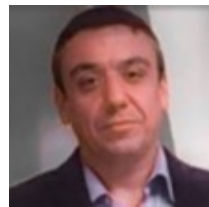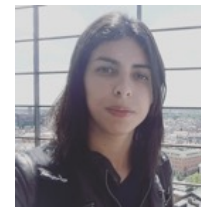# Temporal Graph Mining for Fraud Detection
Part I

Christos Faloutsos
CMU

Pedro Fidalgo
Mobileum

Mirela Cazzolato
USP

Bird's eye view

- Part#1: Introduction – types of fraud
- Part#2: Graphs Mining – patterns and tools
- Part#3: Visualization - conclusions

'Recipe' Structure:

- Problem definition

- Short answer/solution

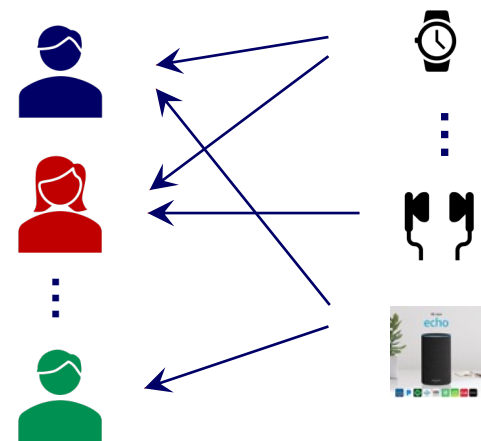- LONG answer – details

- Conclusion/short-answer

Graphs are everywhere!

