Feasibility Study of Social Network Analysis on Loosely Structured Communication Networks

Jan William Johnsen and Katrin Franke
jan.w.johnsen@ieee.org and kyfranke@ieee.org

Highlights

- Organised criminal groups become more active in the cyber domain, where they form online communities used as marketplaces for illegal material, products and services purchased by other criminals.
- Trading of illegal goods drives an underground economy that facilitates almost any type of cyber crime. The challenge for law enforcement agencies is to know which individuals to focus their efforts on, in order to effectively disrupt the marketplaces.
- Our article study the feasiability of using **social network analysis** on loosely structured communication networks with the goal of identifing central individuals who provide services to cyber criminals.

Case study methodology

- Social network analysis studies social relationships through the use of network graphs. In these graphs, **vertices** are individual actors and **edges** are the relationships between them.
- **Centrality measures** identify important and influential individuals in a network. These measures often differ in their evaluation of vertex importance.

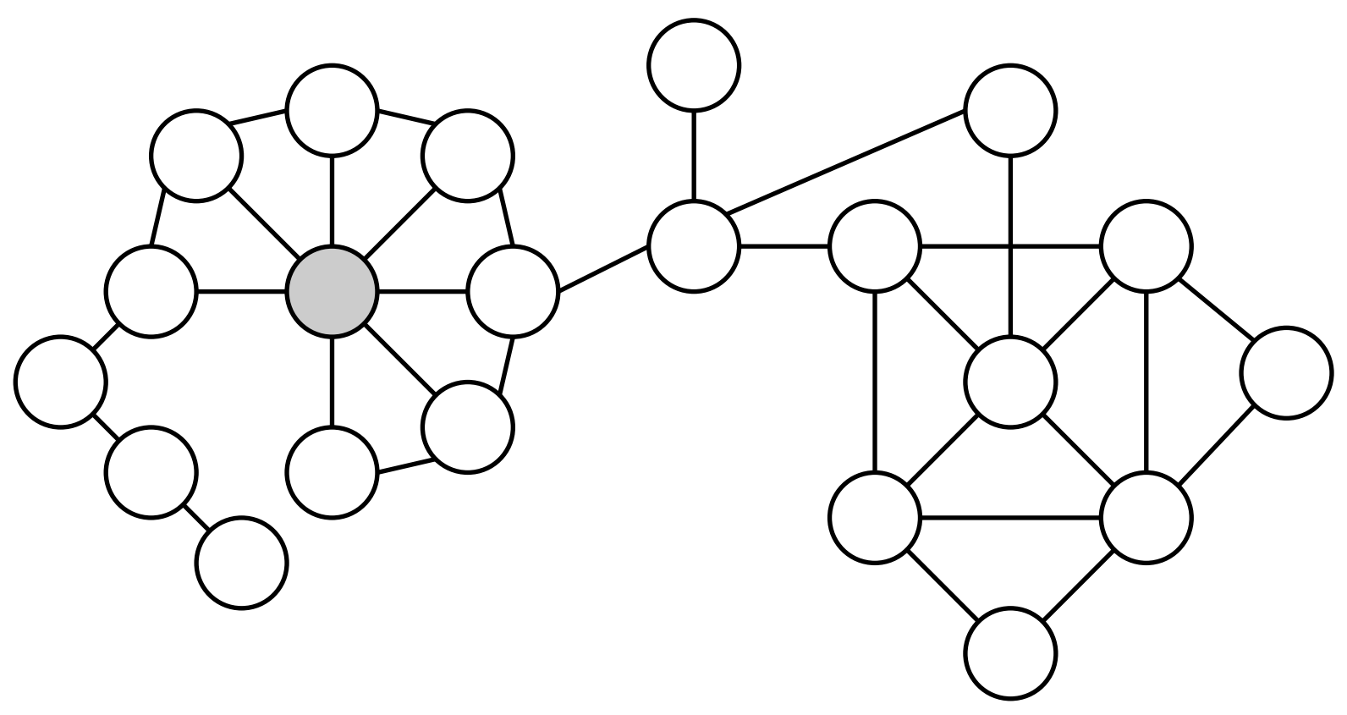

Figure 1: Highlighting largest degree centrality

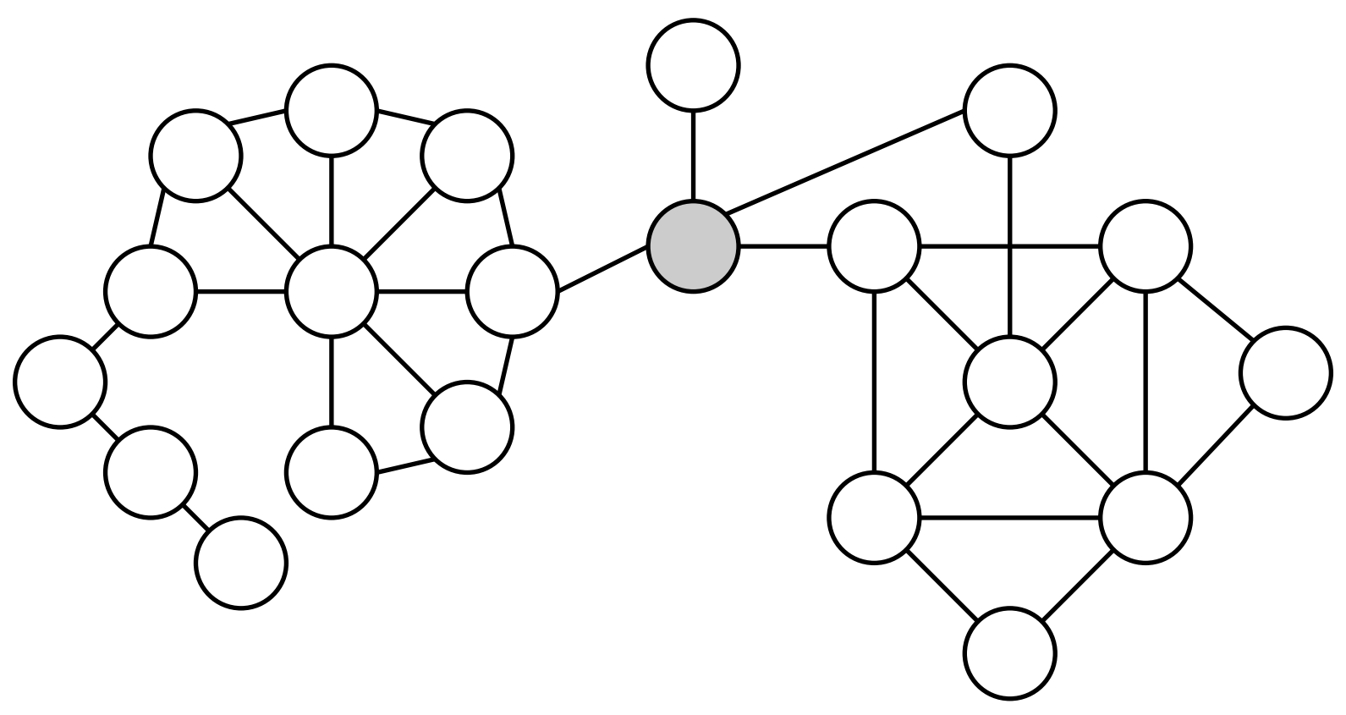

Figure 2: Highlighting largest betweenness centrality

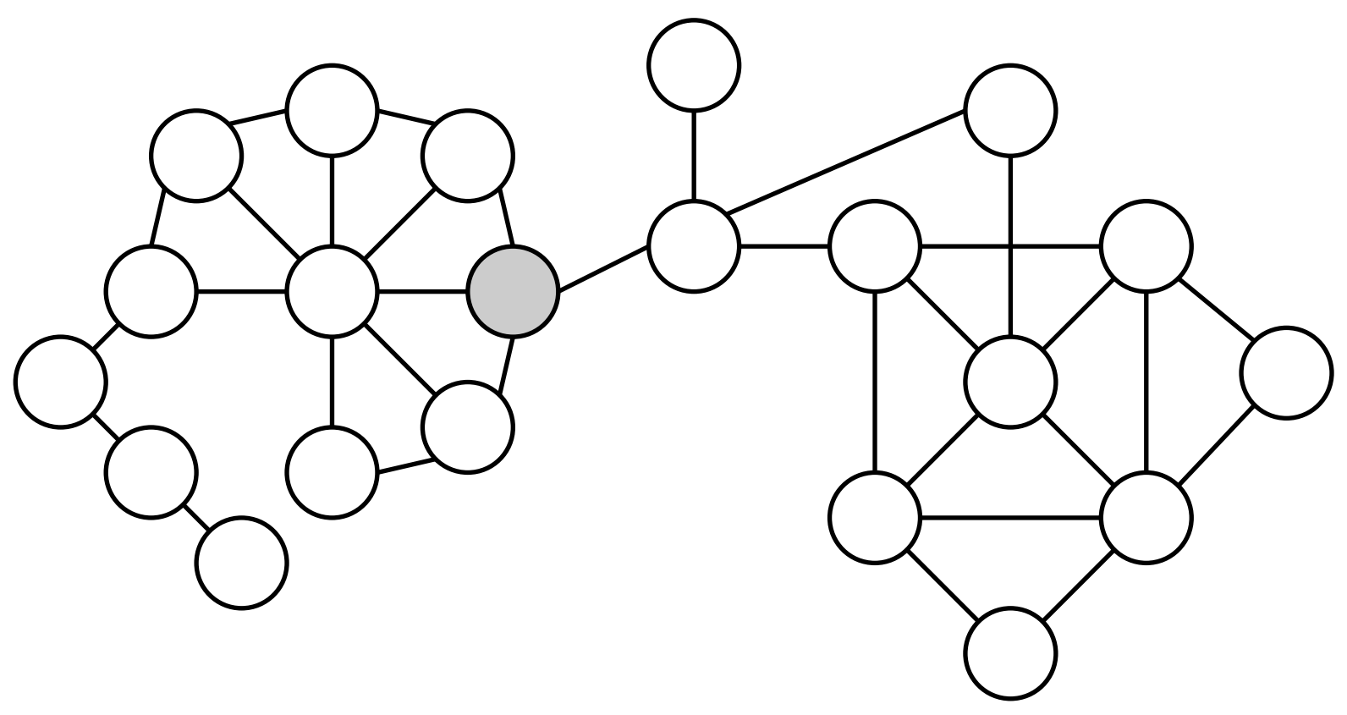

