Analyzing Spammers' Social Networks for Fun and Profit

A Case Study of Cyber Criminal Ecosystem on Twitter

Authors:

Chao Yang, Texas A&M University

Robert Harkreader, Texas A&M University

Jialong Zhang, Texas A&M University

WWW-12

Presented By:
Muhammad Saad

UCF

Outline

- **Criminal accounts on Twitter**
- **Cyber criminal ecosystem**
- **Inner social relationship of criminal accounts**
  - Graph density
  - Reciprocity
  - Following quality
  - Criminal leaves and hubs
  - Criminal following ratio
  - Shared following ratio
- **Outer social relationship**
  - Criminal supporters
  - Mr.SPA algorithm
  - Social butterflies
  - Social promoters
  - Dummies

Outline

- **Inferring criminal accounts**
  - CIA algorithm
  - Evaluation and results
  - Limitations of work
- **Conclusion and discussion**

Criminal Accounts

- **Behavior**

  a) Send spam in tweets
  b) Malicious urls
  c) Phishing

- **Twitter policy**

  a) Blocks spam accounts
  b) If account has few followers and follows many accounts

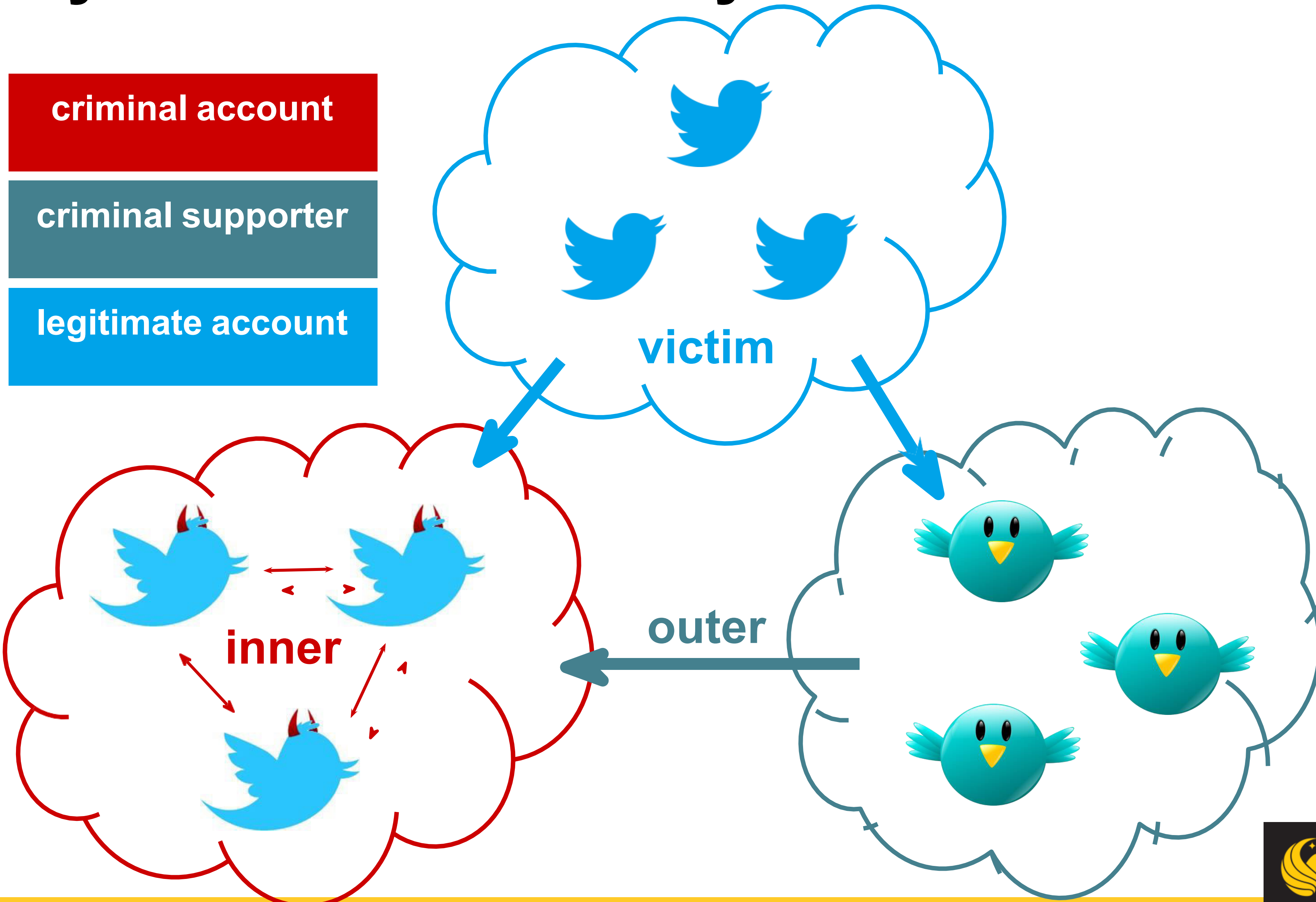
- **Problem**

  a) Criminal accounts still exist
  b) Evade policies of Twitter
  c) Blend in the normal accounts