- E-commerce

- Social networks

- Cyber-security

- Bio-informatics

- …

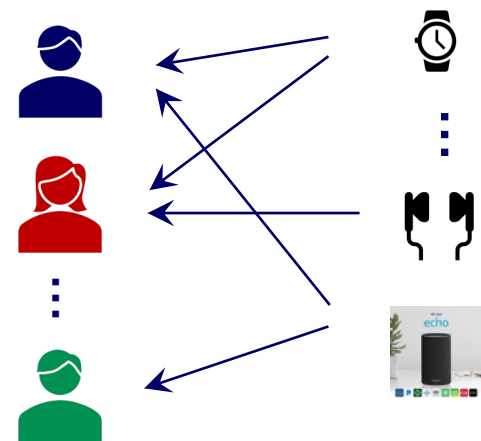# e-commerce examples

Who-buys-what
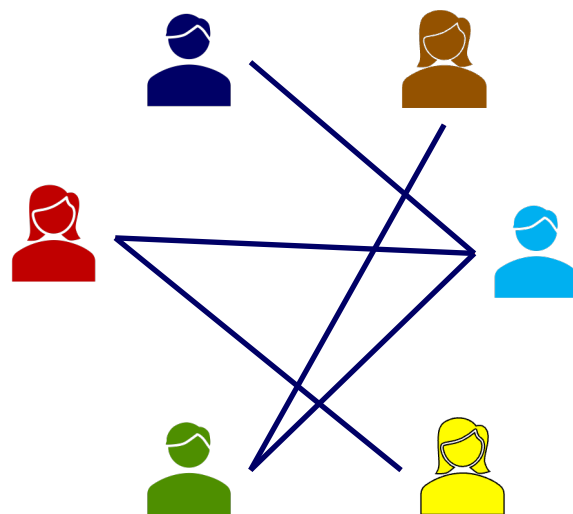
e-commerce examples

Who-buys-what

Who sells what

Who reviews what

Social networks
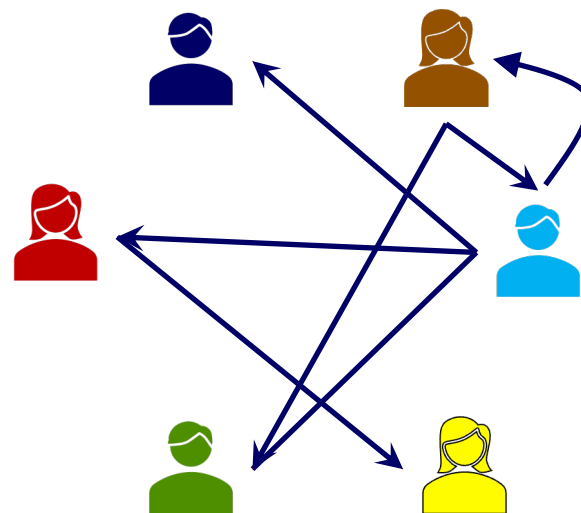
Who-friends-whom
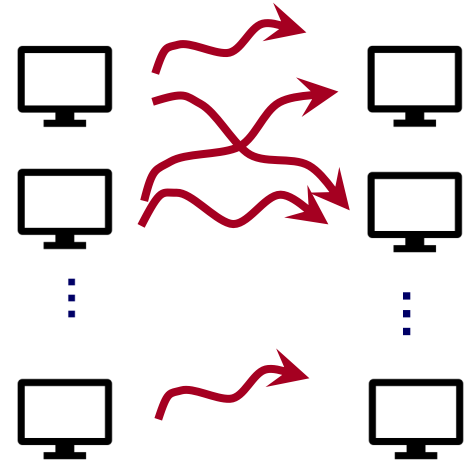
Social networks

Who-friends-whom

Who-follows-whom

Who-retweets-whom

Cyber-security

Who-buys-what ⟵

Who-sells-what

Who-reviews-what

Which_machine - connects_to - what

…

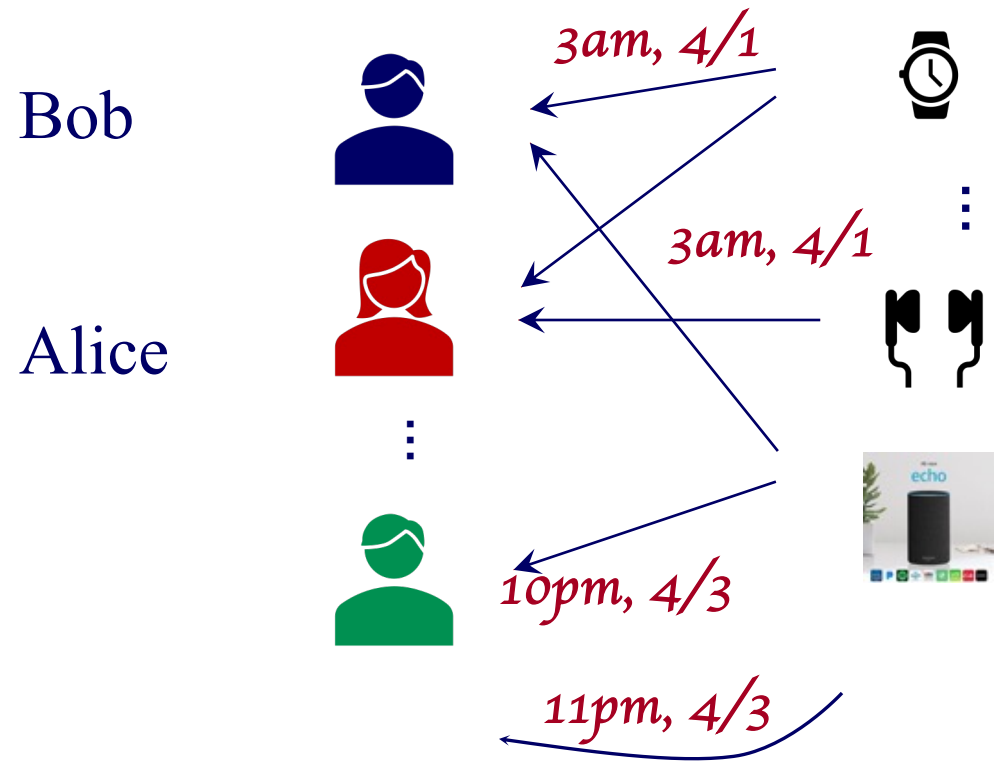\<subject\> related-to \<object\> : graph

Biology/medicine

- Protein-protein interaction networks

- Drugs and side-effects

- Symptoms and disease

Time-evolving graphs

- What is 'normal'? suspicious? Groups?

