

## Part 3: Current Networking Topics

### Goals:

- ❑ Discuss current networking topics
- ❑ Learn emerging technologies

### Overview:

- ❑ Networking at the edge
- ❑ Network apps & services
- ❑ **Network security**
  - Unwanted traffic & network intrusion detection
  - Botnet attacks & defense
  - Achieving anonymity
  - **Leveraging trust in social networks**

Part 3.14 1

## Motivation

- ❑ Internet faces many security problems
  - DoS, spams, phishing, malware, sybil attacks
- ❑ Difficult to solve within today's Internet
  - Recall: security is largely an add-on to Internet
- ❑ What do we do?
  - Approach 1: Patching today's Internet
    - Problem: "arms race" never ends; defenders always lag behind
  - Approach 2: Clean-slate redesign of the Internet
    - Problem: the slate is not clean → it may never get deployed
  - **Approach 3: Looking for help outside the Internet**

**This lecture: How social networks can help us**

Part 3.14 2

## Social Networks

- Network defined by personal interaction
  - E.g., friends, friends of friends
  - E.g., social network for E-mails
    - Can be defined either explicitly through address book, or implicitly through past (non-spam) email exchanges

KEY: Each edge is associated with some degree of trust

Part 3.14 3

## The Rise of Social Networks

Social networks are becoming important in many areas

- ... in daily life
  - MySpace, Facebook, YouTube, LinkedIn, LiveJournal, Digg.com, Twitter, Orkut, Friendster, Cyworld, ...
- ... in business
  - Fraud detection
  - Targeted advertisement
- ... in information access
  - Improving search (e.g. Google Co-op, Yahoo! My Web)
  - Content recommendation (e.g., Netflix, Amazon)
- ... in systems research
  - Defending against Sybil (aka. multi-identity) attack
  - Fighting spams

Part 3.14 4

## SybilGuard: Defending Against Sybil Attacks via Social Networks

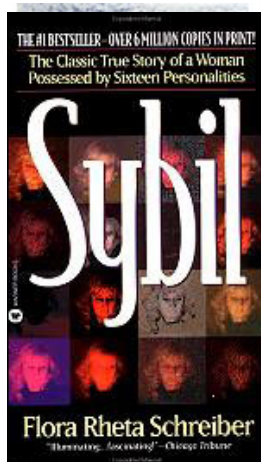
Haifeng Yu, Michael Kaminsky,  
Phillip B. Gibbons, Abraham Flaxman

Credit: Based on slides by Haifeng Yu

Part 3.14 5

## Etymology of Sybil

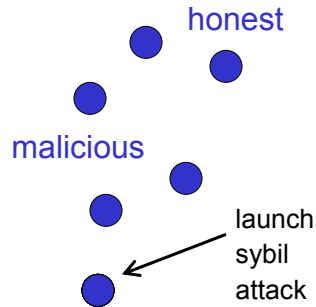
Sybil is a well known character of the 70s , a women possessed with multiple personality disorder, of 16 characters



Part 3.14 6

## Background: Sybil Attack

- ❑ **Sybil attack:** Single user pretends many fake/sybil identities
  - Creating multiple accounts from different IP addresses
- ❑ Sybil identities can become a large fraction of all identities
  - Out-vote honest users in collaborative tasks



Part 3.14 7

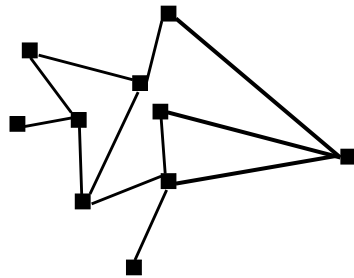
## Background: Defending Sybil Attack

- ❑ Using a trusted central authority
  - Tie identities to actual human beings
- ❑ Not always desirable
  - Can be hard to find such authority
  - Sensitive info may scare away users
  - Potential bottleneck and target of attack
- ❑ Without a trusted central authority
  - Impossible unless using special assumptions [Douceur'02]
  - Resource challenges not sufficient -- adversary can have much more resources than typical user