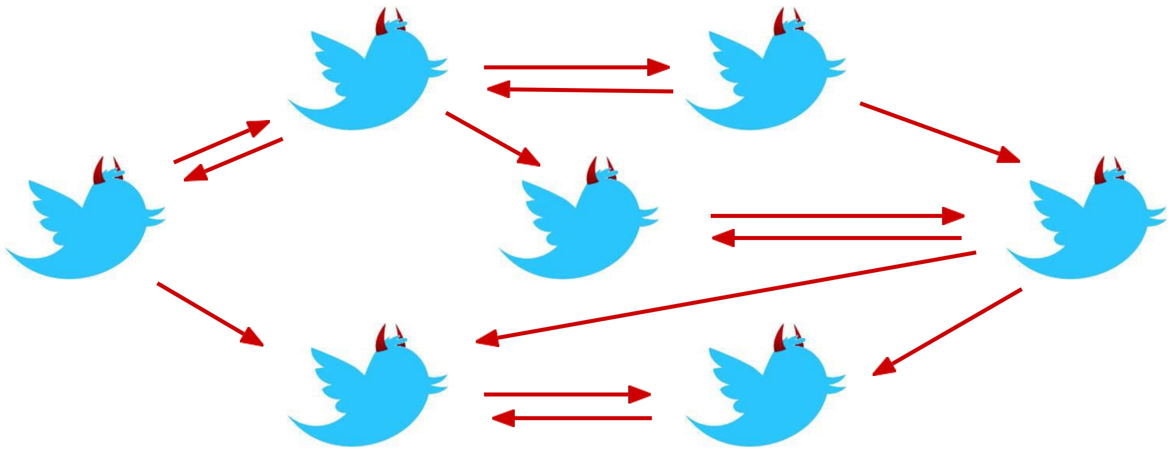
Objectives

- Understand how criminal accounts survive
- Identify their ecosystem
- Understand characteristics
- Study their distribution
- Develop huristic models to spot criminal accounts
- Present countermeasures

Cyber Criminal Ecosystem



Inner Social Relationship

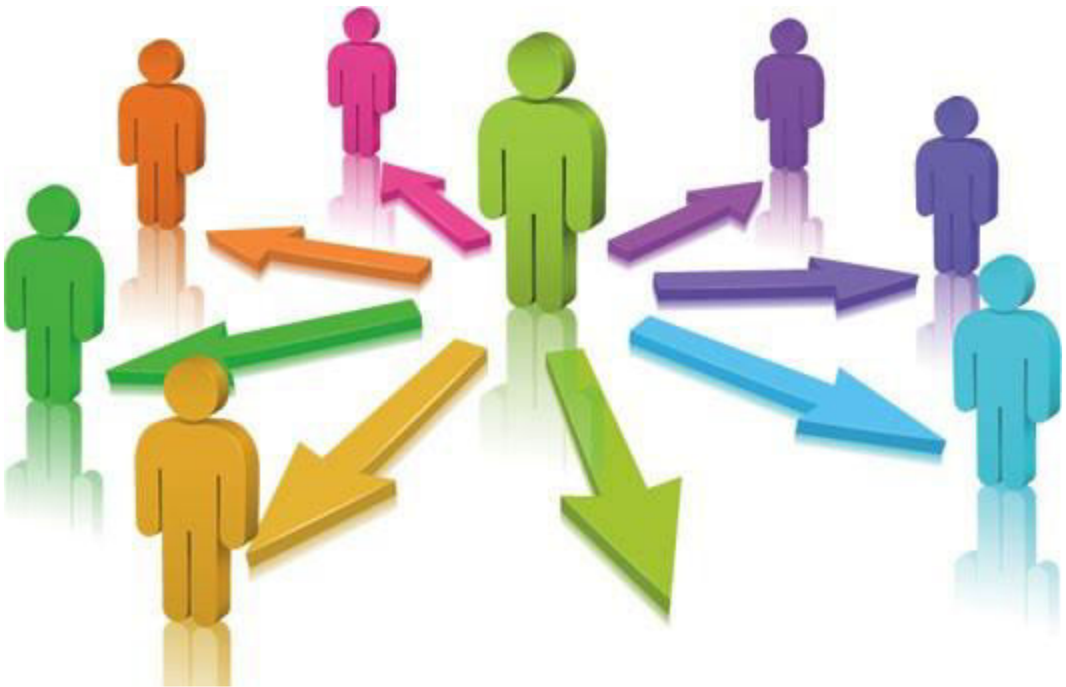


G = (V,E)

V: all criminal accounts
E: all follow relationship, directed edge

Inner Social Relationship

Finding 1:
Criminal accounts tend to be socially connected, forming a small-world network.