Bob

Alice

3am, 4/1

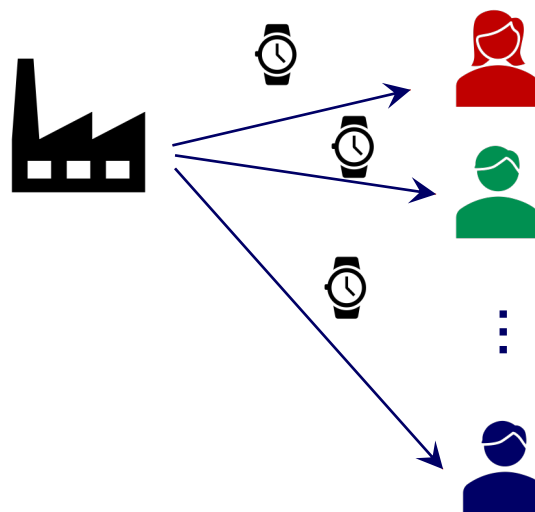3am, 4/1

10pm, 4/3

11pm, 4/3

Bird's eye view

- Part#1: Introduction - motivation
  - Types of fraud
- Part#2: Patterns and tools
  - Static graphs
  - Time evolving graphs
- Part#3: Visualization - Practitioner's guide
- Conclusions

(multiple) types of fraud

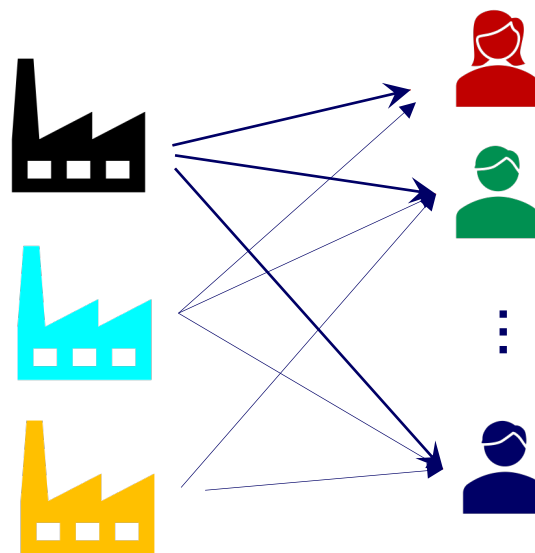- F1) E-commerce
- F2) Social networks
- F3) Phone-call graphs
- …

F1: Fraud in e-commerce

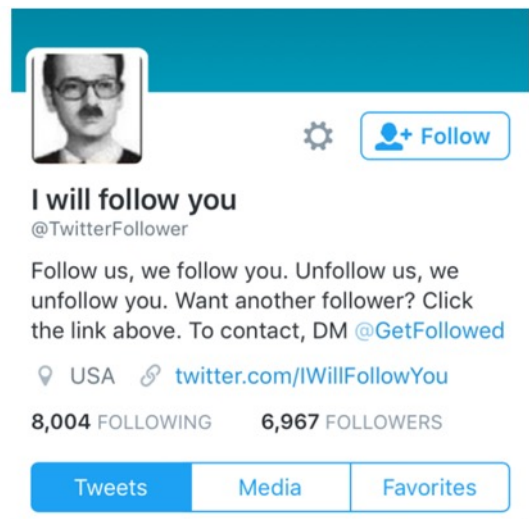- 'brushing' ([Wikipedia](); [WSJ]())
  - Un-wanted packages, to boost 'sales'

F1: Fraud in e-commerce

- 'brushing' ([Wikipedia](); [WSJ]())
  - Un-wanted packages, to boost 'sales'
- Buyer-seller collusion
- …

