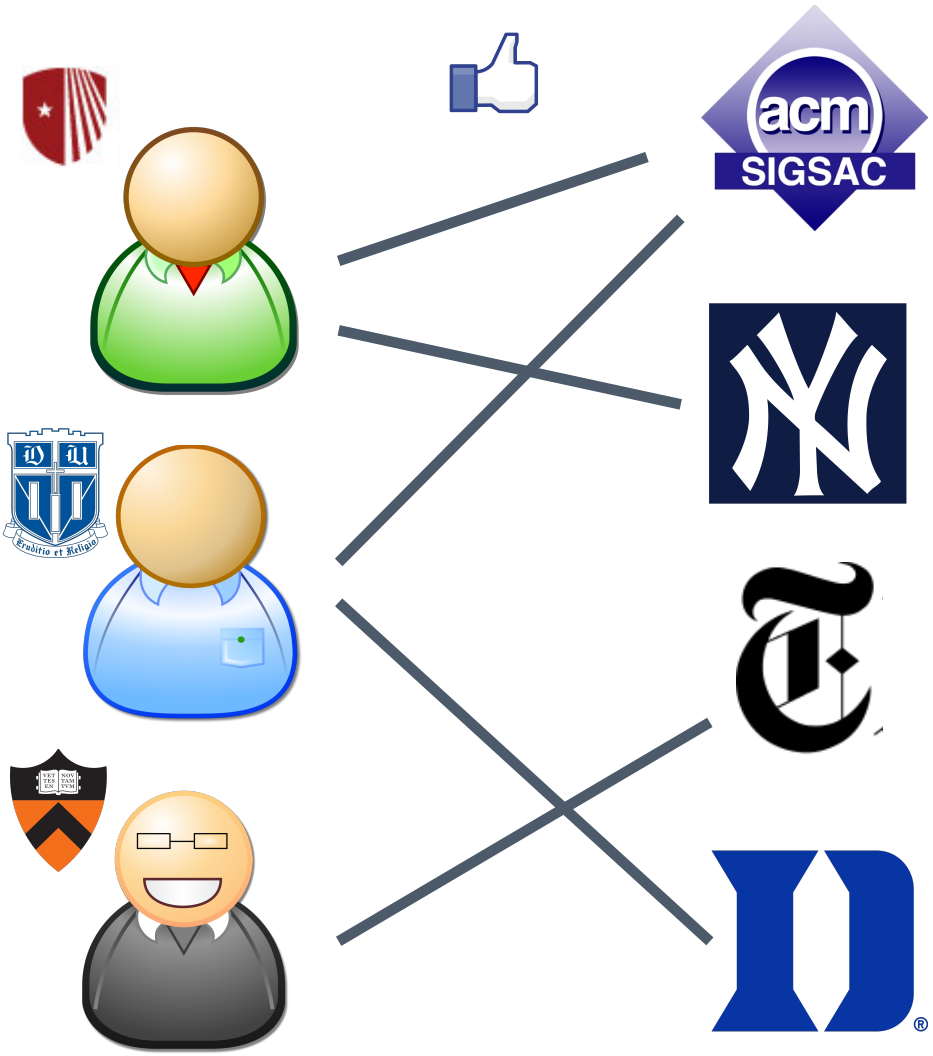
Graphs of User Behavior



- Undirected graphs
- Directed graphs
- Bipartite graphs

facebook
YouTube
GitHub

Graphs of User Behavior



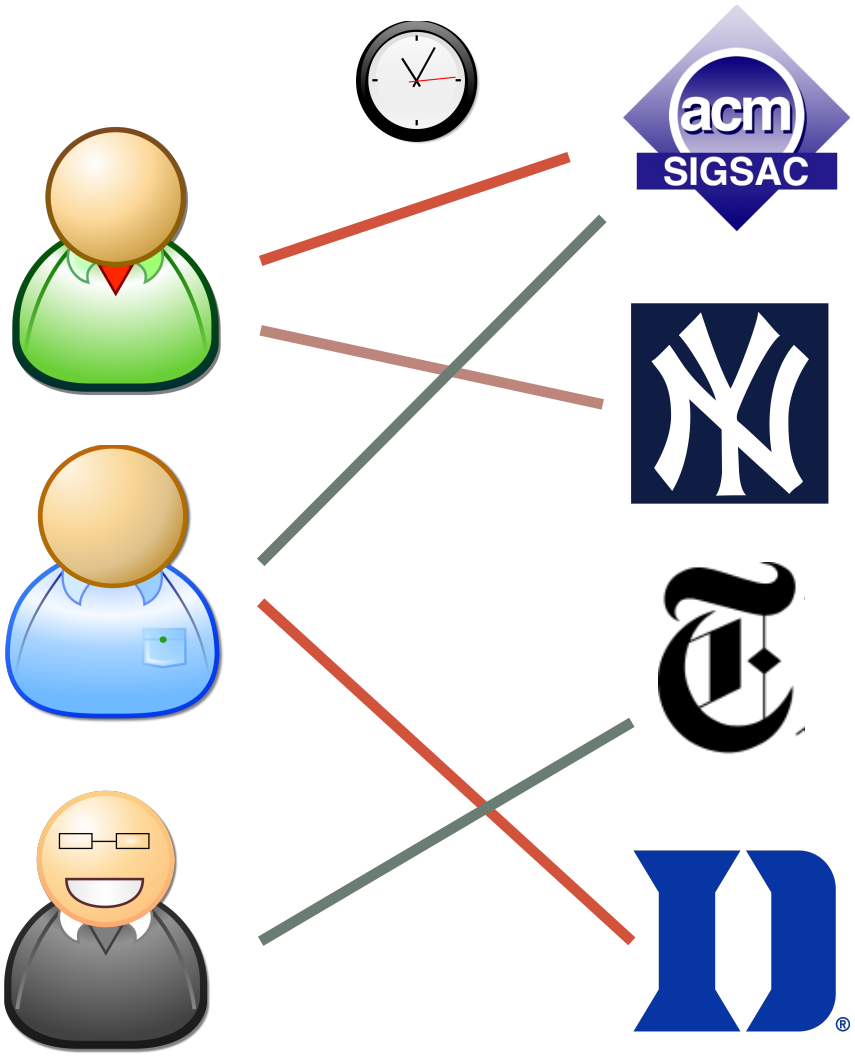
- Undirected graphs
- Directed graphs
- Bipartite graphs
- Node attributes

facebook

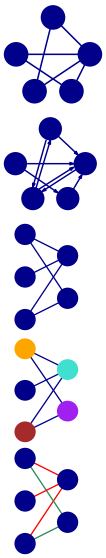
YouTube

GitHub

Graphs of User Behavior



- Undirected graphs
- Directed graphs
- Bipartite graphs
- Node attributes
- Edge attributes