Part 3.14 8

## SybilGuard Basic Insight: Leveraging Social Networks

### Our Social Network Definition

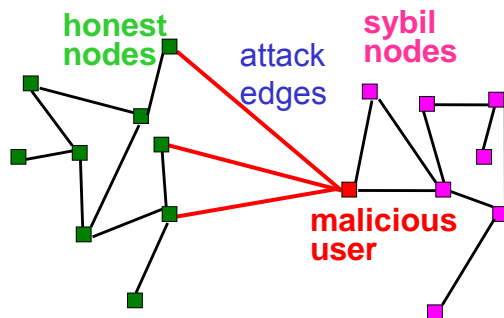


- Undirected graph
- Nodes = identities
- Edges = **strong** trust
  - E.g., colleagues, relatives

Part 3.14 9

## SybilGuard Basic Insight

- $n$  honest users: One identity/node each
- Malicious users: Multiple identities each (sybil nodes)

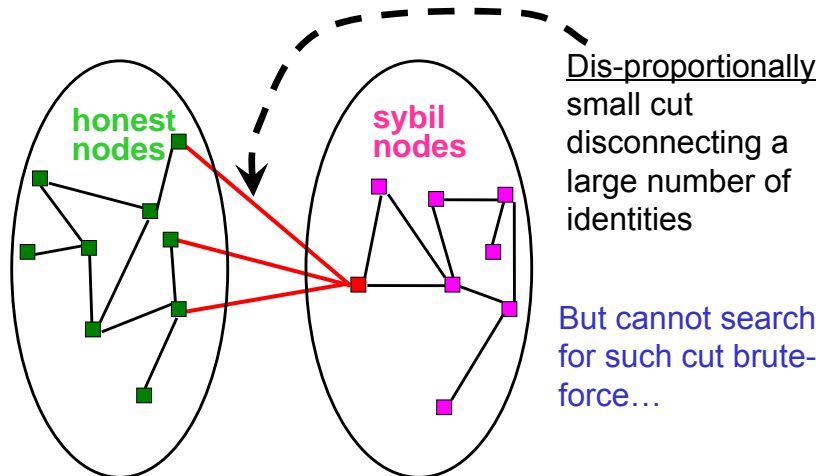


Sybil nodes may collude – the adversary

Observation: Adversary cannot create extra edges between honest nodes and sybil nodes

Part 3.14 10

## SybilGuard Basic Insight



Part 3.14 11

## Outline

- ✓ Motivation and SybilGuard basic insight
- Overview of SybilGuard: Random routes
- Properties of SybilGuard protocol
- Evaluation results
- Conclusions

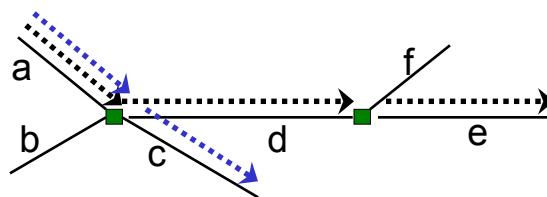
Part 3.14 12

## Goal of Sybil Defense

- Goal: Enable a *verifier* node to decide whether to **accept** another *suspect* node
  - **Accept**: Provide service to / receive service from
  - Idealized guarantee: An honest node accepts and only accepts other honest nodes
  
- SybilGuard:
  - Bounds the number of sybil nodes accepted
  - Guarantees are with high probability
  - Approach: Acceptance based on **random route intersection** between verifier and suspect