F2: Fraud in social networks

- Fake twitter followers
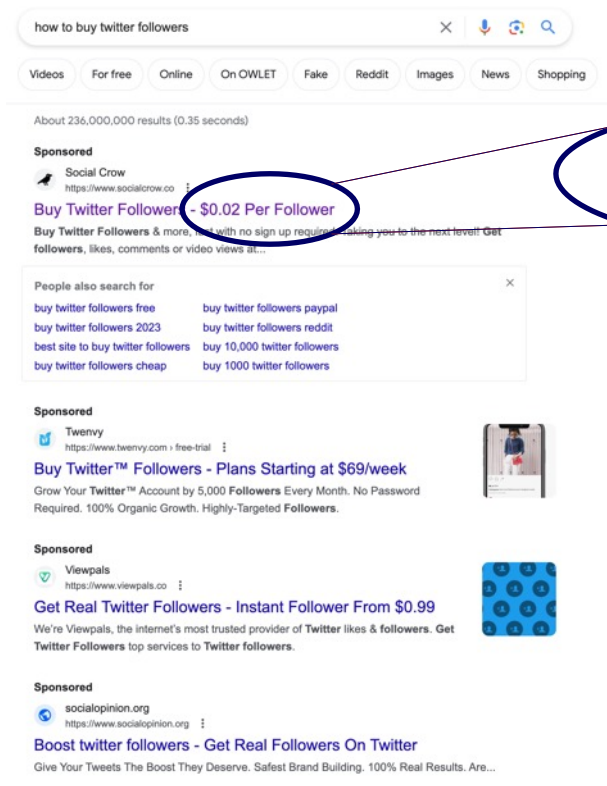
$0.02 Per Follower

FRAUDAR:Bounding Graph Fraud …; **B. Hooi, H.A. Song, A. Beutel, N. Shah, K. Shin, C. Faloutsos, KDD 2016 (best paper)**

F2: Fraud in social networks

"Block"

F2: Fraud in social networks

"Block"

F3) Phonecall graphs

- Telemarketers

- 'wangiri' 'one-ring scam'
  - Europol; AT&T

  1 ring
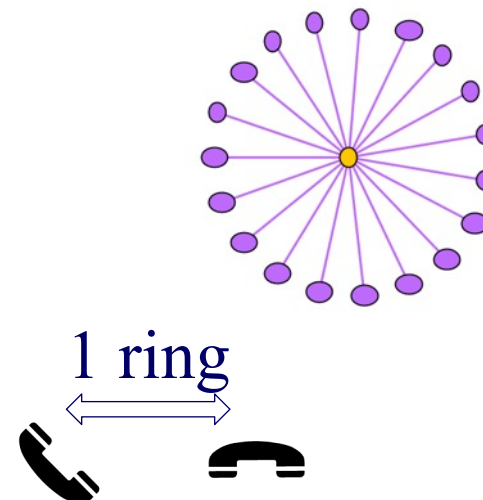
- Telephony Denial of Service (DHS)

. . .
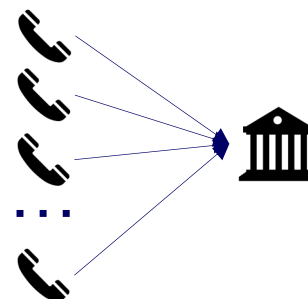
Fraudulent Behavior: *"Know Thy Enemy"*

Indicator signs for some of the fraudulent behaviors. +(/-) means abnormally high(/low).