Figure 3: Highlighting largest closeness centrality

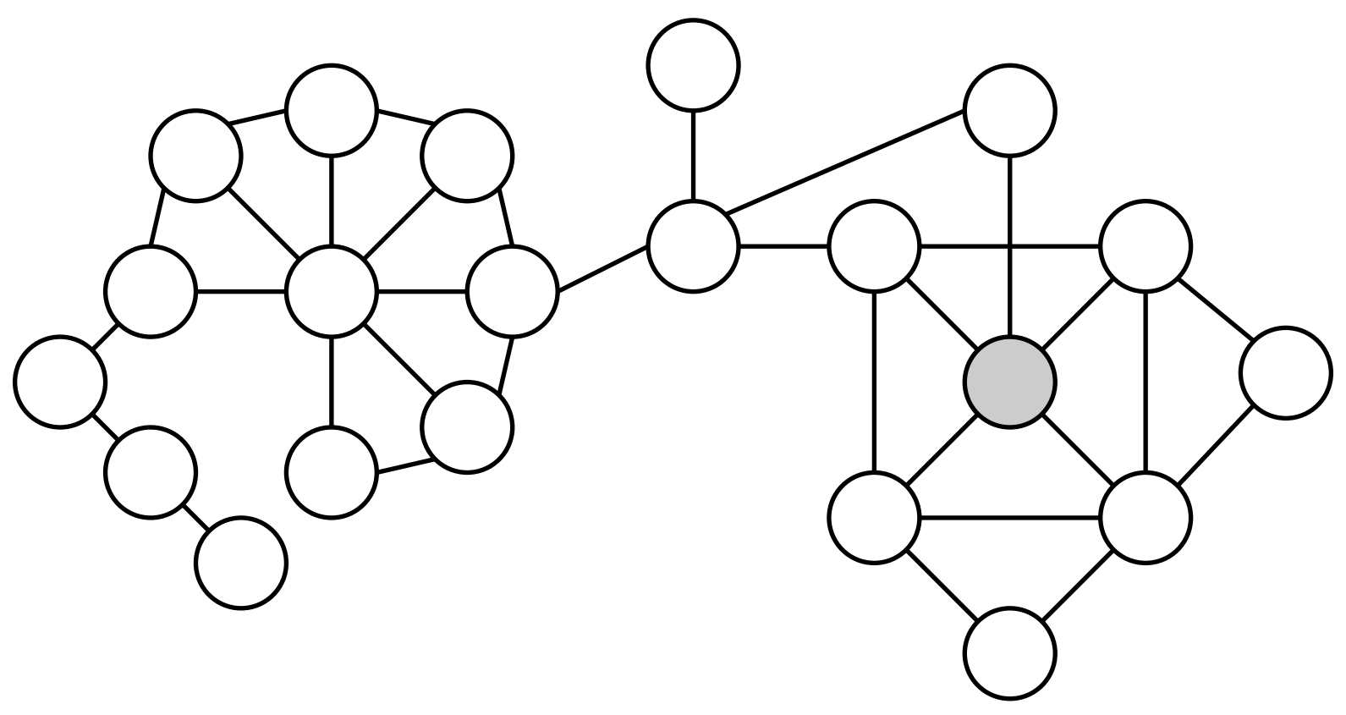

Figure 4: Highlighting largest eigenvector centrality

Case study and novel hacker forum dataset

- A novel dataset from **Nulled.IO** was leaked on 12/05/2017. It is from an online forum for distributing cracked software and leaked credentials.
- The database dump contains details for about 600 000 users, including around 800 000 private and 3.5 million public messages.
- Two networks – modelled by **undirected graphs** – were created to model both private and public communciations.

NULLED IO
EXPECT THE UNEXPECTED

Centrality measures results

Table 1: Top ten public centrality results

ID	Degree	ID	Closeness	ID	Betweenness	ID	Eigenvector
15398	0.31449	15398	0.51280	15398	0.50134	15398	0.47951

Table 2: Top ten private centrality results

ID	Degree	ID	Closeness	ID	Betweenness	ID	Eigenvector
1	0.09466	1	0.37928	1	0.17174	193974	0.48531
15398	0.03441	334	0.35757	15398	0.05871	61078	0.47249
1337	0.03275	1471	0.35631	1337	0.04811	51349	0.29031
1471	0.03194	1337	0.35437	1471	0.04593	315929	0.24046
51349	0.03074	51349	0.35118	334	0.03985	336307	0.16937
8	0.02776	88918	0.35101	8	0.03918	10019	0.15016
334	0.02738	448198	0.35042	51349	0.03436	88918	0.13975
88918	0.02580	3507	0.34918	88918	0.03223	157899	0.10703
3507	0.02325	8	0.34864	3507	0.02946	1	0.10647
448198	0.02116	15398	0.34624	448198	0.02833	3507	0.10156

