Paper Introduction:

An Analysis of Social Network-Based Sybil Defenses

Survey by: Kazuhiro Inaba

この論文について

- ACM SIGCOMM Conference 2010 で発表
  - ネットワーク関係のトップカンファレンス

An Analysis of Social Network-Based Sybil Defenses

Bimal Viswanath
MPI-SWS
bviswana@mpi-sws.org

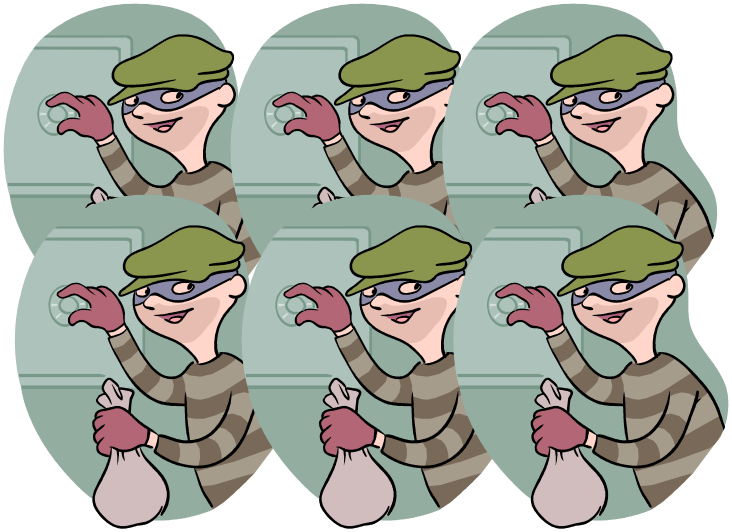
Ansley Post
MPI-SWS
abpost@mpi-sws.org

Krishna P. Gummadi
MPI-SWS
gummadi@mpi-sws.org

Alan Mislove
Northeastern University
amislove@ccs.neu.edu

Sybil

- P2P や SNS において、多数のアカウントを作って不正なことをする行為
  - 例: Social Bookmark Service で狙った記事を一斉にブックマークして目立たせる
  - 例: Amazon review で “この記事は参考になりましたか？” を不正に増やす
  - 例: P2Pサービスへの攻撃



読もうと思った動機

- Graph clustering / Community detection の “良さ” の評価方法について考えたい
  - Modularity, Conductance, Coverage, Surprise ...??
  - 特定の metric が高い値を出すと、“良い”のか？

It reminds me of a PLDI'98 paper.

Type-Based Alias Analysis*

Amer Diwan　　Kathryn S. McKinley　J. Eliot B. Moss

- 「プログラム中の変数と別の変数が、同じメモリ領域を指す可能性があるか？」の推定手法
  - ものすごくシンプルで速く使いやすい、が
  - 標準的な評価法：検出されたmay-aliasペアの数 (少ない→良い) では競合手法に大差
  - この論文の用いた評価方法：may-alias情報を使う最適化がコンパイラで実際に行われた回数

読もうと思った動機

- Graph clustering / Community detection の“良さ” の評価方法について考えたい
  - Modularity, Conductance, Coverage, ...????
  - 特定の metric が高い値を出すと、“良い”のか？
  - Community 検出の具体的な応用を使った、勝敗のつけやすい指標による評価について調査

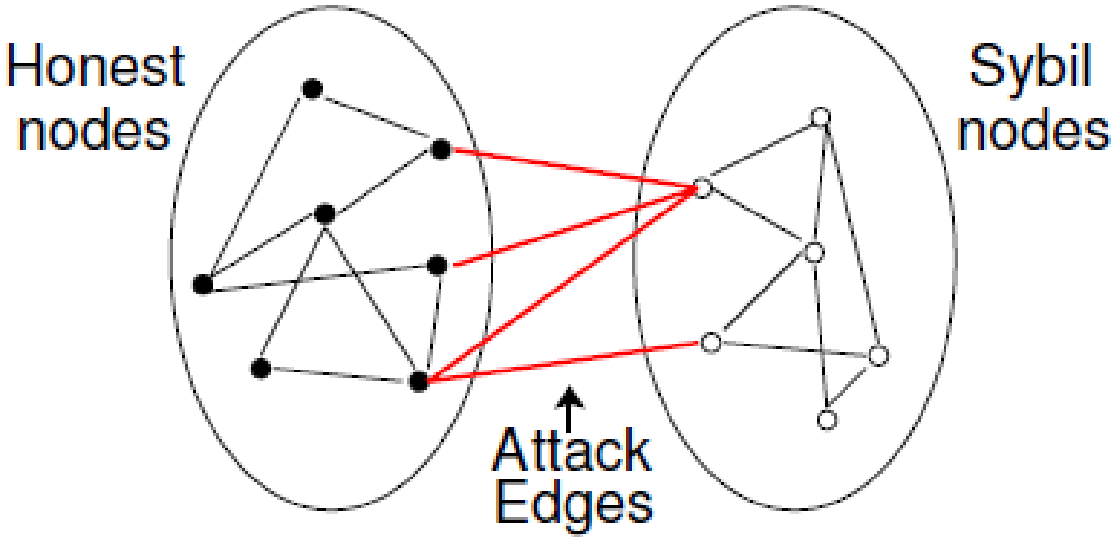
本題: AN ANALYSIS OF SOCIAL NETWORK-BASED SYBIL DEFENSES

概要

- 「Sybil Defense の既存手法の内容は全て、実質的に、Community Detection では？」
  - 実験的に、この考察を評価する
  - 逆に、既存の Community Detection のアルゴリズムをそのまま用いて Sybil Defense してみる
  - この考察に基づき、既存手法の有効性に疑問を投げかける