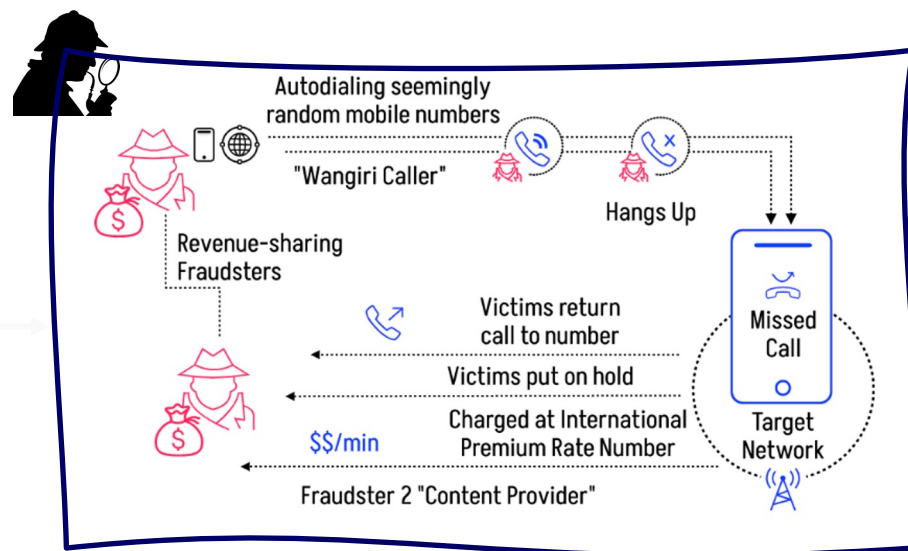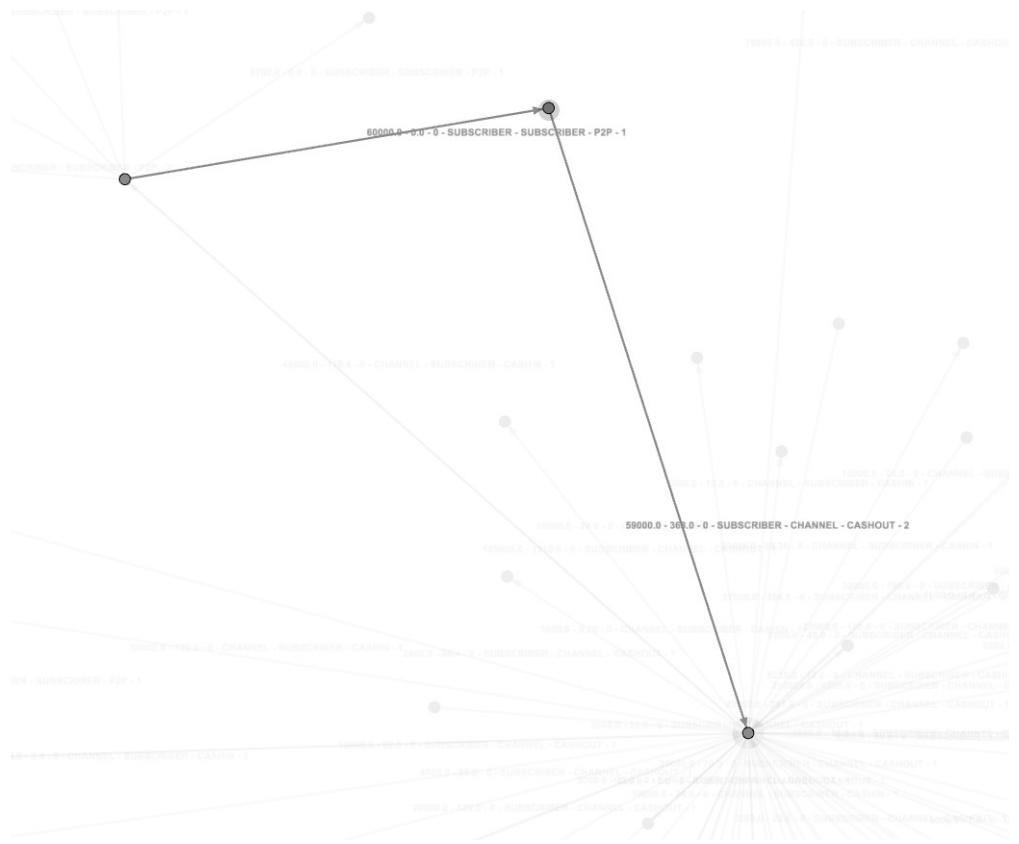|	out-degree	in-degree	in-weighted-deg.	out-weighted-deg.	in-call-count	out-call-count	IAT	density
Fraud Type								
Revenue Share (IRSF)	+	−	−	+		+		
Arbitrage	+	−	−	+		+	−	+
Voice Interconnect Bypass	+		−		−	+	−	+
Fraud Method								
CLI Spoofing	+			+				−
Wangiri	+			+		+		
Robocalling	+	−		+				+

Autodialing seemingly random mobile numbers

"Wangiri Caller"

Hangs Up

Revenue-sharing Fraudsters

Victims return call to number — Missed Call

Victims put on hold

Charged at International Premium Rate Number — Target Network

$$/min

Fraudster 2 "Content Provider"

F4) Money Laundry

F6) Terrorism Networks (9/11)