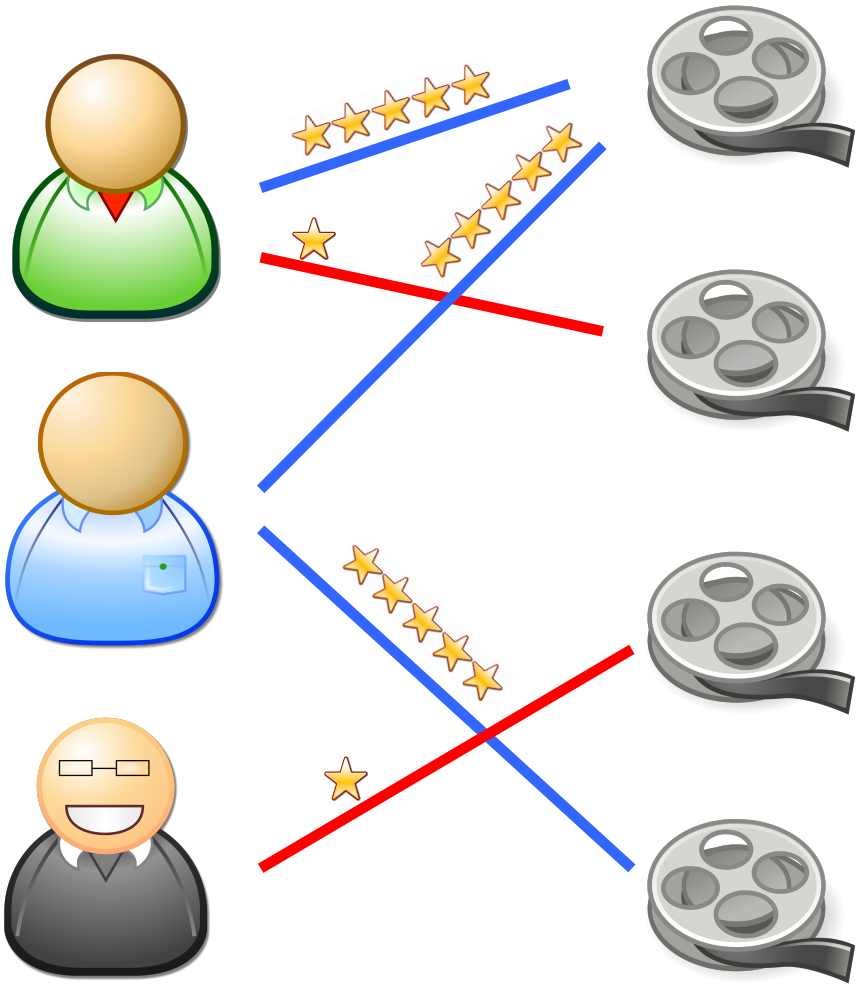


facebook

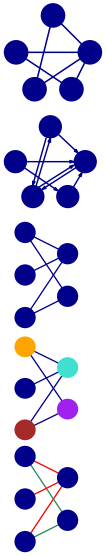
YouTube

GitHub

Graphs of User Behavior

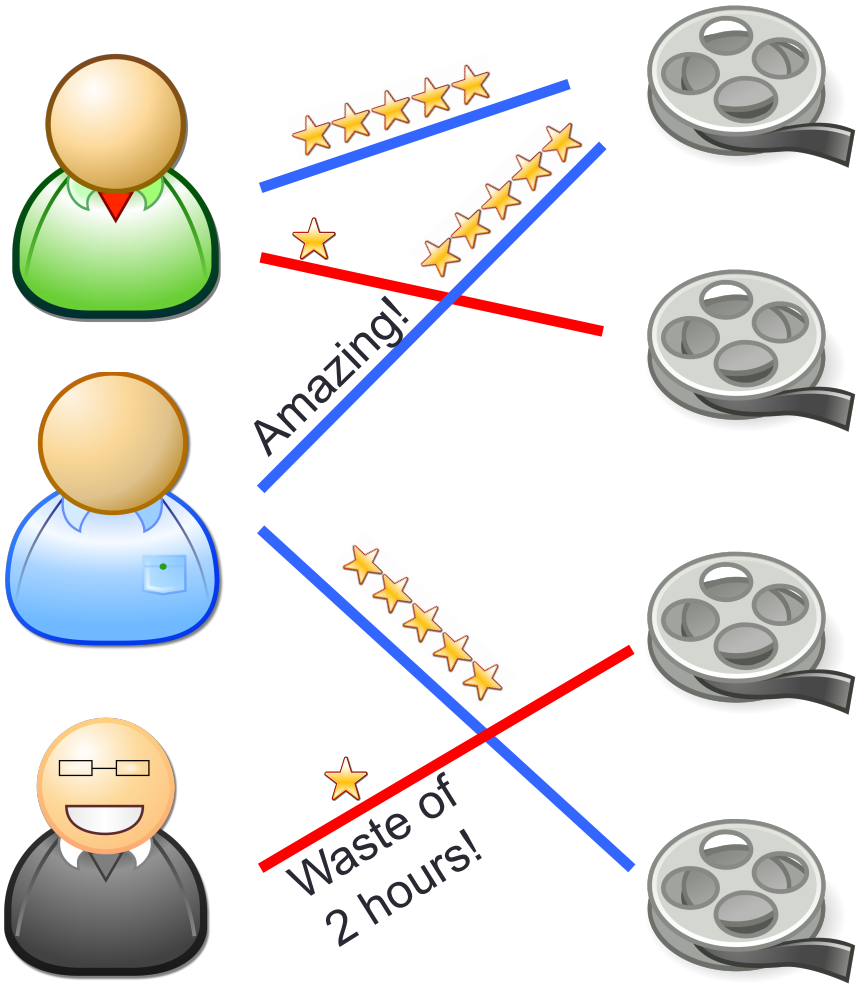


- Undirected graphs
- Directed graphs
- Bipartite graphs
- Node attributes
- Edge attributes

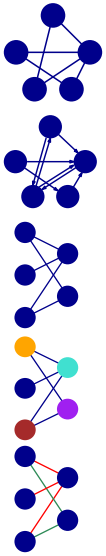


NETFLIX amazon.com yelp newegg Google play reddit

Graphs of User Behavior

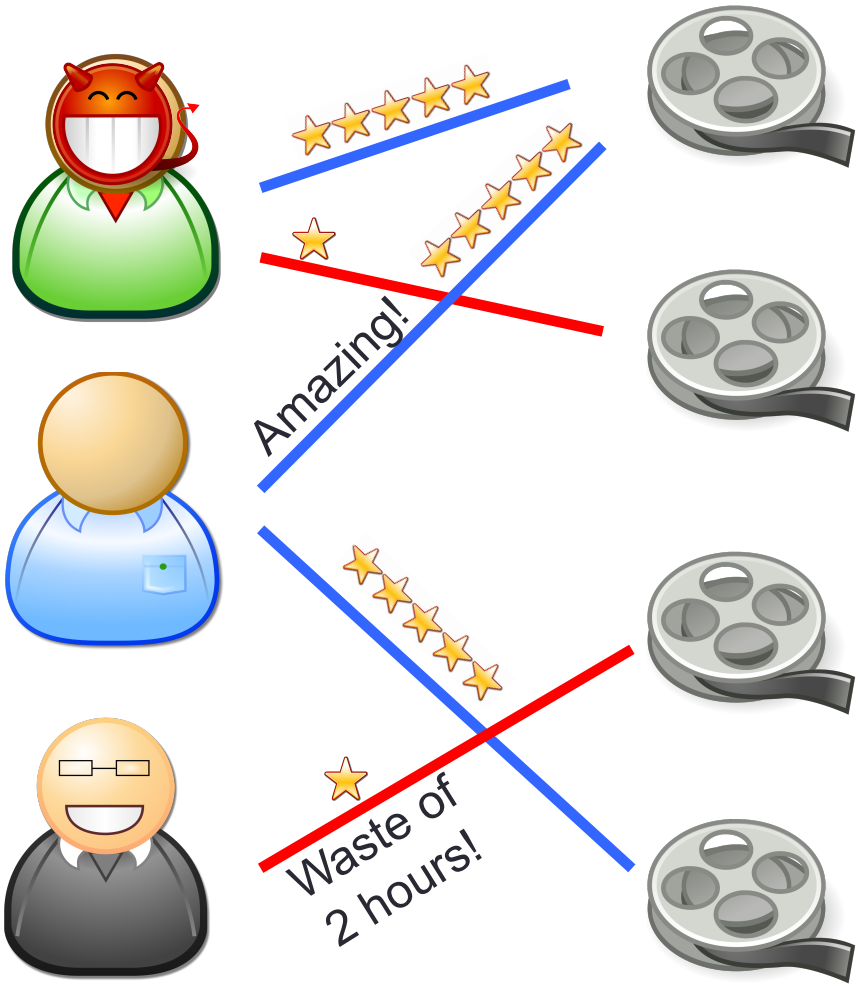


- Undirected graphs
- Directed graphs
- Bipartite graphs
- Node attributes
- Edge attributes