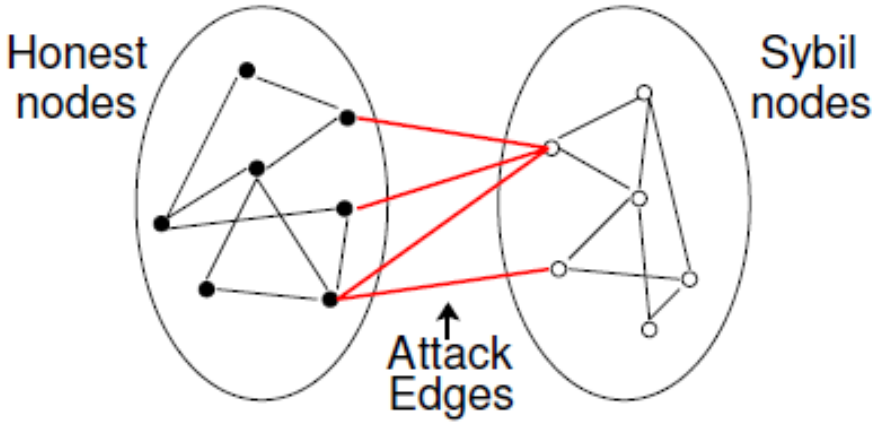
既存手法に共通する仮定 (1)

- Sybil ノードが Honest ノードと friend 関係を結ぶのは、（巧く騙す必要があり）難しい
  - ➔ “Attack Edge” は少ない



既存手法に共通する仮定 (2)

- “Attack Edge” は少ない



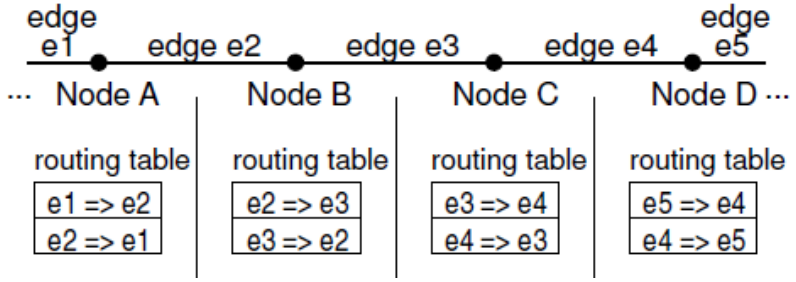
- Honest ノードのなすグラフは fast-mixing
  (i.e., O(log|V|) ステップの乱歩で定常分布に収束)
- Attack Edge が少ないため、全体では違う

既存手法
（として取り上げられているもの）

- SybilGuard
  - Yu, Kaminsky, Gibbons, and Flaxman (SIGCOMM’06)
- SybilLimit
  - Yu, Kaminsky, Gibbons, and Xiao (S&P‘08)
- SybilInfer
  - Danezis and Mittal (NSDI’09)
- SumUp
  - Tran, Min, Li, and Subramanian (NDSS’09)

比較対象 (1) SybilGuard

- 問題 : Honest ノードが friend request を他のノードから受けた。相手は Sybil か否か？



- 手法 : “RandomRoute”
  - 各ノードは接続するEdge→Edgeのランダムな全単射を持ち、それに従い歩く
  - 双方からの $\Theta(\sqrt{|V|}\log|V|)$ 歩の Random Route が交差すれば Honest と見なす

比較対象 (2) SybilLimit

- SybilGuard のグループの後続研究
  - Θ(log |V|) 歩の RandomRoute を双方から r 回
  - RandomRouteのTail集合の共通部分から一つedgeを選択
  - 各 edge につき |V|/r 回まで Honest として受理

TABLE I
NUMBER OF SYBIL NODES ACCEPTED PER ATTACK EDGE (OUT OF AN UNLIMITED NUMBER OF SYBIL NODES), BOTH ASYMPTOTICALLY FOR n HONEST NODES AND EXPERIMENTALLY FOR A MILLION HONEST NODES. SMALLER IS BETTER

Number of attack edges g (unknown to protocol)	**SybilGuard accepts**	**SybilLimit accepts**
$o(\sqrt{n}/\log n)$	$O(\sqrt{n}\log n)$	$O(\log n)$
$\Omega(\sqrt{n}/\log n)$ to $o(n/\log n)$	unlimited	$O(\log n)$
below $\sim 15,000$	~ 2000	~ 10
above $\sim 15,000$ and below $\sim 100,000$	unlimited	~ 10