○ 9/11 organizers and leaders
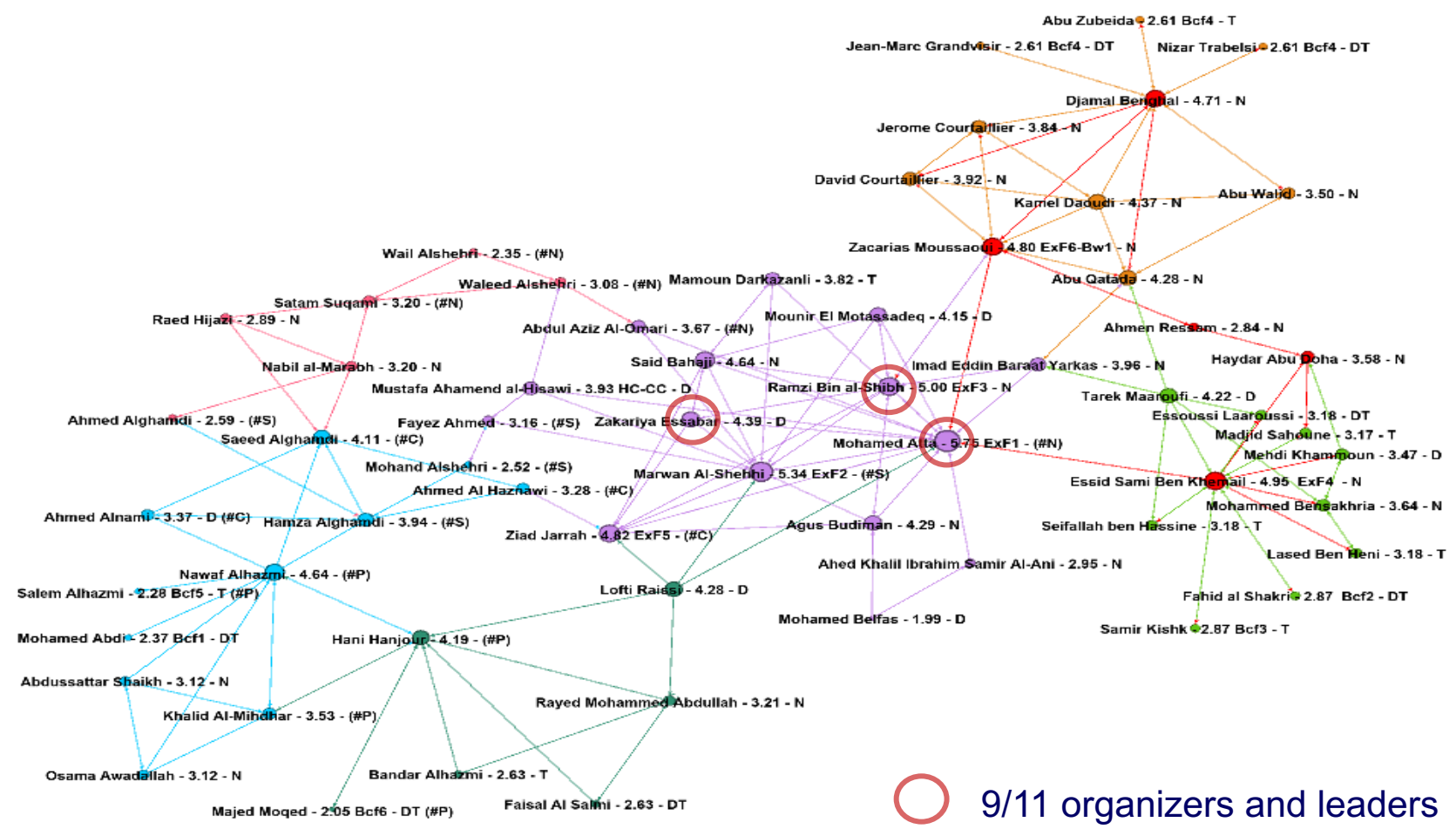
F5) Criminal Associations (BFP)

High centrality: 'lawyers'

Near-clique: 'road warriors'