Part 3.14 13

## Random Walk Review



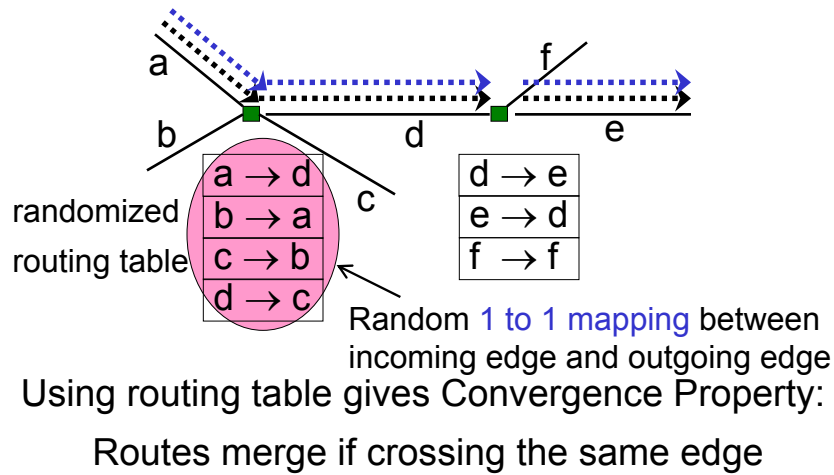
pick random edge d

pick random edge e

pick random edge c

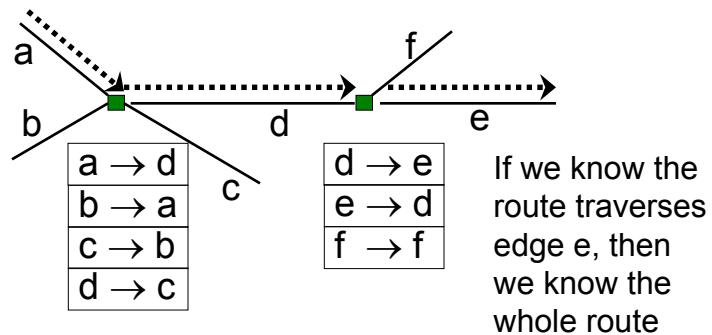
Part 3.14 14

## Random Route: Convergence



Part 3.14 15

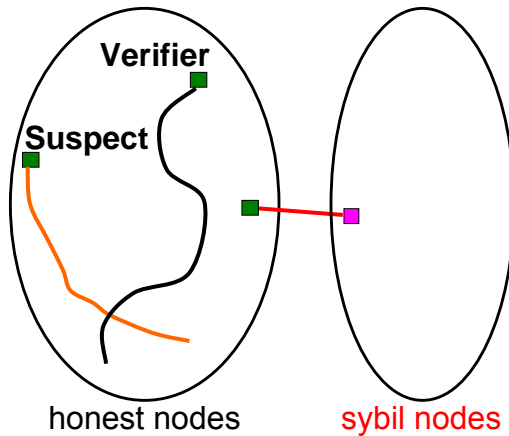
## Random Route: Back-traceable



Using 1-1 mapping gives Back-traceable Property:  
Routes may be back-traced

Part 3.14 16

## Random Route Intersection: Honest Nodes



- Verifier accepts a suspect if the two routes intersect
  - Route length  $w$ :  
 $\sim \sqrt{n \log n}$
  - W.h.p., verifier's route stays within honest region
  - W.h.p., routes from two honest nodes intersect

**Assumption: SN among honest nodes is fast mixing**

17

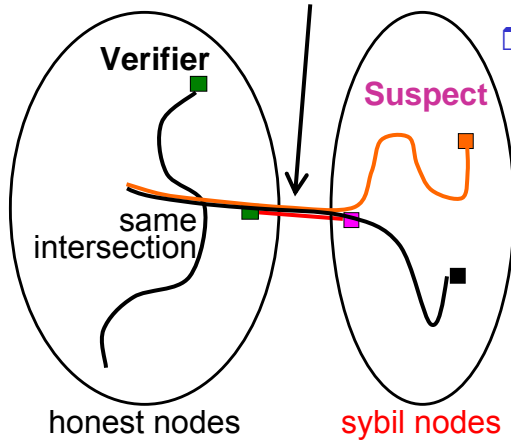
## Random Route Intersection: Sybil Nodes

- SybilGuard bounds the number of accepted sybil nodes within  $g^* w$ 
  - $g$ : Number of attack edges
  - $w$ : Length of random routes
- Next ...
  - Convergence property to bound the **number of intersections** within  $g$
  - Back-traceable property to bound the **number of accepted sybil nodes per intersection** within  $w$

Part 3.14 18

## Bound # Intersections Within $g$

must cross attack edge to intersect even if sybil nodes do not follow the protocol