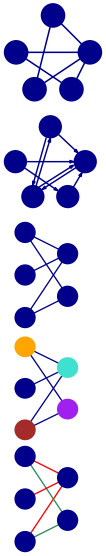


NETFLIX amazon.com yelp newegg Google play reddit

Graphs of User Behavior



- Undirected graphs
- Directed graphs
- Bipartite graphs
- Node attributes
- Edge attributes



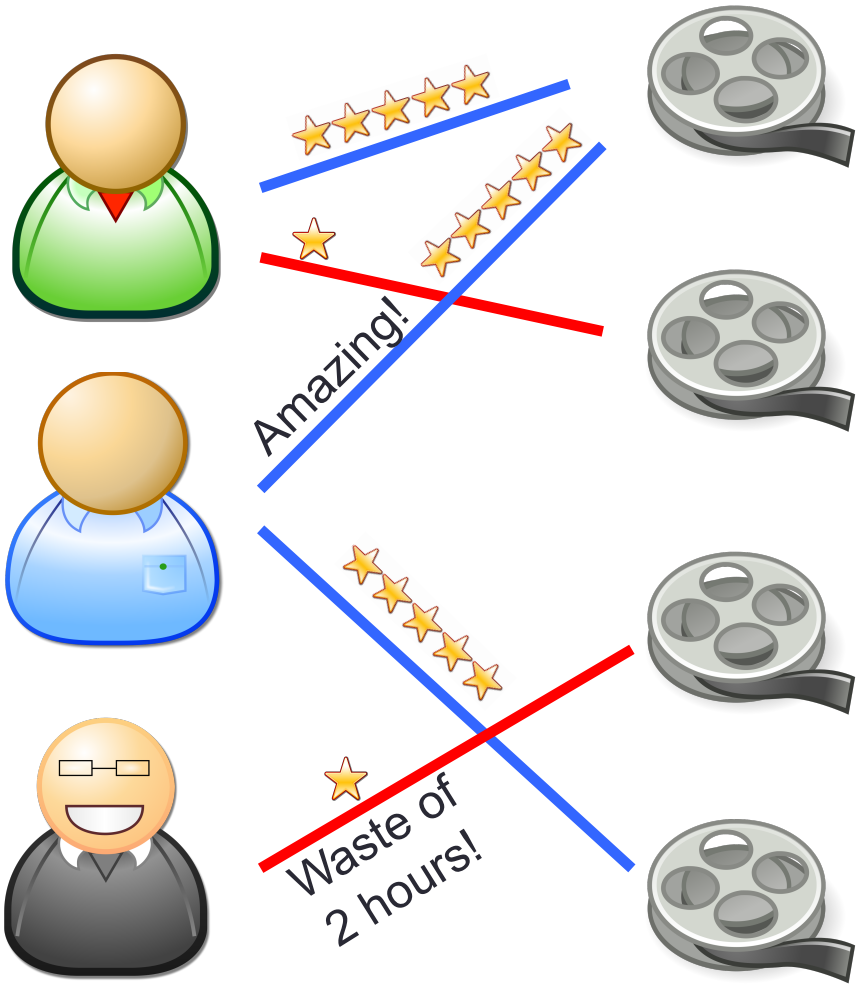