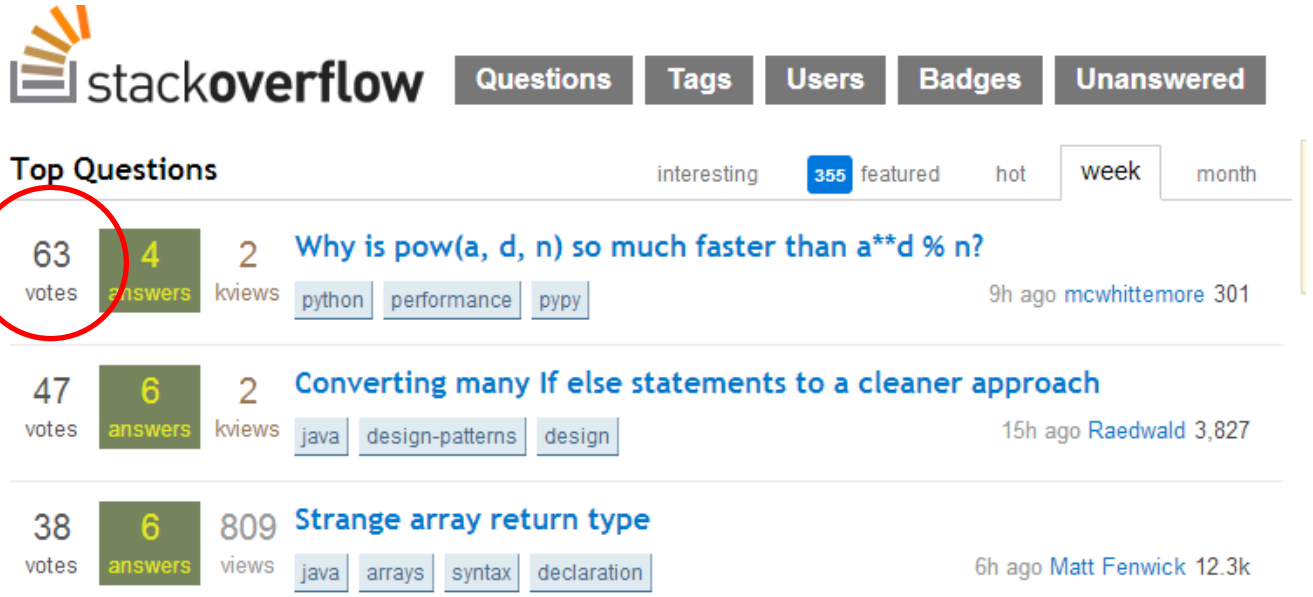
比較対象 (3) SybilInfer

- ノード u から v に移る確率を
  Puv = min(1/deg(u), 1/deg(v))
  とした遷移行列で Θ(log |V|) 歩ランダム歩き
- T := ランダムウォークの始点・終点ペアの集合

- P(X=SetOfAllHonestNodes | T) を最大化するXを Honest ノードの集合と見なす
  - 焼きなまし

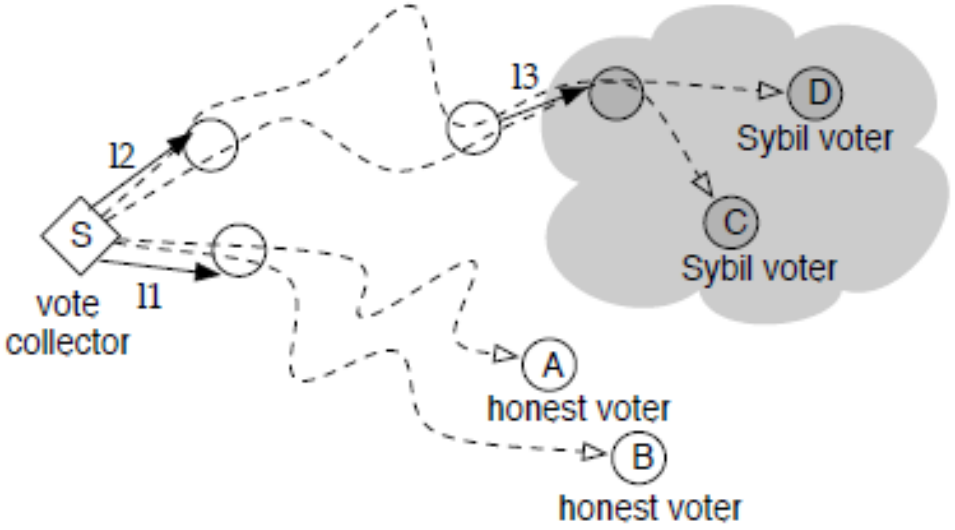
比較対象 (4) SumUp

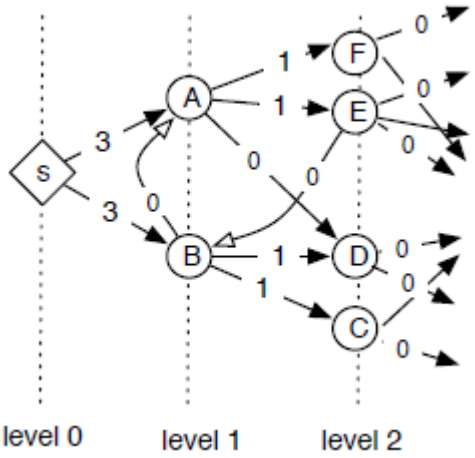
- “Sybil Resilient” social voting service
  - こういう系のサービス
  - Sybil からの票をできるだけ数えず Honest からの票だけ数えたい



比較対象 (4) SumUp

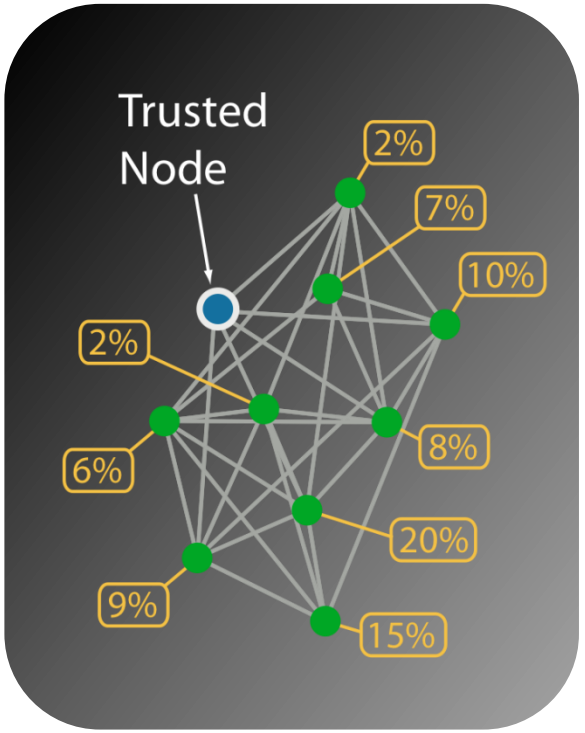
- Maxflow を計算することで集計をする
  - Source : trusted node(s)
  - Sink: 投票をした人
  - Source付近が混まないように容量を多少工夫