Inner Social Relationship

Graph Density

$$\frac{|E|}{|V| \times (|V| - 1)}$$

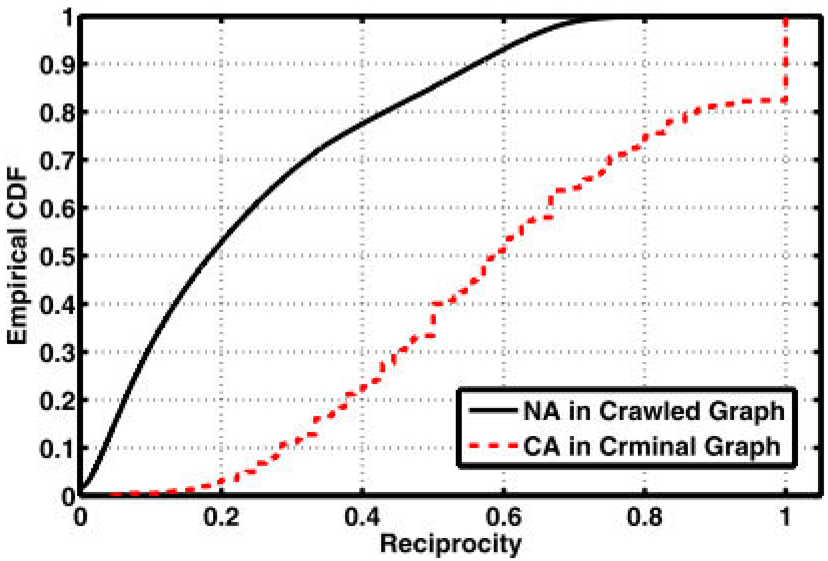
	Account	Follow Relationship	Density
Criminal Space in Sample	**2,060**	**9,868**	**2.33×10^{-3}**
Entire Twitter Space	**41.7×10^{6}**	**1.47×10^{9}**	**8.45×10^{-7}**

UCF

Inner Social Relationship

Reciprocity

Number of Bidirectional Links



Reciprocity of **95%** criminal accounts higher than 0.2.

Reciprocity of **55%** normal accounts higher than 0.2.

Reciprocity of around **20%** criminal accounts are nearly 1.0.

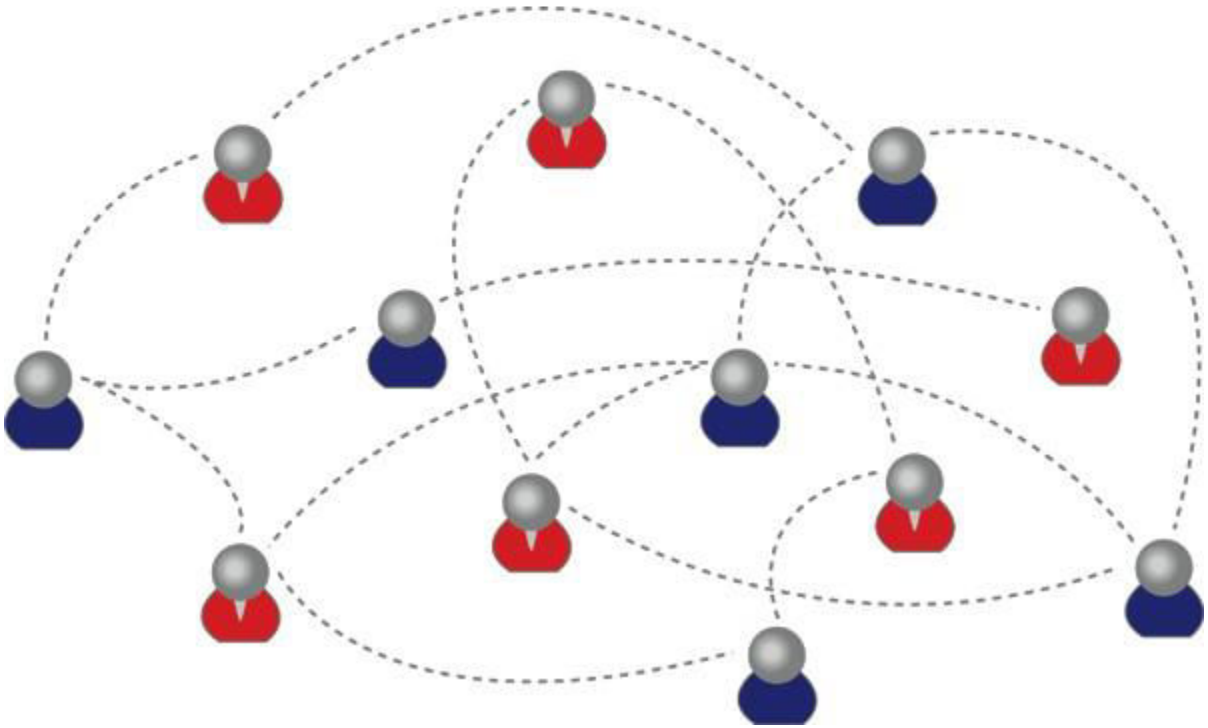
Inner Social Relationship

Average Shortest Path Length

Average number of steps along the shortest paths for all possible pairs of graph nodes.