Network visualisation

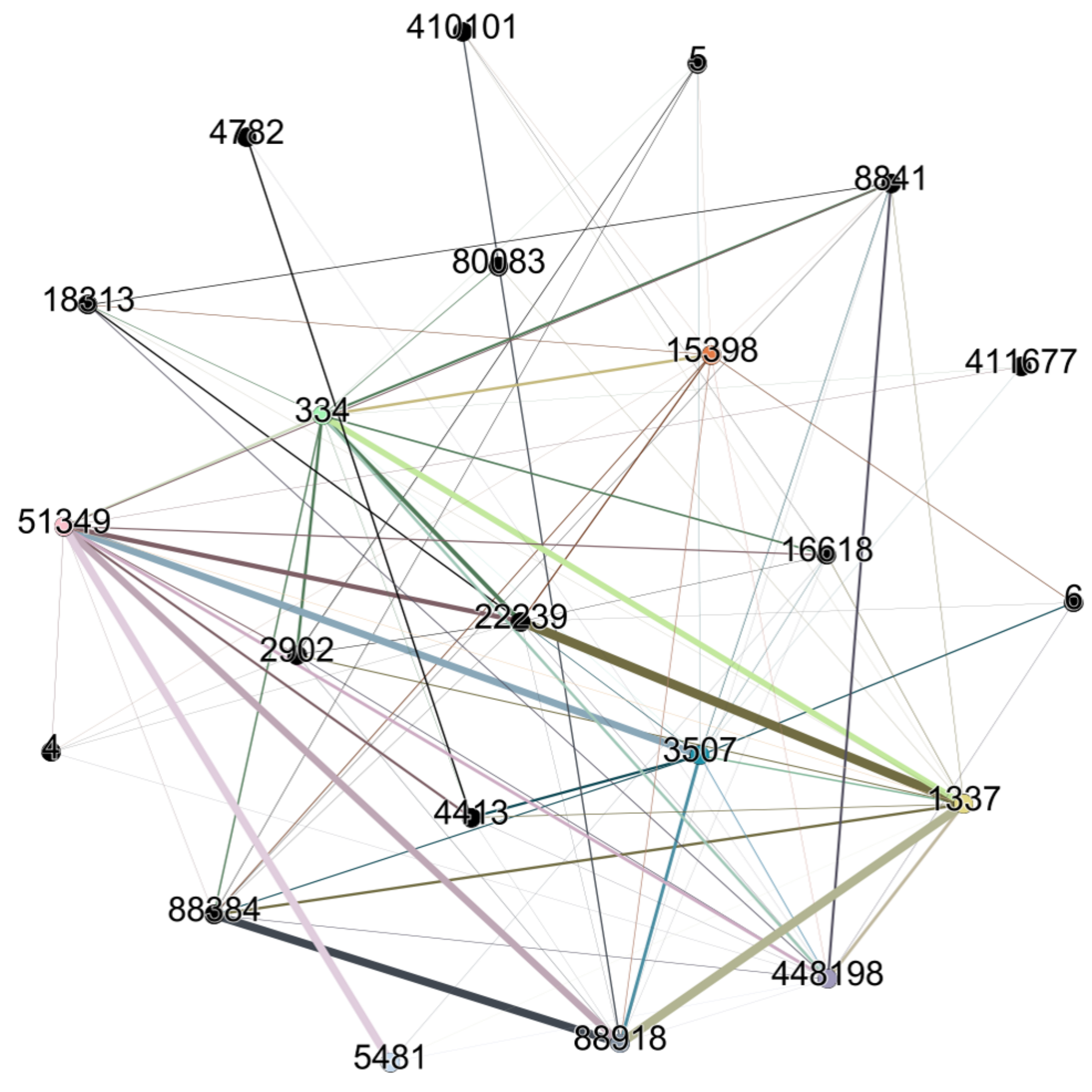

Figure 5: Public threads

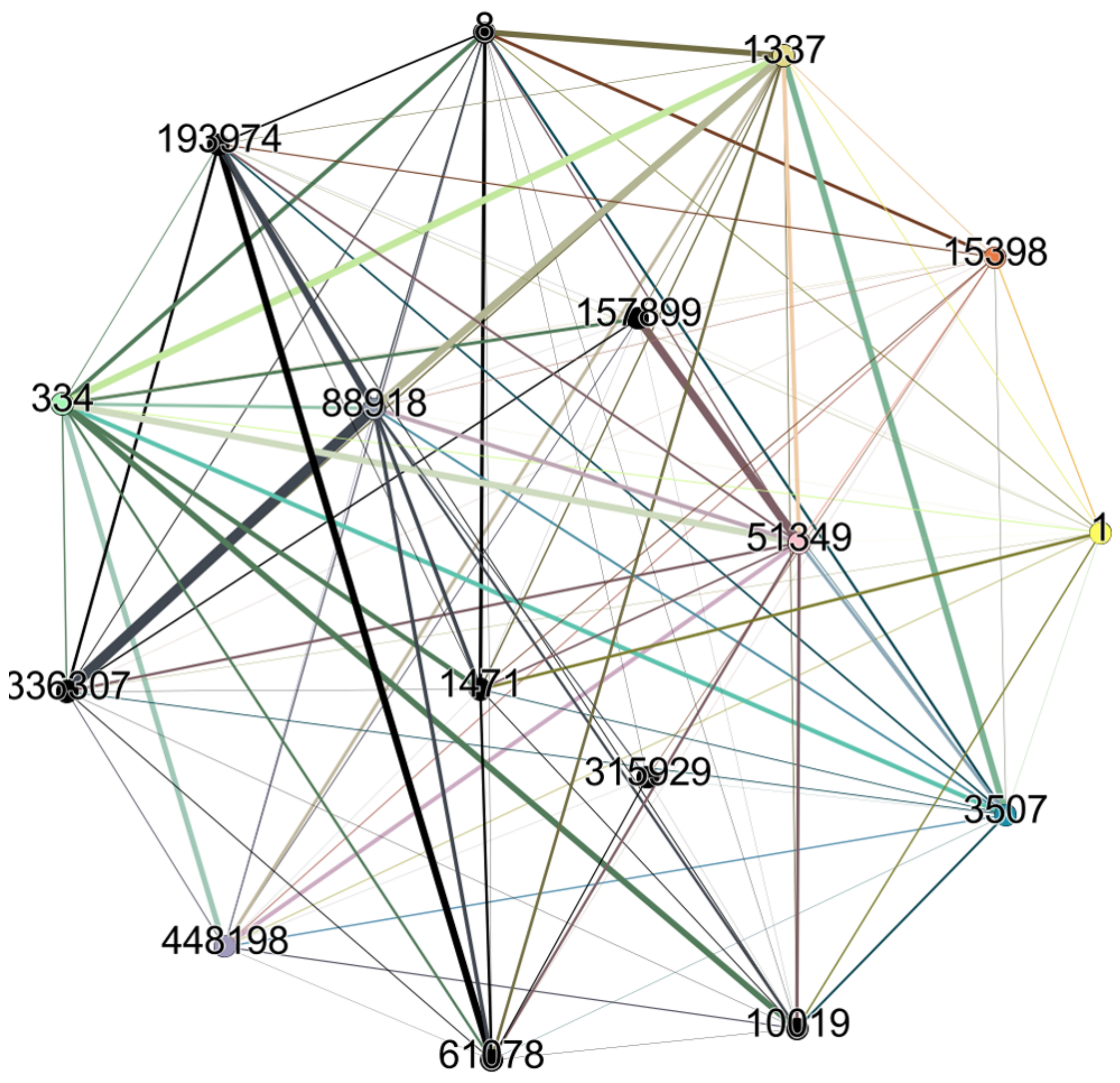

Figure 6: Private messages

Summary

- Centrality measures ranked administrators as more important than cyber criminals who provide illegal services to others. Focusing on disrupting server administrators is an inefficient approach addressing this problem, as their removal represents only a temporarily setback for prolific cyber criminal networks.

theguardian

Life after Silk Road: how the darknet drugs market is booming

NTNU
Norwegian University of
Science and Technology