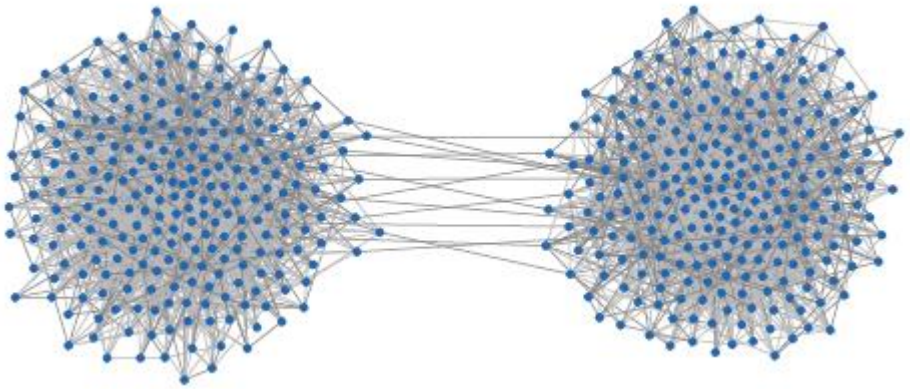


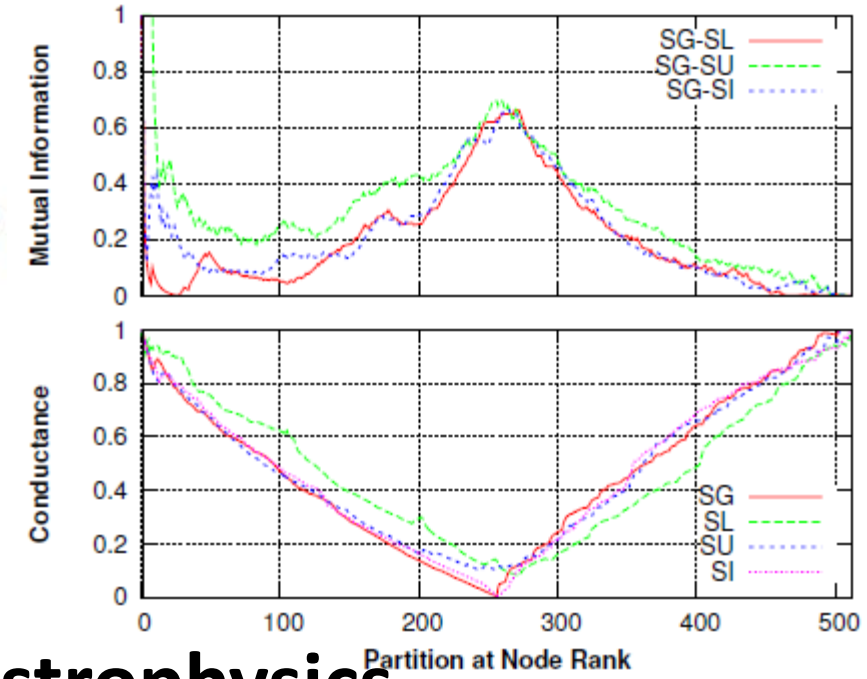
各手法の比較

- 各手法は、全ノードに “Sybil 度” のランク付けをするアルゴリズムと見なすことができる
  - 例: SybilGuard 交差するまでの RandomRoute の長さが長い = Sybil度が高い
- このランキングの様子を実験で調査する