	ASPL
Criminal Accounts	**2.60**
Legitimate Accounts	**4.12**

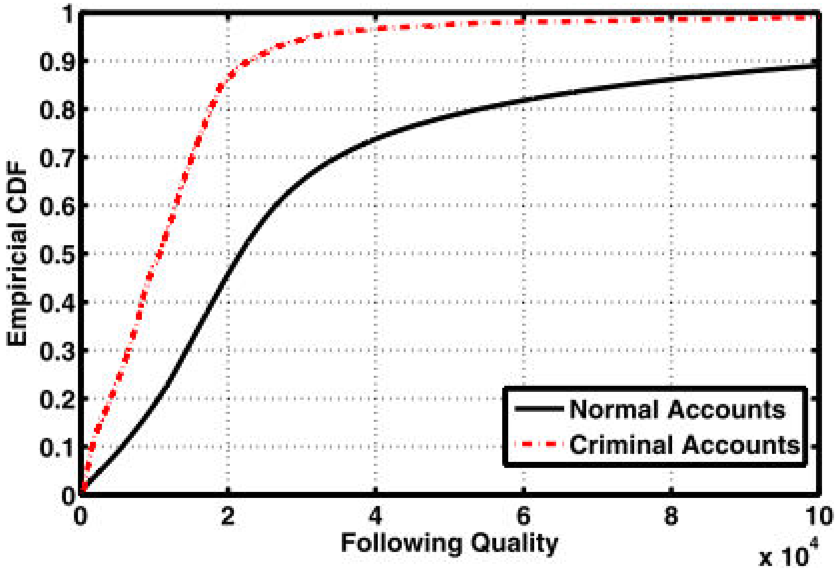
Inner Social Relationship



Criminal accounts have strong social connections with each other.
REASON?

Inner Social Relationship

Tend to follow many accounts without considering those accounts' quality much.



FQ of **85%** criminal accounts lower than 20,000.

FQ of **45%** normal accounts lower than 20,000.

Inner Social Relationship

Criminal accounts, belonging to the same criminal organizations.

Inner Social Relationship

Criminal accounts, belonging to the same criminal organizations.

Group criminal accounts into different criminal campaigns by **malicious URL**.