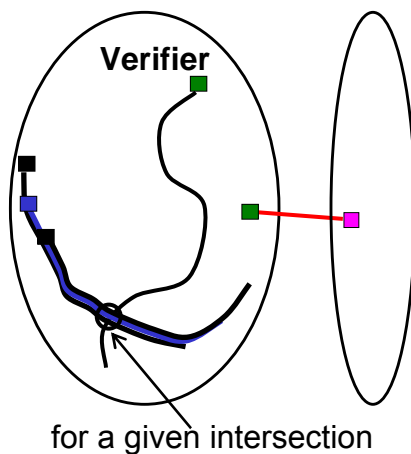


- Convergence: Each attack edge gives one intersection  
 $\Rightarrow$  at most  $g$  intersections with  $g$  attack edges

Intersection =  
(node, incoming edge)

Part 3.14 19

## Bound # Sybil Nodes Accepted per Intersection within $w$



- Back-traceable: Each intersection should correspond to routes from at most  $w$  honest nodes
- Verifier accepts at most  $w$  nodes per intersection
  - Will not hurt honest nodes

Part 3.14 20

## Summary of SybilGuard Guarantees

- Power of the adversary:
  - *Unlimited* number of *colluding* sybil nodes
  - Sybil nodes may not follow SybilGuard protocol
- W.h.p., honest node accepts  $\leq g^* w$  sybil nodes
  - $g$ : # of attack edges
  - $w$ : Length of random route

If SybilGuard bounds # accepted sybil nodes within	Then apps can do
$n/2$	byzantine consensus
$n$	majority voting
not much larger than $n$	effective replication

Part 3.14 21

## Outline

- √ Motivation and SybilGuard basic insight
- √ Overview of SybilGuard
- Properties of SybilGuard protocol
- Evaluation results
- Conclusions

Part 3.14 22

## SybilGuard Protocol

### ❑ Security:

- Protocol ensures that nodes cannot lie about their random routes in the honest region

### ❑ Decentralized:

- No one has global view
- Nodes only communicate with direct neighbors in the social network when doing random routes

Part 3.14 23

## SybilGuard Protocol (continued)

### ❑ Efficiency: Random routes are performed only once and then "remembered"

- No more message exchanges needed unless the social network changes
- Verifier incurs  $O(1)$  messages to verify a suspect

### ❑ User and node dynamics:

- Different from DHTs, node churn is a non-problem in SybilGuard ...

### ❑ See paper for all the details ...

Part 3.14 24

## Evaluation Results

- ❑ Simulation based on synthetic social network model [Kleinberg'00] for 106, 104, 102 nodes
- ❑ With 2500 attack edges (i.e., adversary has acquired 2500 social trust relationships):
  - Honest node accepts honest node with 99.8% prob
  - 99.8% honest node properly bounds the number of accepted sybil nodes
  - See paper for full results ...

Part 3.14 25

## SybilGuard Summary

- ❑ Sybil attack: Serious threat to collaborative tasks in decentralized systems
- ❑ SybilGuard: Fully decentralized defense protocol
  - Based on random routes on social networks
  - Effectiveness shown via simulation and analysis
- ❑ Follow-up work: SybilLimit [IEEE S&P 08]
  - SybilGuard accepts  $O(g \cdot \log(n) \cdot \sqrt{n})$  sybil nodes
    - $g$ : number of attack edges (assuming  $g = o(\sqrt{n}/\log(n))$ )
    - $w$  (in  $g \cdot w$ ) needs to be as large as  $O(\sqrt{n} \cdot \log(n))$  to ensure fast mixing
  - SybilLimit gives much better guarantee  
honest node accepts  $\leq g \cdot \log(n)$  sybil nodes
  - Close to optimal -  
any algorithm would accept at least  $O(g)$  sybil nodes

Part 3.14 26

## Defending Against SPAM via Social Networks

Part 3.14 27

### Applied in Two Ways

- Reduce false positives of spam filtering by white-listing friends and friends of friends
  - RE: Reliable Email [NSDI'06]
    - Infer friendship from non-spam email exchanges
    - Protocol preserves privacy
  - Can reduce FP by 87% (71% direct, 16% FoF)
- Social spam filtering
  - E.g. TrustMyMail.com
    - Infer social network from past email exchanges
    - Compute trust metric based on distance in social network
    - Filter SPAM if trust metric is too low

Part 3.14 28