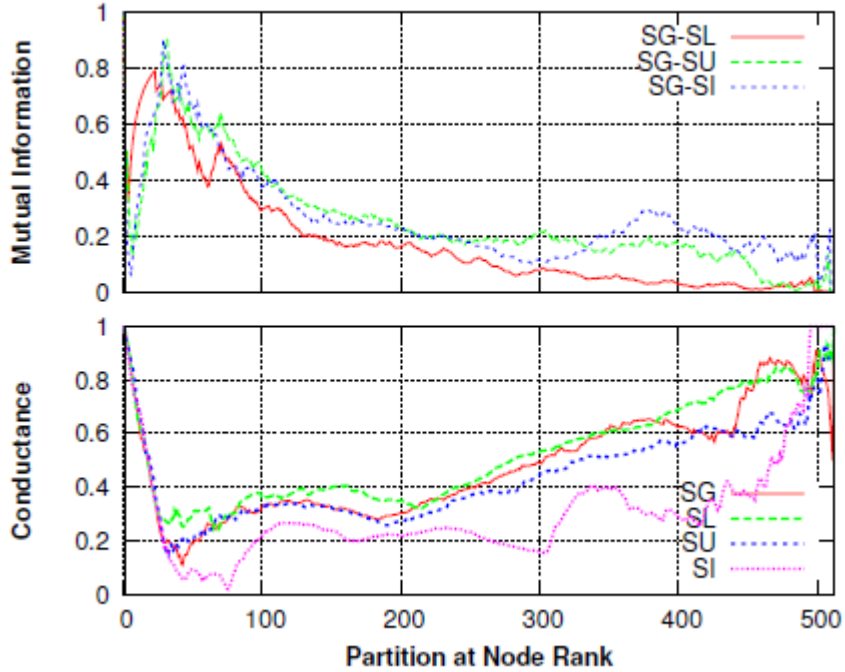


人エデータ

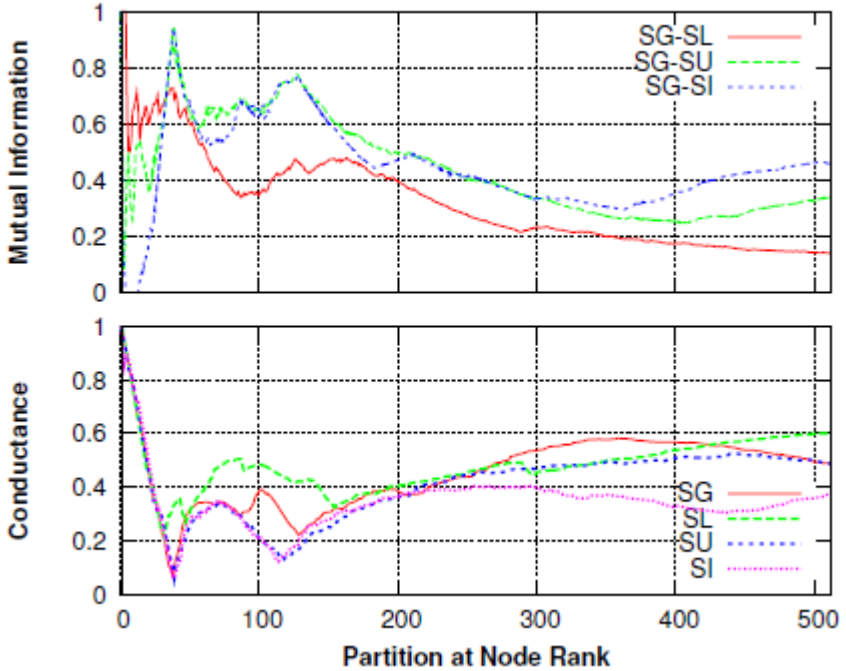




Facebook

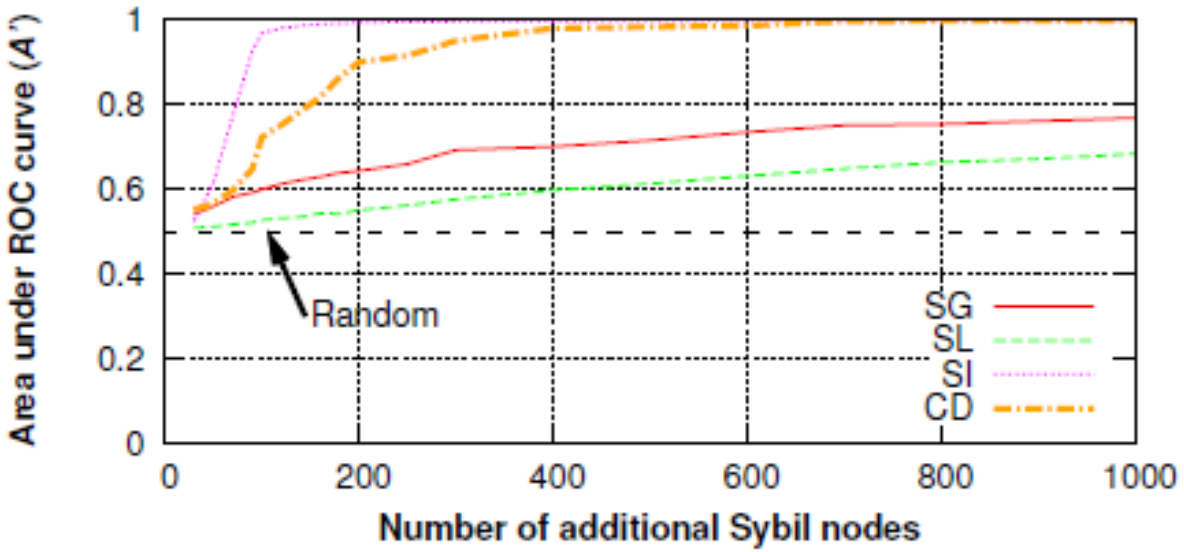


Astrophysics



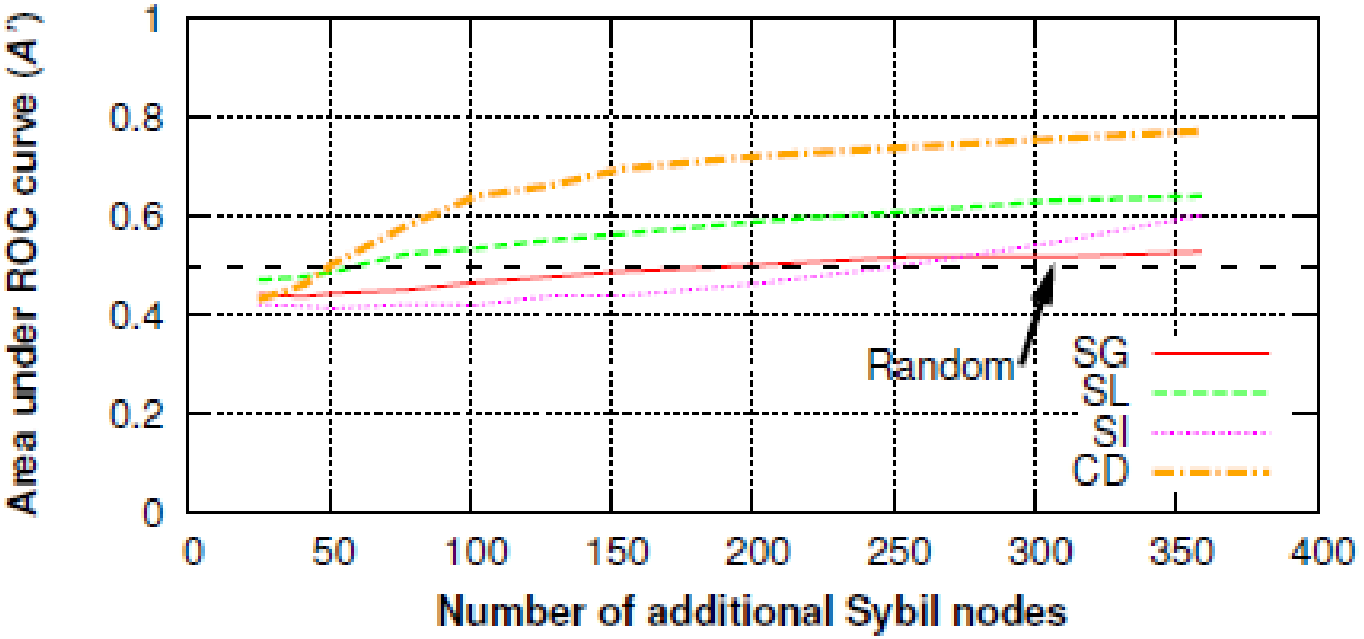
Sybil 検出力の実験

- 人工データ
  - Scale-free graph を生成 (Honest nodes)
  - 10% をランダムに選ぶ (Malicious nodes)
  - Sybil node を追加して Sybil+Malicious でグラフ生成



Sybil 検出力の実験

- Facebook Graph (500 node)
  - 10% をランダムに選ぶ (Malicious nodes)