↓

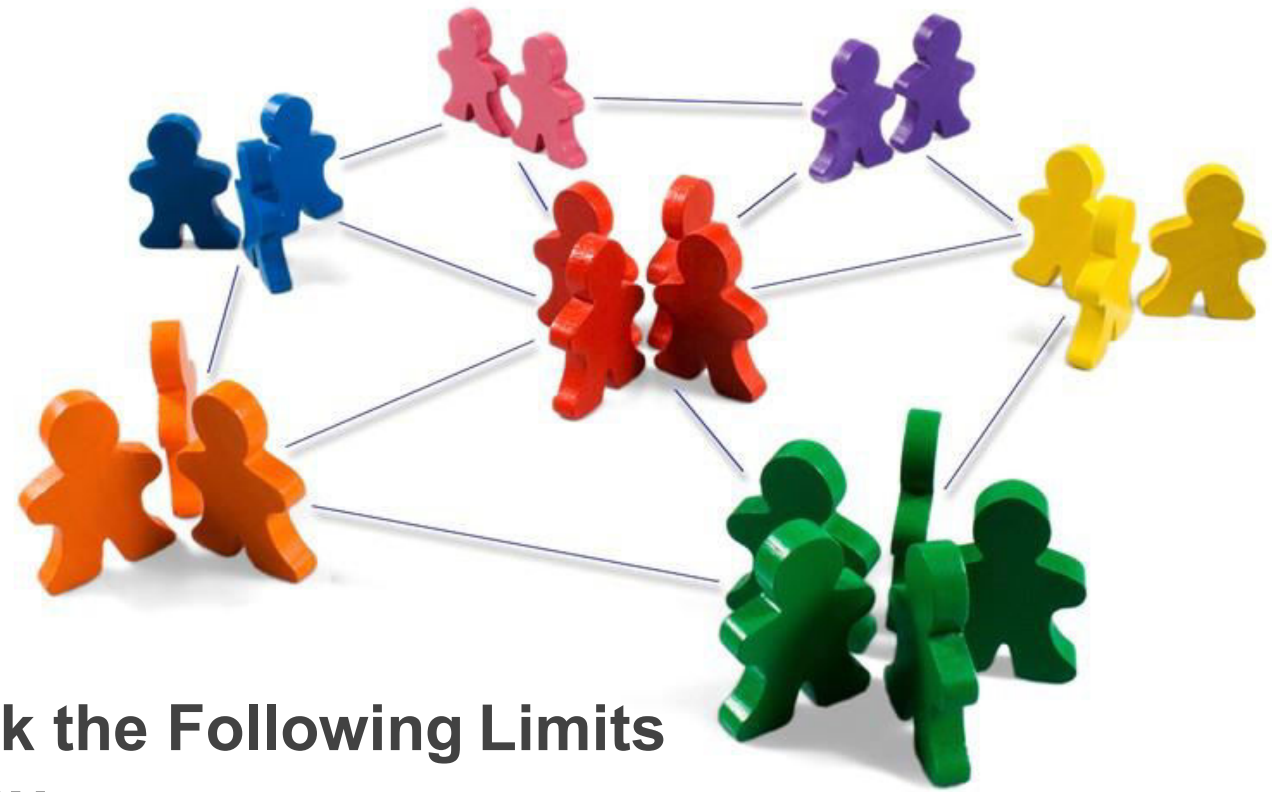
17 campaigns

↓

8,667 edges → **87.8 %**

Inner Social Relationship

Provide followers to criminal accounts



1. Break the Following Limits Policy

2. Evade spam detection

Inner Social Relationship

criminal hubs

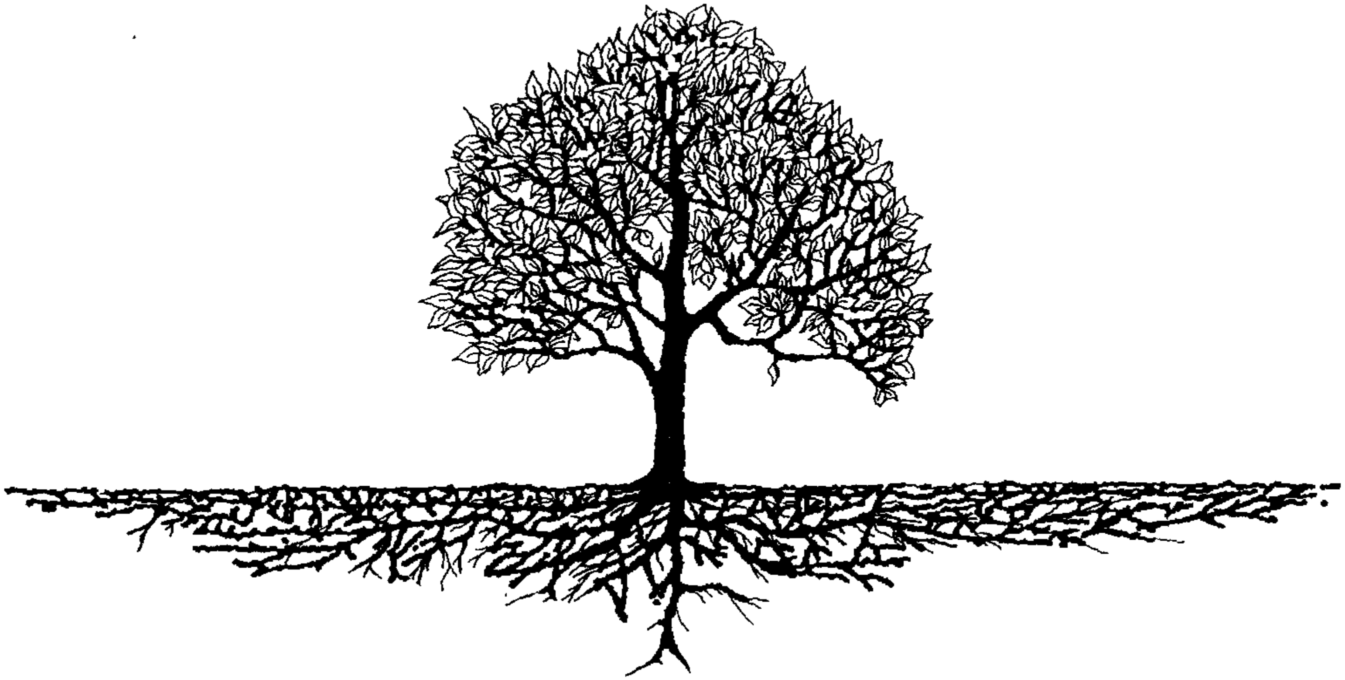
following leaves and acquiring their followers' information

criminal leaves

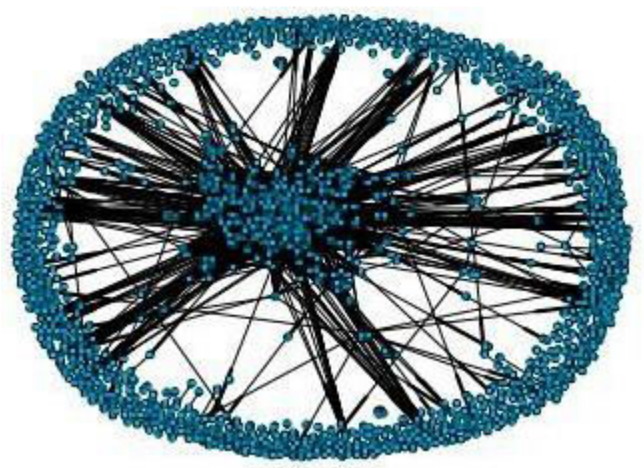
randomly following other accounts to expect them to follow back