Semi-supervised

NETFLIX amazon.com

yelp newegg

Google play reddit

Graphs of User Behavior



{ Undirected
Directed
Bipartite }

×

{ Node Attributes }

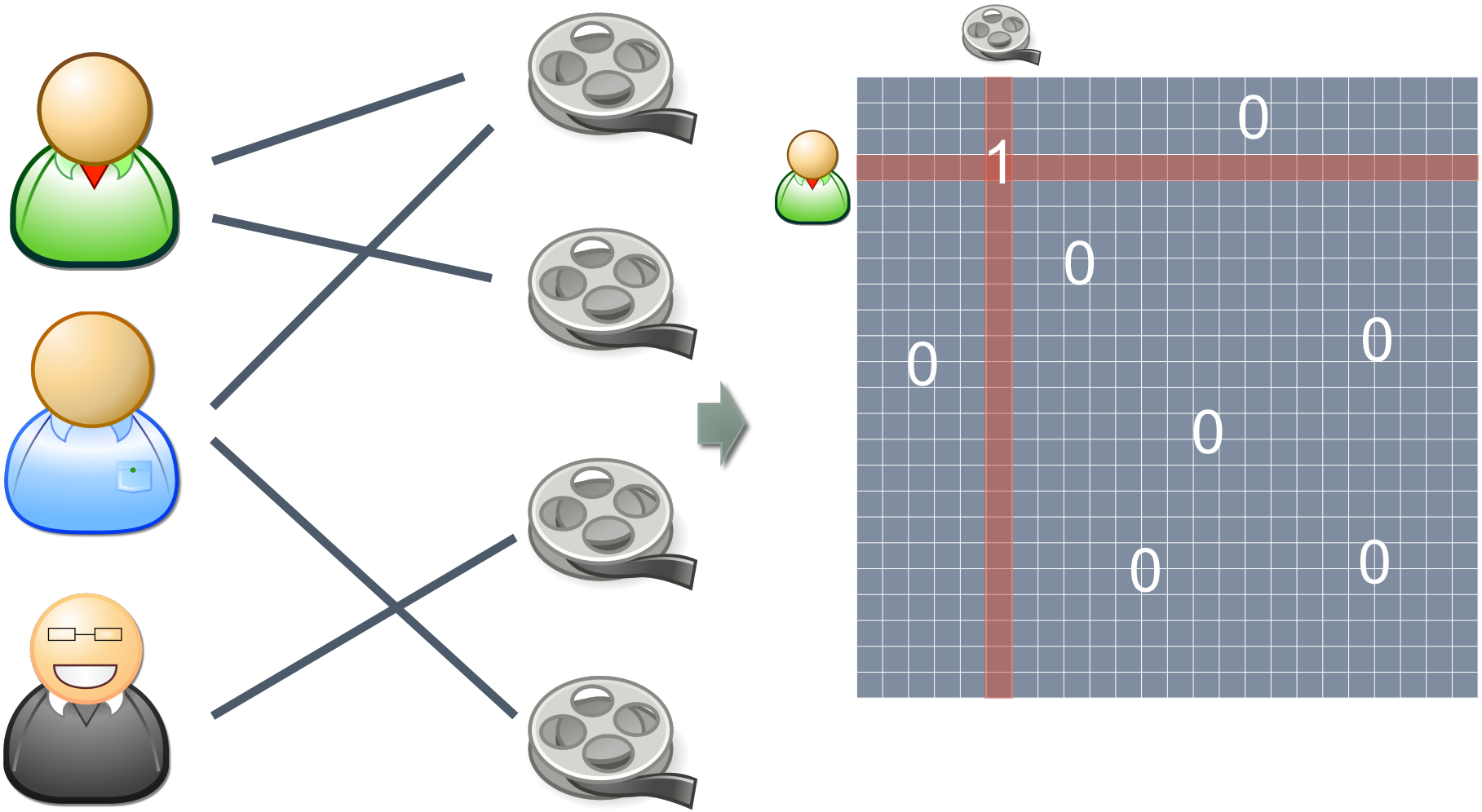
×

{ Edge Attributes }

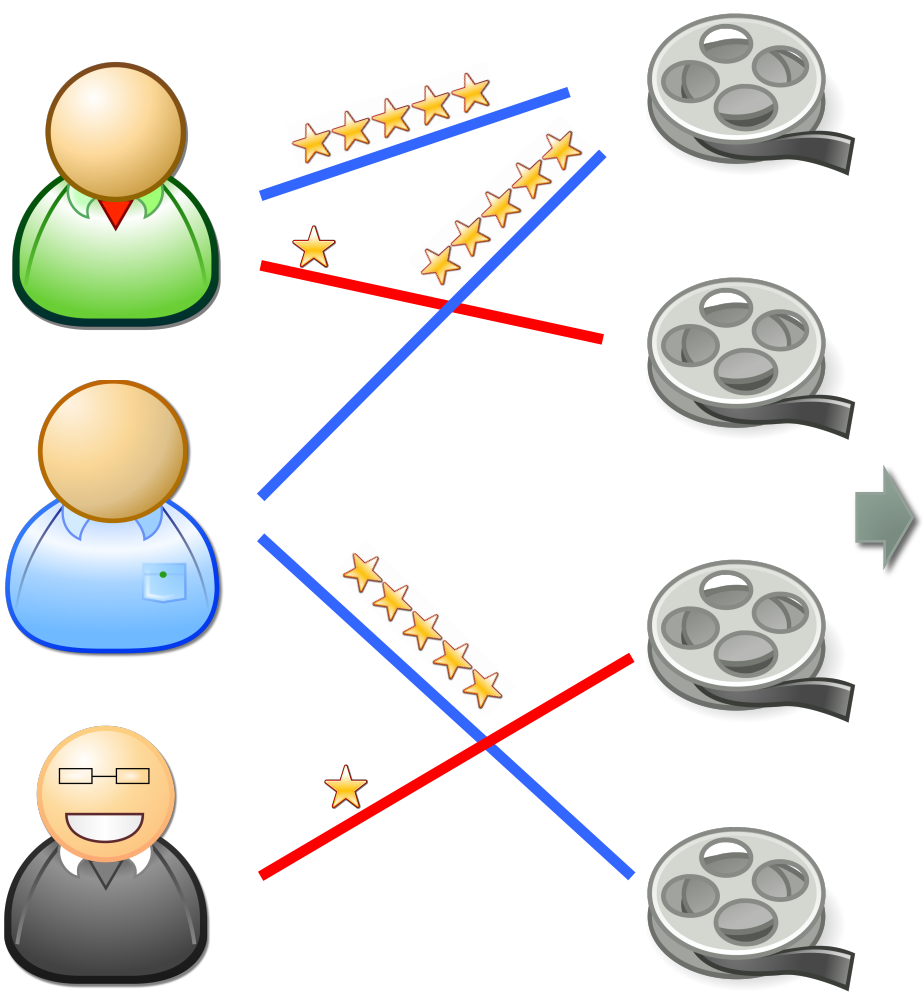