  - Sybil node を追加して Sybil+Malicious でグラフ生成

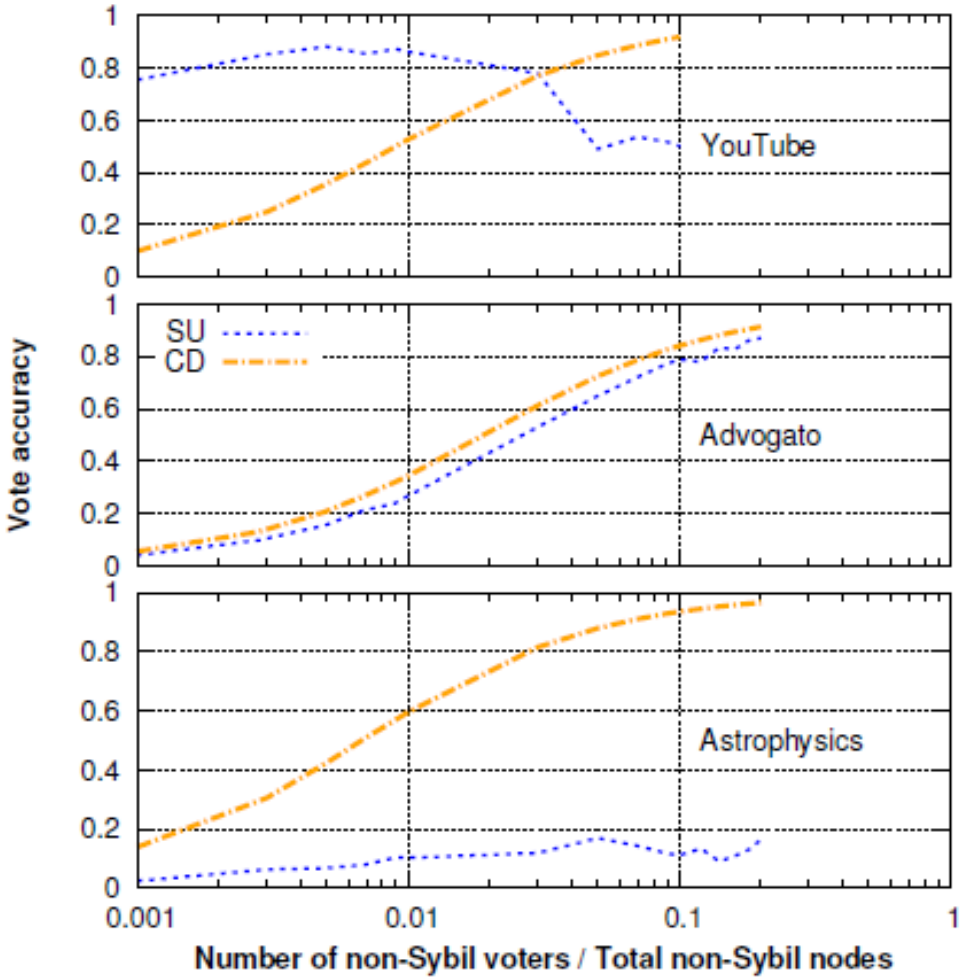


CD : (Local) Community Detection による方法

- 以下の論文のアルゴリズムを使用
  - Mislove, Viswanath, Gummadi, and Druschel, “You are who you know: inferring user profiles in online social networks”, WSDM’10
- Trusted node の単一元集合 S={v} から始めて、*conductance* を最小にする元をgreedyに追加
  - 極小になった所を v の属する community とする
  - 今回は、ランキングのために極小になっても止めず全ノードを処理する

