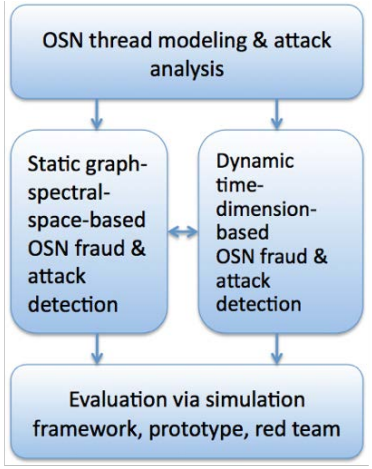
Collaborative: Online Social Network Fraud and Attack Research and Identification

Challenge:

- Ever-evolving OSN fraud and attack space
- OSN data size and complexity
- Few labeled training data
- Little ground truth
- Inefficient interactive attack detection
- Limited research access to OSN platforms



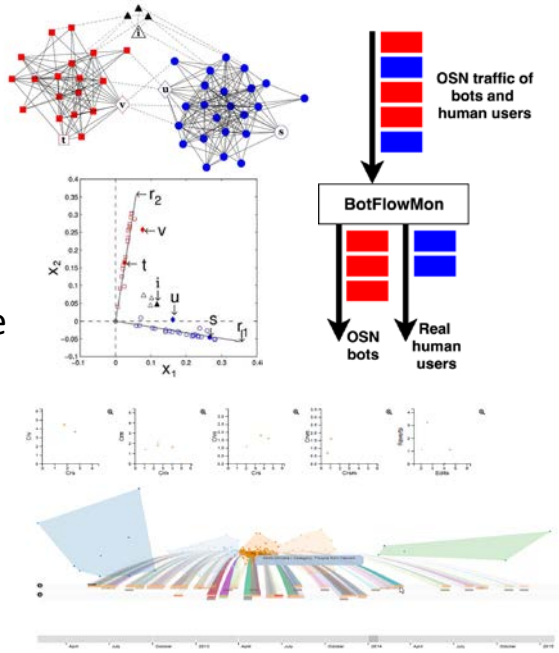
Research components and relationships

Scientific Impact:

- Pushed the state-of-the-art in OSN fraud and attack detection
- Advanced theoretical under-standing of spectral graph analysis
- Advanced the art and techniques of applying machine learning and deep learning to computer security
- Applied visualization for security

Solution:

- Spectrum-based attack detection
- One-class generative adversarial networks for fraud detection
- Neural temporal point processes for dynamic attack detection
- Contrastive learning for fraud detection
- Explainable visualization of collaborative vandal behaviors in Wikipedia
- Learning-based, content-agnostic identification of social bot traffic flows



Broader Impact:

- Less OSN social bot damage
- Better online reviews
- Insights for defense against Wikipedia vandalism and insider threats
- Curriculum development
- Annual Oregon Cyber Security Day
- Involvement of female and undergraduate students

1564348, Univ. of Oregon, Jun Li
1564250, Univ. of Arkansas, Xintao Wu
1564039, UNC Charlotte, Aidong Lu