×

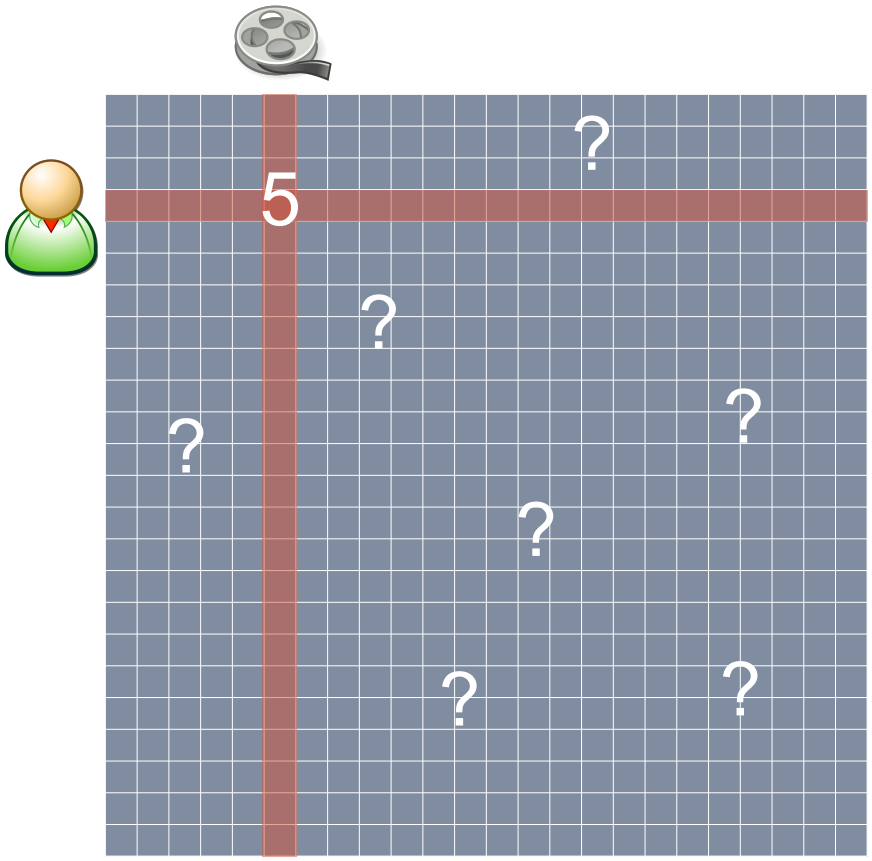
{ Unsupervised
Semi-Supervised }

Graphs of User Behavior

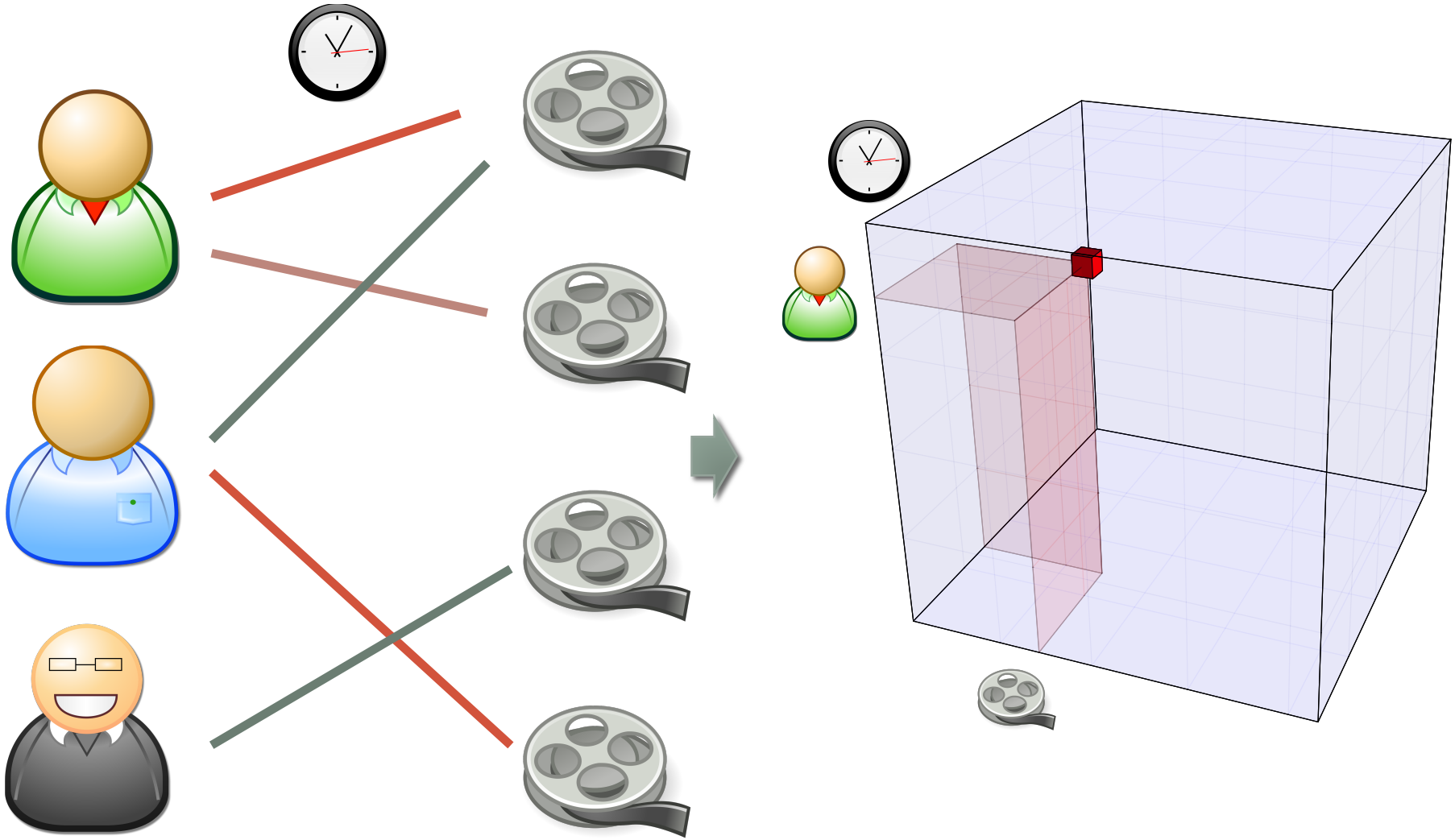


Graphs of User Behavior

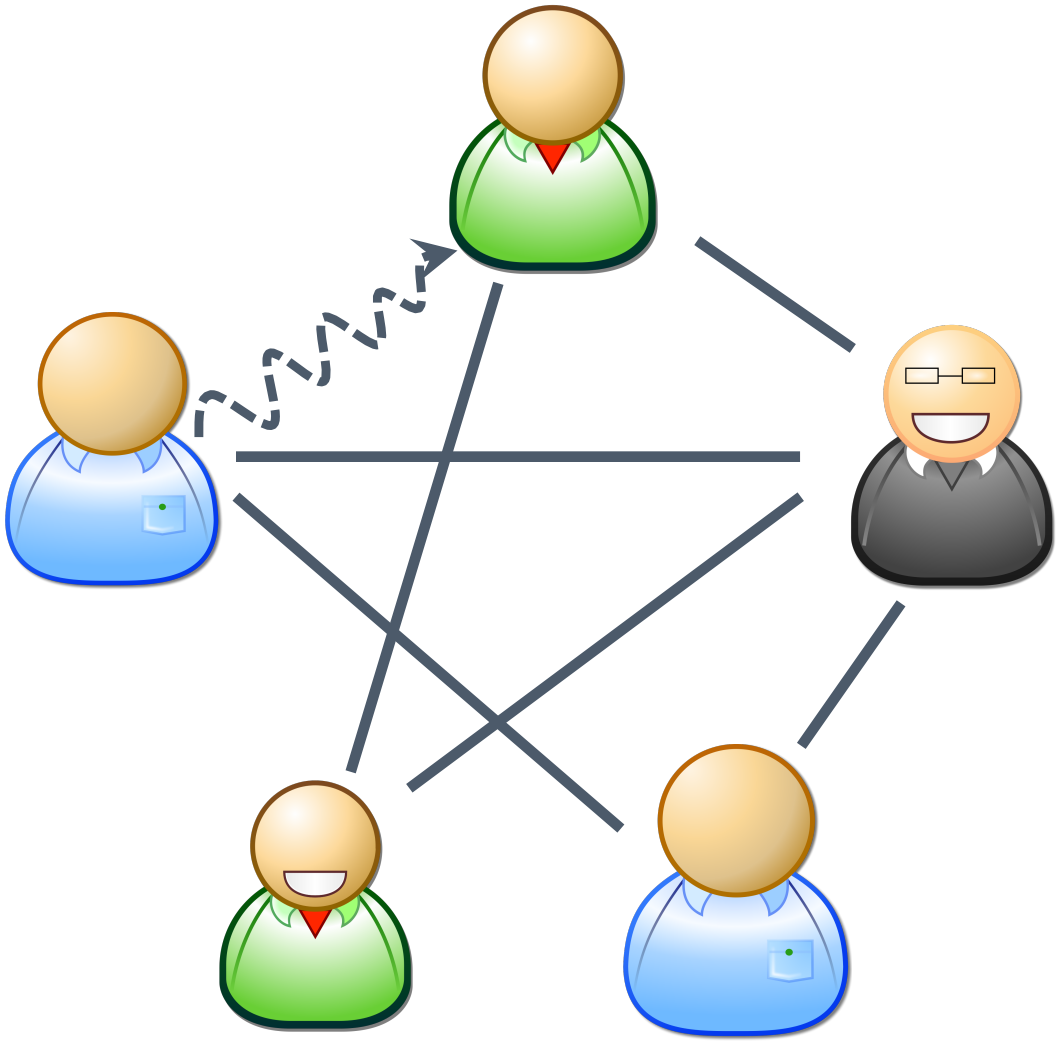




Graphs of User Behavior