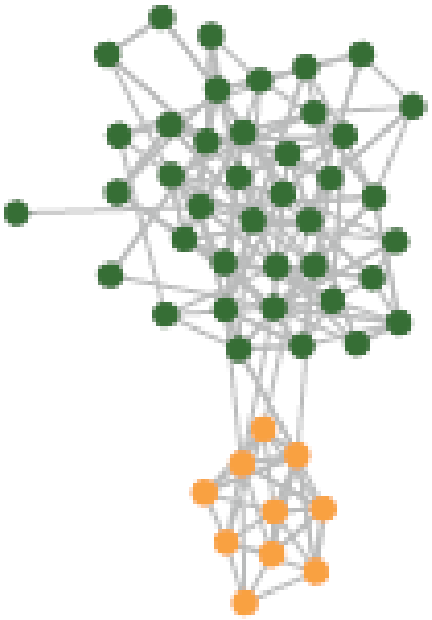
SumUp との比較実験

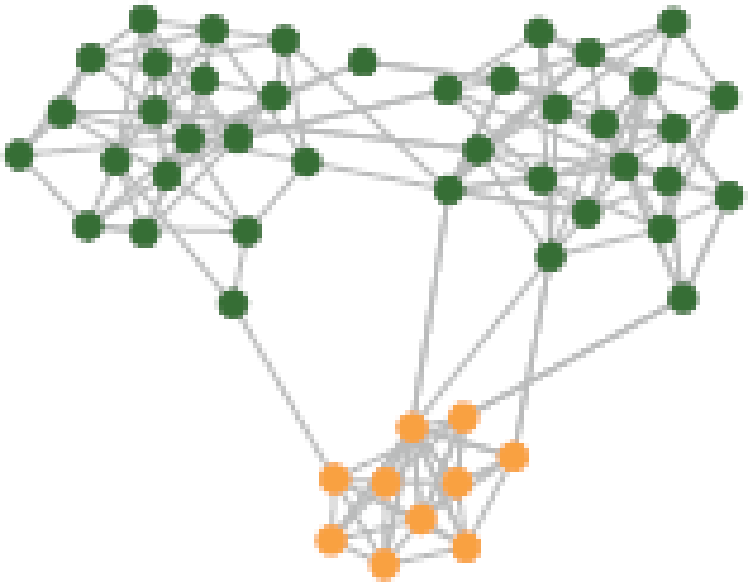
- 5000〜50万 nodes
- 100本のattack edge
- 縦軸は
  - 回収されたHonest 票 / 投票数



既存手法への疑問点

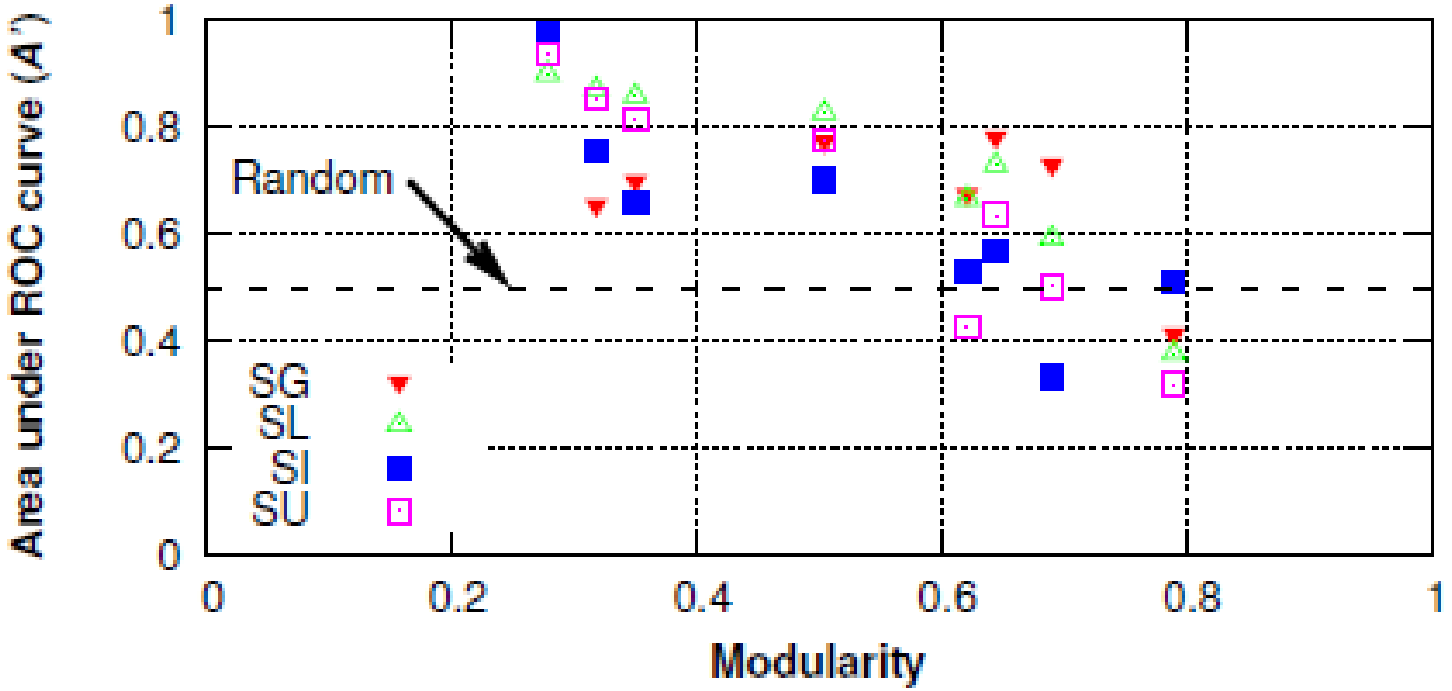
- 右図のような構造のネットワークに対応できるのか？





できていない

Network	Nodes	Links	Modularity
Facebook undergrad [21]	1,208	43,043	0.278
Advogato [1]	5,264	43,027	0.318
Wikipedia votes [13]	7,066	100,736	0.350
URV email [11]	1,133	5,451	0.504
Astrophysicists [25]	14,845	119,652	0.621
Facebook grad [21]	514	3,313	0.644
High-energy physics [14]	8,638	24,806	0.690
Relativity [14]	4,158	13,422	0.790