Inner Social Relationship

Finding 2:
Compared with criminal leaves, criminal hubs are more inclined to follow criminal accounts.



Inner Social Relationship



Relationship Graph

HITS algorithm to calculate hub score

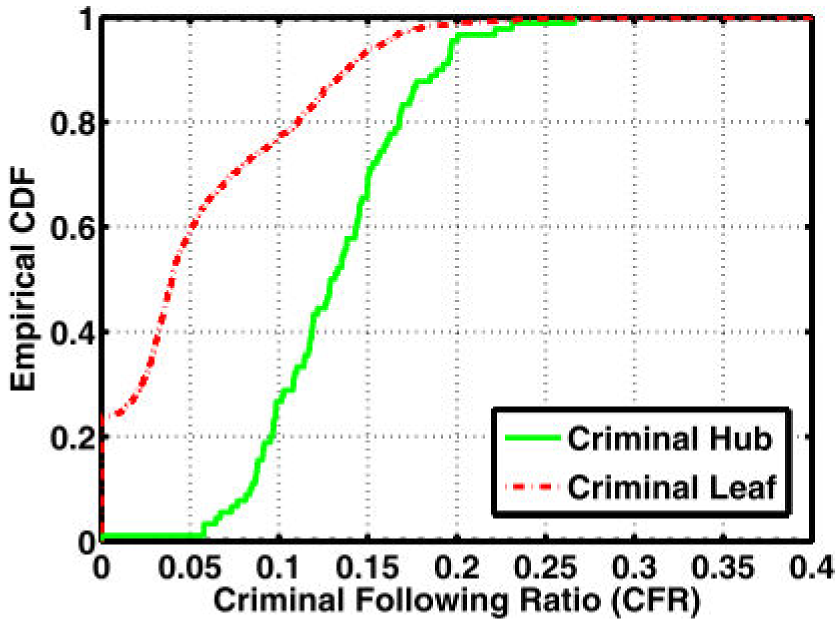
↓

k-means algorithm to cluster them

↓

criminal hubs: **90**
criminal leaf: **1,970**

Inner Social Relationship

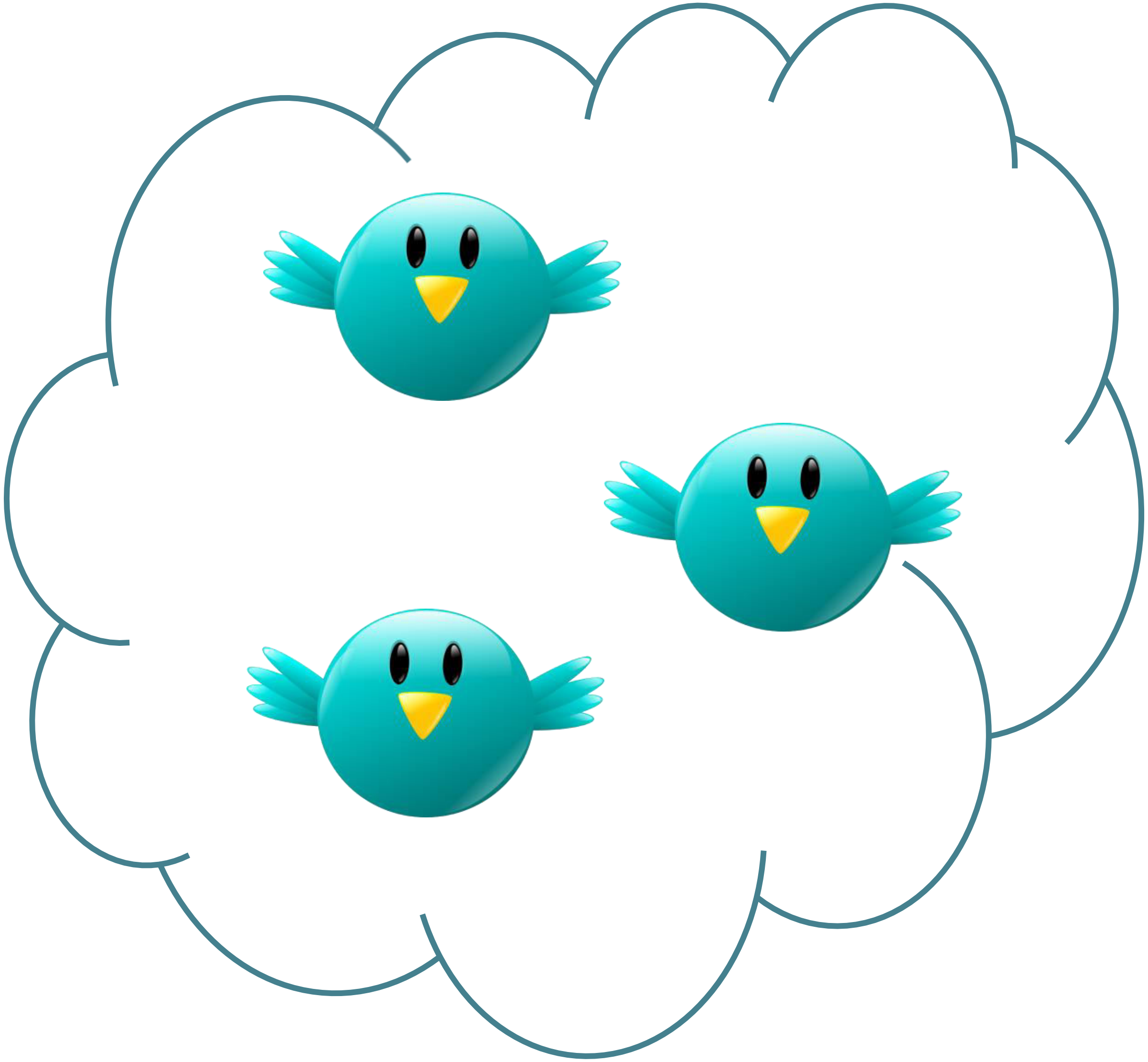


CRF of **80%** criminal hubs higher than 0.1.

CRF of **20%** criminal leaves higher than 0.1.

CRF of **60%** criminal leaves lower than 0.05.

Outer Social Relationship



Outer Social Relationship

criminal supporters

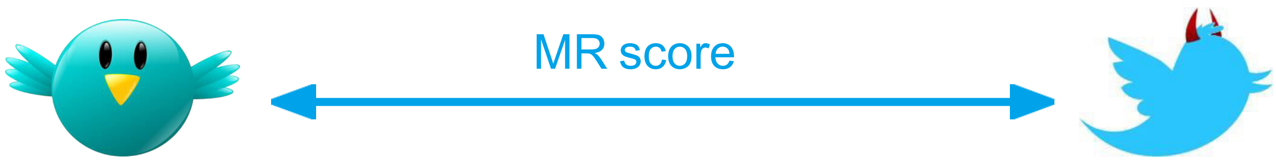
accounts outside the criminal community, who have close "follow relationships" with criminal accounts

Outer Social Relationship

Malicious Relevance Score Propagation Algorithm (Mr.SPA)

MR score:

measuring how closely this account follows criminal accounts



Outer Social Relationship

Malicious Relevance Score Propagation Algorithm (Mr.SPA)

1. the **more** criminal accounts followed, the **higher** score

2. the **further** away from a criminal account, the **lower** score

3. the **closer** the support relationship between a Twitter account and a criminal account, the **higher** score

UCF

Outer Social Relationship

Malicious Relevance Score Propagation Algorithm (Mr.SPA)

Malicious Relevance Graph, G=(V,E,W)

V: all accounts
E: all follow relationship, directed edge W: weight for each edge, closeness of relationship

$$W(i, j) = \frac{1}{indegree(j)}$$