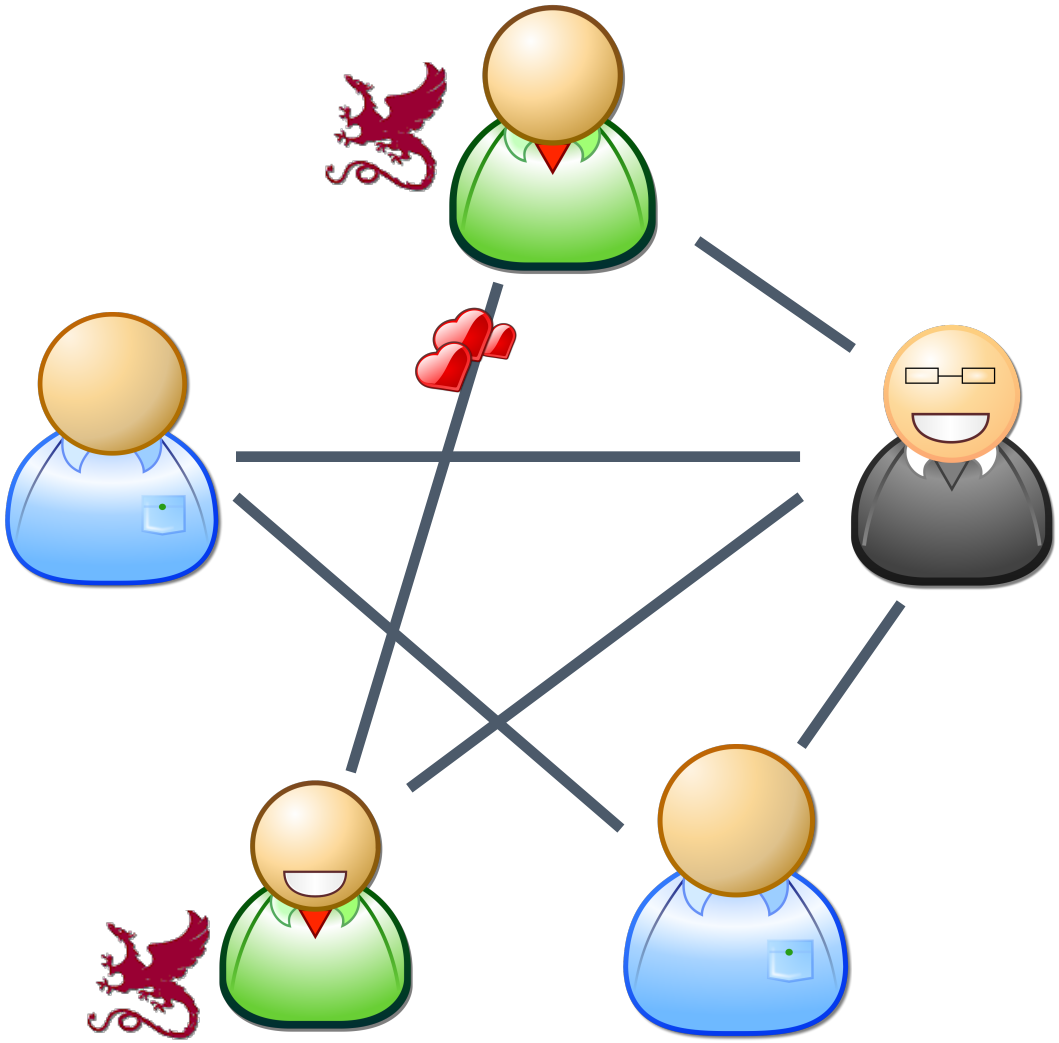


Modeling "Normal" Behavior



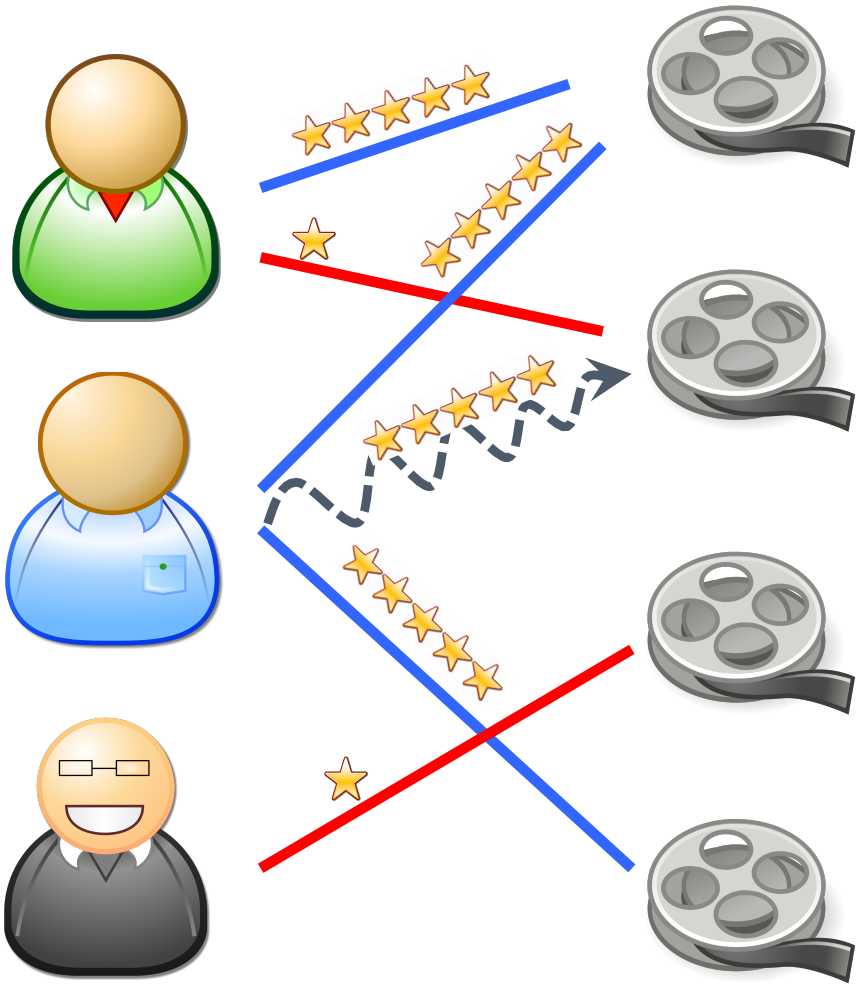
- Predict edges

Modeling User Behavior



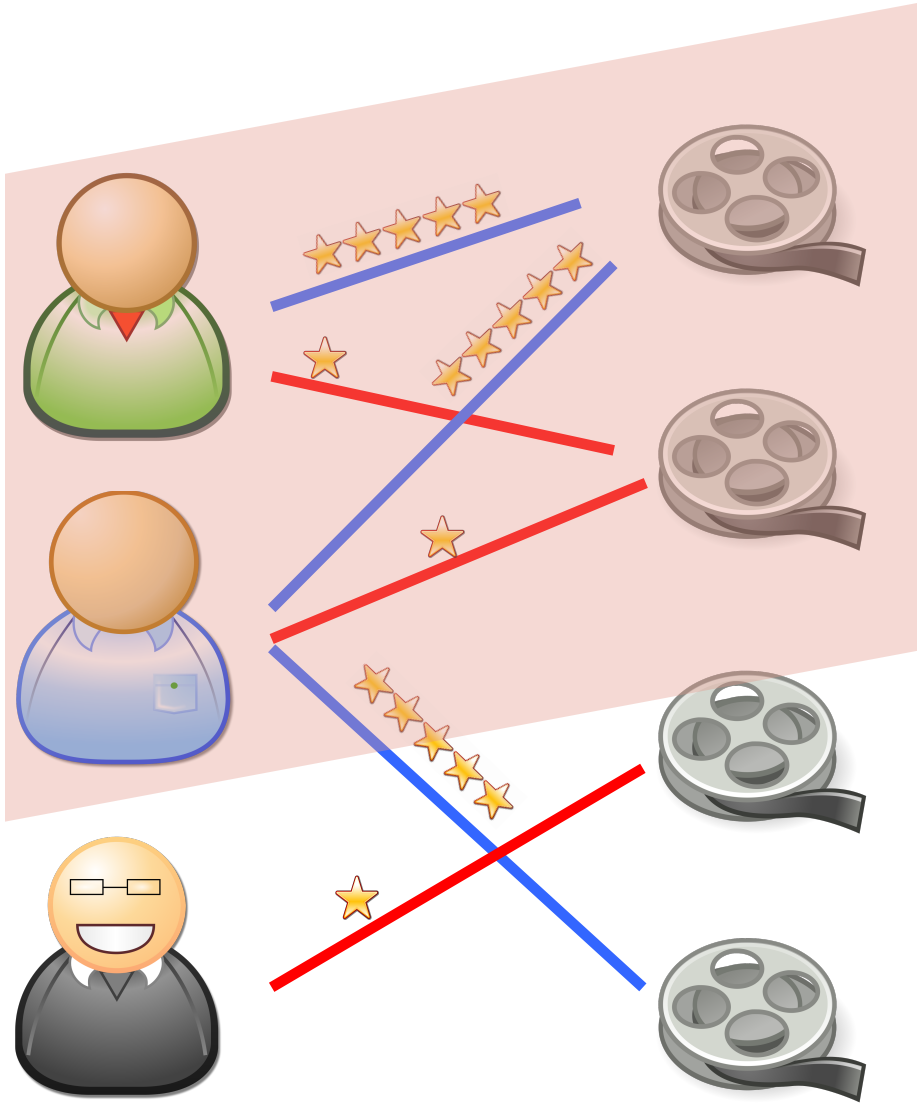
- Predict edges
- Predict node attributes
- Predict edge attributes

