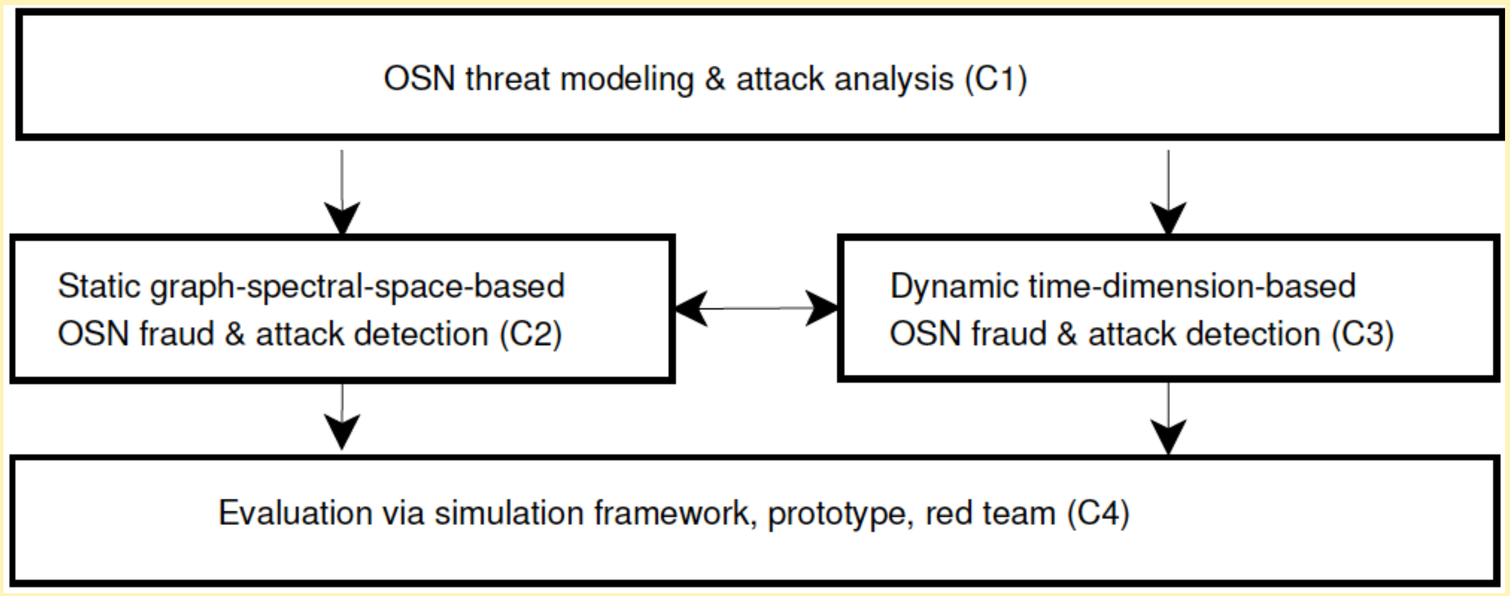
OSN Fraud and Attack Research and Identification

Jun Li, Univ. of Oregon; Xintao Wu, Univ. of Arkansas; Aidong Lu, UNC Charlotte
http://ccsp.uoregon.edu

Online Social Network (OSN) participants face various forms of fraud and attacks.

This research will:

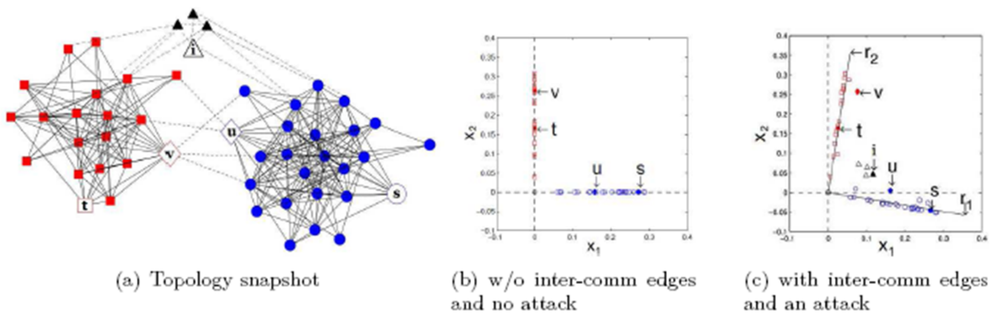
- embrace a systematic, comprehensive study of OSN fraud and attacks
- model, analyze, and characterize OSN fraud and attacks
- design, develop, and evaluate a new approach to detecting OSN collusive fraud and attacks in the graph spectral space
- enhance this approach to handle dynamic attacks with multiple phases