Outer Social Relationship

After Mr. SPA...

use **x-means algorithm** to cluster accounts based on their MR scores

most accounts have relatively small scores and are grouped into one single cluster

most accounts do not have very close follow relationships with criminal accounts

5,924 criminal supporters

Outer Social Relationship

Social Butterflies

Those accounts that have extraordinarily large numbers of followers and followings.

use **2,000** following as a threshold

↓

3,818 social butterflies

The reason why social butterflies tend to have close friendships with criminals is mainly because most of them usually follow back the users who follow them without careful examinations.

Outer Social Relationship

Social Promoters

Those accounts that have large following-follower ratios, larger following numbers and relatively high URL ratios.

whose URL ratios are higher than **0.1**, and following numbers and following-follower ratios are both at the top **10-percentile**

↓

508 social promoters

Outer Social Relationship

Dummies

Those accounts who post few tweets but have many follow

post fewer than **5** tweets and
whose follower numbers are at the
top **10-percentile**

81 dummies

Inferring Criminal Accounts

Criminal account Inference Algorithm (CIA)

1. criminal accounts tend to be socially connected

2. criminal accounts usually share similar topics, thus having strong semantic coordinations among them

Inferring Criminal Accounts

Criminal account Inference Algorithm (CIA)

Malicious Relevance Graph, G=(V,E,W)