Modeling User Behavior



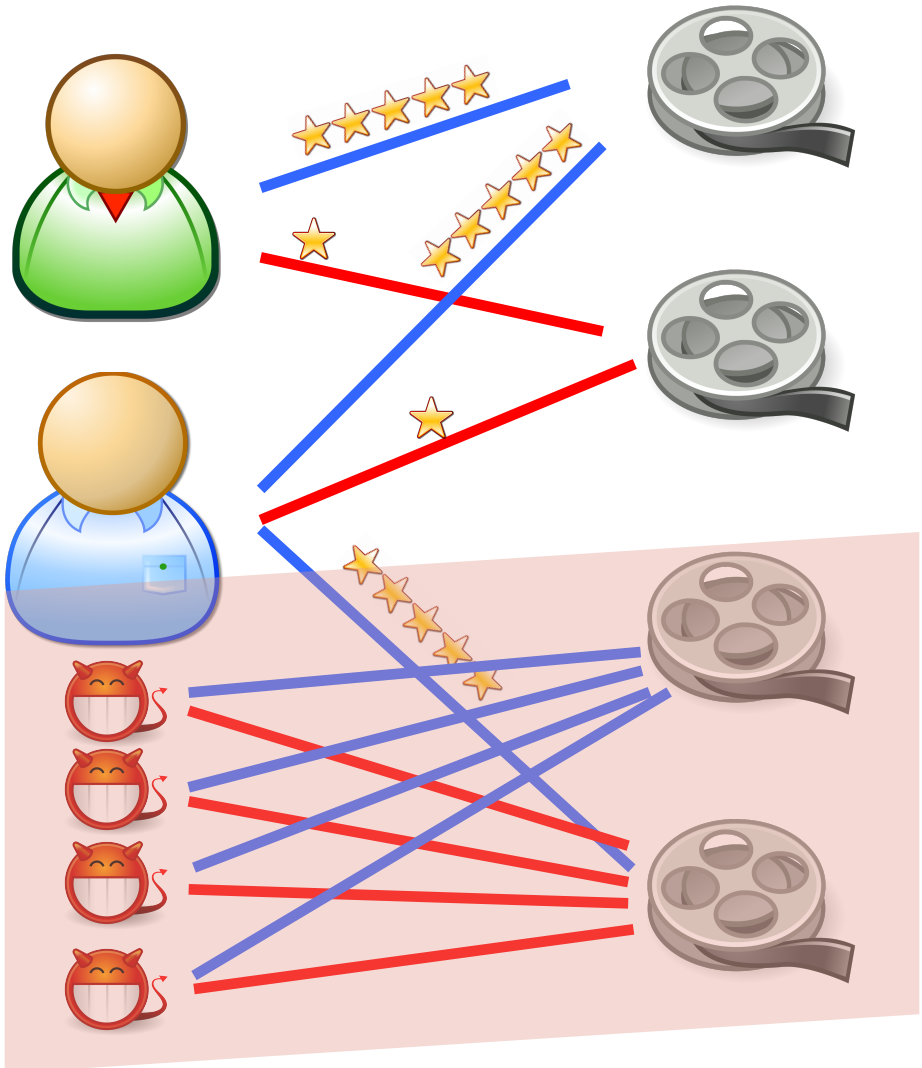
- Predict edges
- Predict node attributes
- Predict edge attributes
  - “Netflix Problem”

Modeling User Behavior



- Predict edges
- Predict node attributes
- Predict edge attributes
  - “Netflix Problem”
- Frequent Itemset Mining & Community Detection

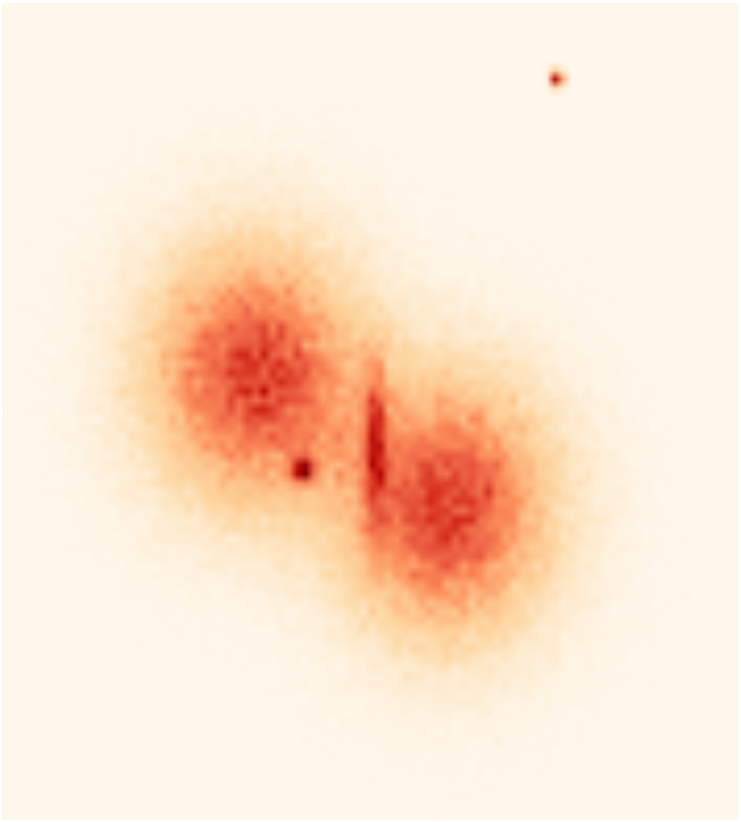
Modeling User Behavior



- Predict edges
- Predict node attributes
- Predict edge attributes
  - "Netflix Problem"
- Frequent Itemset Mining & Community Detection
- **Fraud Detection**

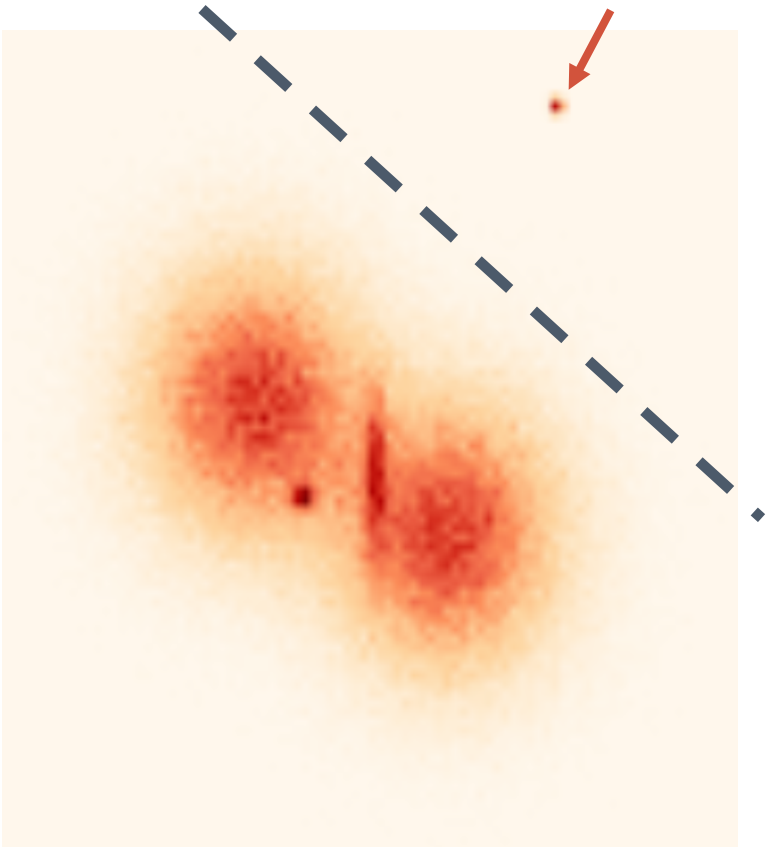
Deceives users and manipulates recommendations!