Faloutsos, Fidalgo, Cazzolato
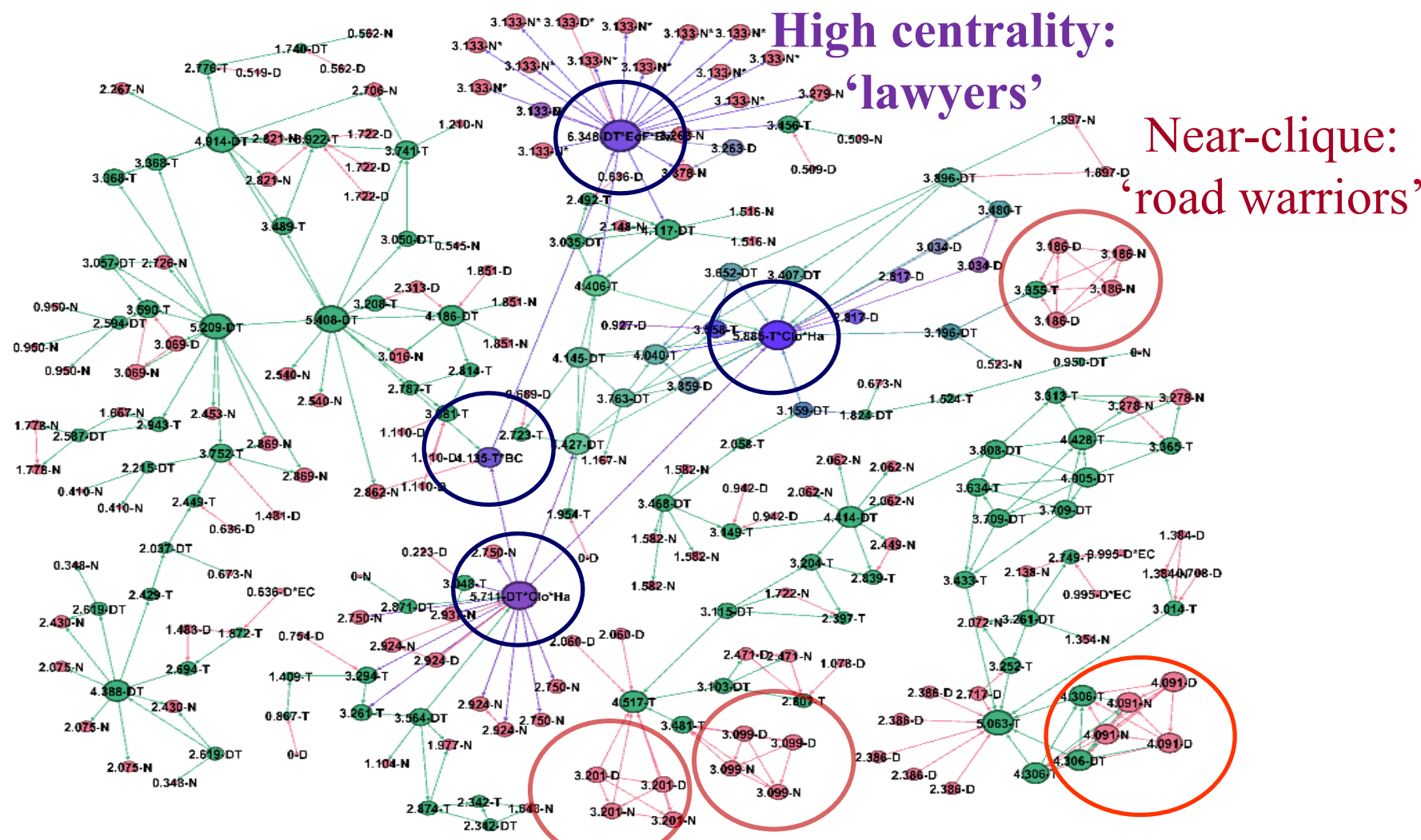
F5) Telecom Fraud (Credit Cards)