V: all accounts

E: all follow relationship, directed edge W: weight for each edge, WS(i,j)

$$WS(i, j) = \frac{SS_{ij}}{\sum_{e_{kj} \in E} SS_{kj}}$$

UCF

Inferring Criminal Accounts

Evaluation of CIA

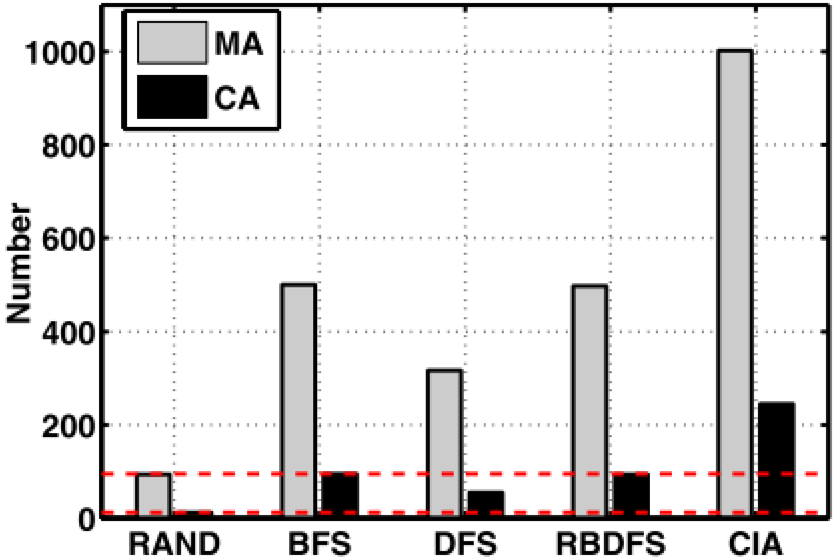
Dataset I: around half million accounts from previous study

Dataset II: another new crawled 30,000 accounts by starting from 10 newly identified criminal accounts and using BFS strategy

Inferring Criminal Accounts

Evaluation of CIA

Dataset I



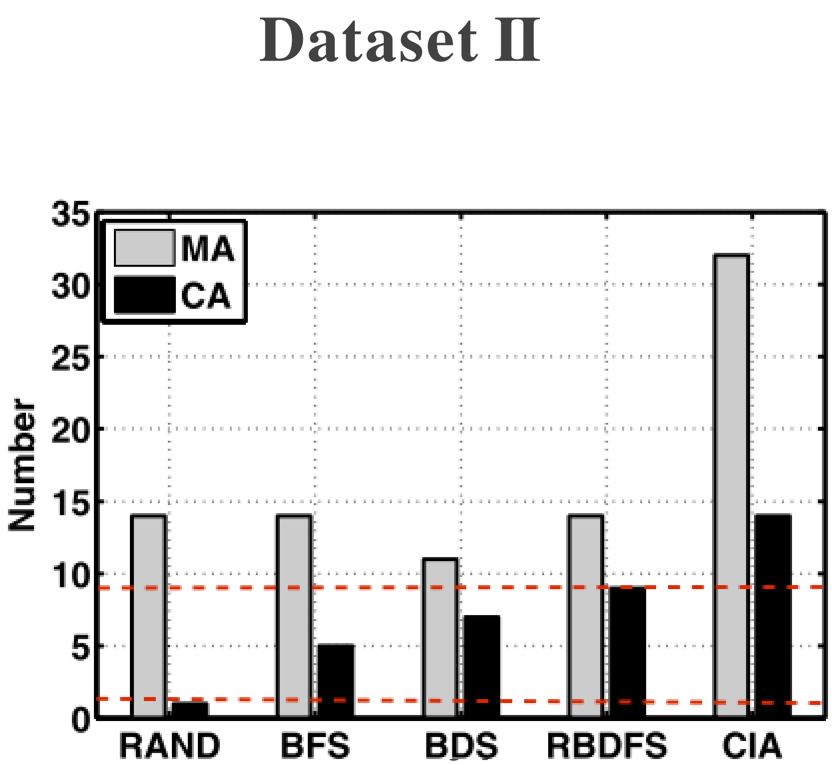
Selection Strategies

CA: Criminal Account
MA: Malicious Affected Account

100 seeds, select 4,000 accounts

Inferring Criminal Accounts

Evaluation of CIA



CA: Criminal Account
MA: Malicious Affected Account

10 seeds, select 4,000 accounts

Limitations

- Data set may have bias
- The number of criminal accounts analyzed are a lower bound of the actual criminal accounts
- There may be other types of accounts supporting criminal accounts

Conclusion

- Emperical study of cyber criminal ecosystem on Twitter
- Analysis of inner an outer relationships of criminal accounts
- Effective algorithms to catch criminal accounts
- The design is composable for accounts generating fake news, fake likes, and forming collusion networks

Thank You

UCF