Modeling User Behavior



Modeling normal users and detecting anomalies are two sides of the same coin – understanding user behavior.

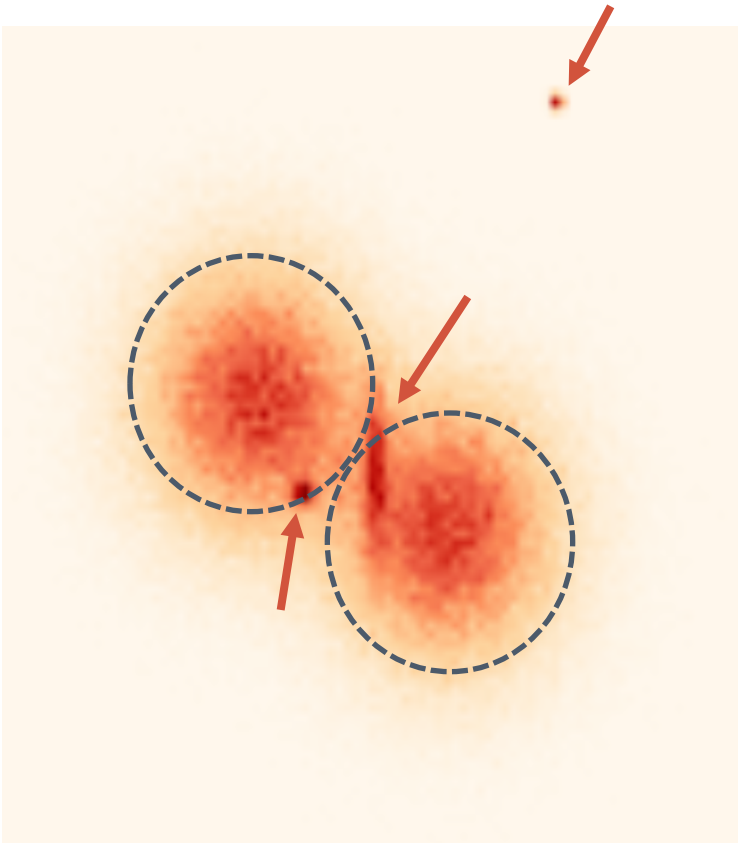
Modeling User Behavior



Modeling normal users and detecting anomalies are two sides of the same coin – understanding user behavior.

Rough model of normal – detect general outliers

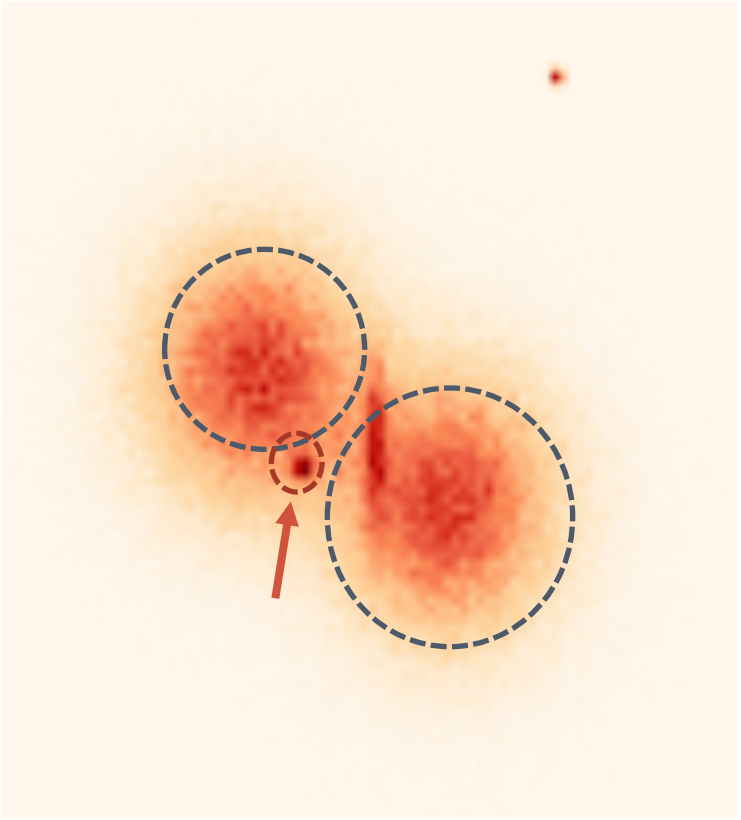
Modeling User Behavior



Modeling normal users and detecting anomalies are two sides of the same coin – understanding user behavior.

More fine grained model of normal can find more subtle outliers

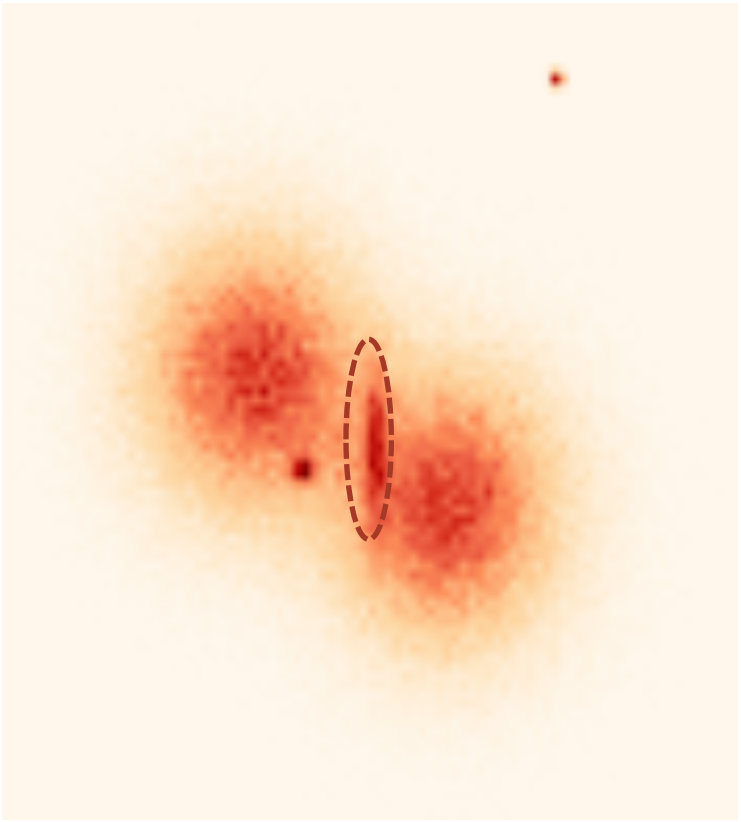
Modeling User Behavior



Modeling normal users and detecting anomalies are two sides of the same coin – understanding user behavior.

More complex model can capture both normal and abnormal patterns – micro-clusters with small variance are particularly suspicious

Modeling User Behavior



Modeling normal users and detecting anomalies are two sides of the same coin – understanding user behavior.

Sometimes domain experts know a specific pattern is fraudulent, and we can search for exactly that pattern.

THREE MAIN TECHNIQUES

1. Local Subgraph Analysis: Patterns and Features

2. Global: Propagation Methods

3. Global: Latent Factor Models and Spectral Methods

FOR ALL THREE PARTS

a) Background

b) Normal

c) Abnormal