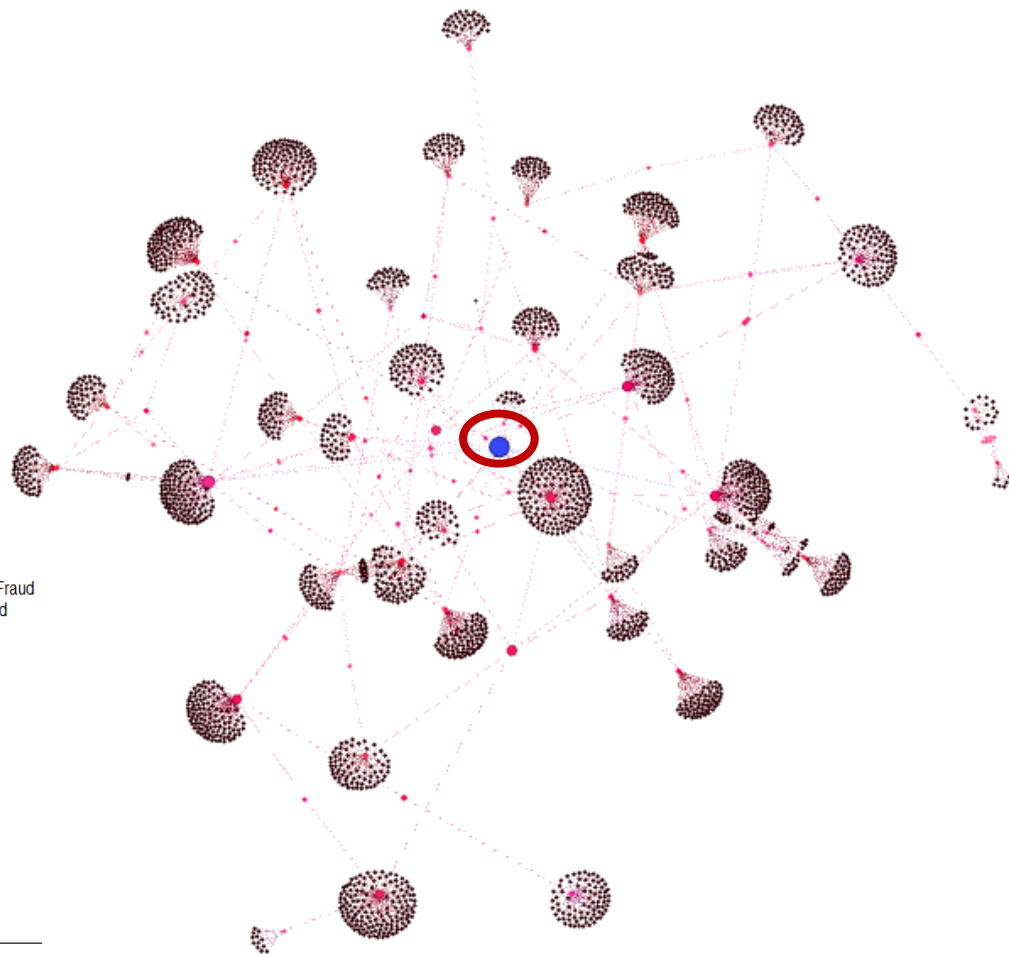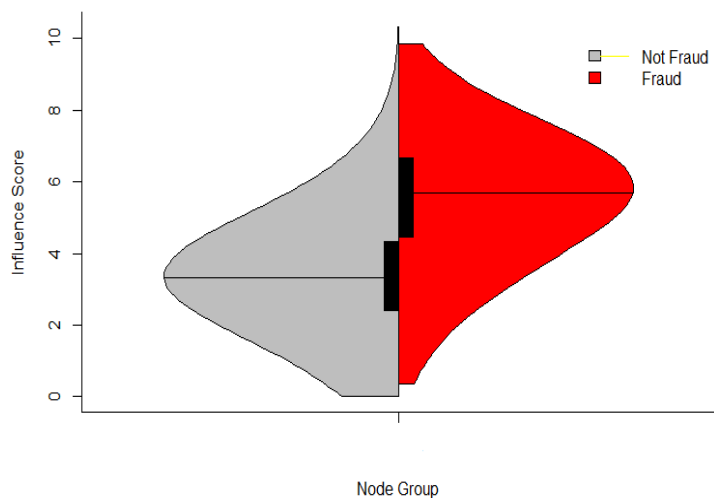➔ Bridge nodes with low degree

➔ Interconnected Hubs

➔ Strategic position

➔ High Influence

➔ Roles in the network (Control)

(multiple) types of fraud

- F1) E-commerce
- F2) Social networks
- F3) Phone-call graphs
- F4) Financial Fraud
- F5) Money Laundering
- …

The Many Faces of Link Fraud, Neil Shah, Hemank Lamba, Alex Beutel, Christos Faloutsos, <u>arxiv</u>