おまけ (1)
SumUp: Sybil-Resilient Online Content Voting (2009)

- digg.com のクロールデータで実験
- 300万ユーザー / 38000記事
- SumUp を使ったシミュレーションと実際の結果が食い違った記事を手作業で検証

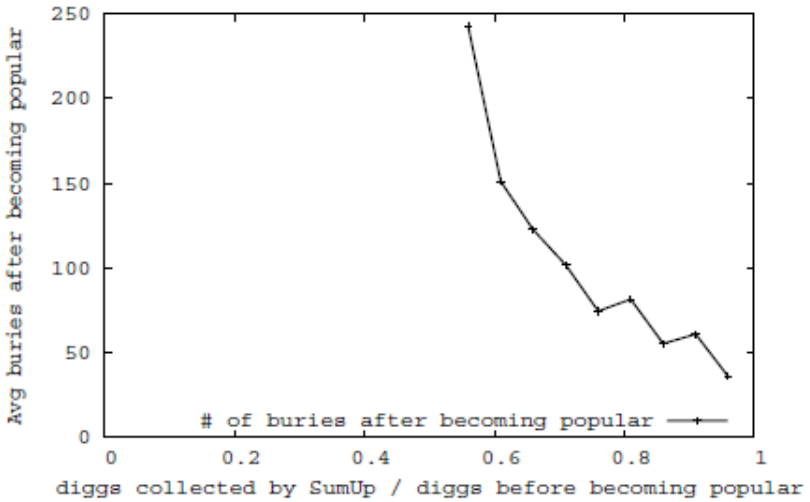


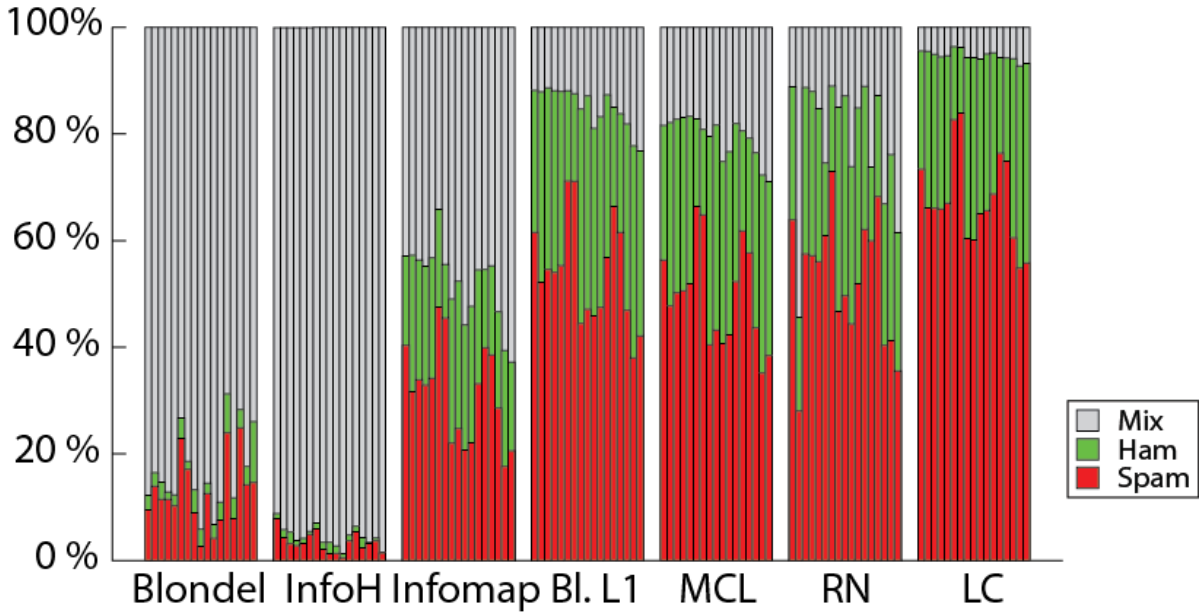
Figure 14: The average number of buries an article received *after* it was marked as popular as a function of the fraction of

Threshold of the fraction of collected diggs	20%	30%	40%	50%
# of suspicious articles	41	131	300	800
Advertisement	5	4	2	1
Phishing	1	0	0	0
Obscure political articles	2	2	0	0
Many newly registered voters	11	7	8	10
Fewer than 50 total diggs	1	3	6	4
No obvious attack	10	14	14	15

Table 3: Manual classification of 30 randomly sampled suspi-

おまけ (2)
An Evaluation of Community Detection Algorithms on Large-Scale Email Traffic (2012)

- コミュニティ検出でスパムメール判定
  - node: メールアドレス，edge: メール
  - 正解は SpamAssassin によるメール本文からの判定



おまけ (2)

An Evaluation of Community Detection Algorithms on Large-Scale Email Traffic (2012)