Approach

- Characterize attacks in graph space
- Evaluate state-of-the-art fraud analysis and defense approaches
- Develop a spectral-analysis-based static attack detection approach in complex networks
- Develop a spectral-analysis-based dynamic attack detection approach using network dynamics and vector autoregressive models
- Develop interactive approaches to detecting dynamic attacks
- Build a simulation framework and employ a red team for evaluation

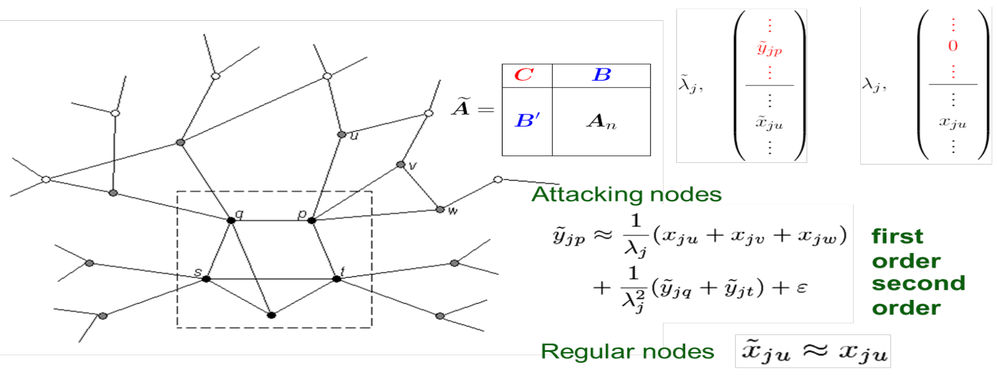
Illustrative example of spectral projection



(a) Topology snapshot (b) w/o inter-comm edges and no attack (c) with inter-comm edges and an attack

Fig. 2. Detecting random link attack in 2-D spectral space.

Spectral perturbation



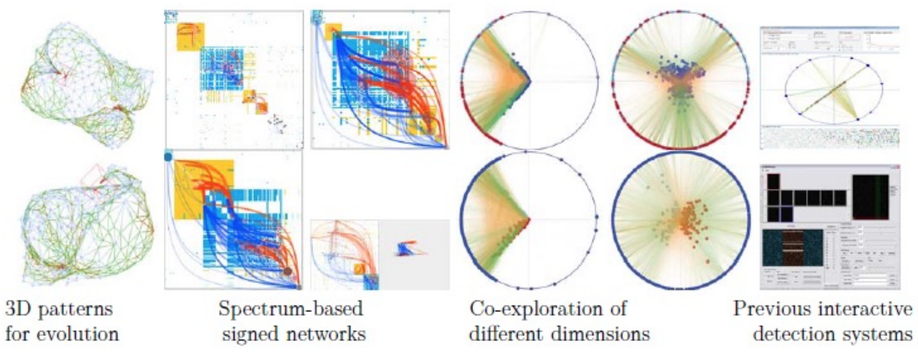
Evaluation on Web spam challenge data

Table 2: Evaluation results on Web Spam data set, 8 RLA attacking groups, 650 total attackers, and 56144 total victims.

RLA	setting size	setting $\bar{v}_i$ p_{in}	SPCTRA ssp	SPCTRA atck	GREEDY ssp	GREEDY atck
1	50	100 .3	50	50	49	47
2	50	100 .6	50	50	0	0
3	50	100 1	50	50	50	50
4	50	200 .3	50	50	79	47
5	100	100 .3	100	100	3	3
6	50	degree	49	49	20	20
7	100	degree	97	97	6	6
8	200	degree	188	188	27	27
final results (total)			634	634	4534	200

Much faster:
36s vs. 26h

Visual detection



3D patterns for evolution | Spectrum-based signed networks | Co-exploration of different dimensions | Previous interactive detection systems

Fig. 3. Our preliminary work on spectrum-based network visualization and visual analytics provides a strong foundation for the proposed research. The examples from left to right show three sets of visual patterns related to the spectral spaces for revealing different attack characteristics. The last column demonstrates two of our previous visualization systems for supporting various interactive detection tasks.

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9–11, 2017
Arlington, Virginia

National Science Foundation
WHERE DISCOVERIES BEGIN

UNIVERSITY OF OREGON

UNC CHARLOTTE