Reference Papers

1. SybilGuard Defending Against Sybil Attacks via Social Networks, *Haifeng Yu, Michael Kaminsky , Phillip B. Gibbons , Abraham Flaxman*

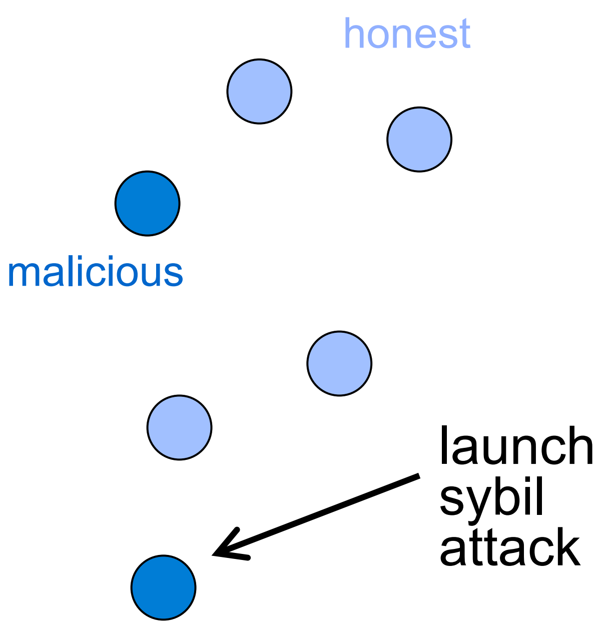
Outline

- Sybil Attack
- Sybil Guard

Background: Sybil Attack

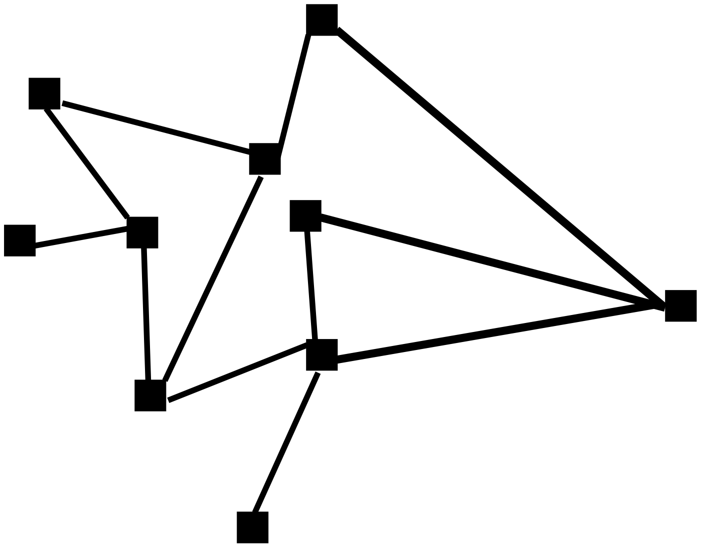
- Sybil attack: Single user pretends many fake/sybil identities
  - Creating multiple accounts from different IP addresses

- Sybil identities can become a large fraction of all identities
  - Out-vote honest users in collaborative tasks



SybilGuard Basic Insight: Leveraging Social Networks

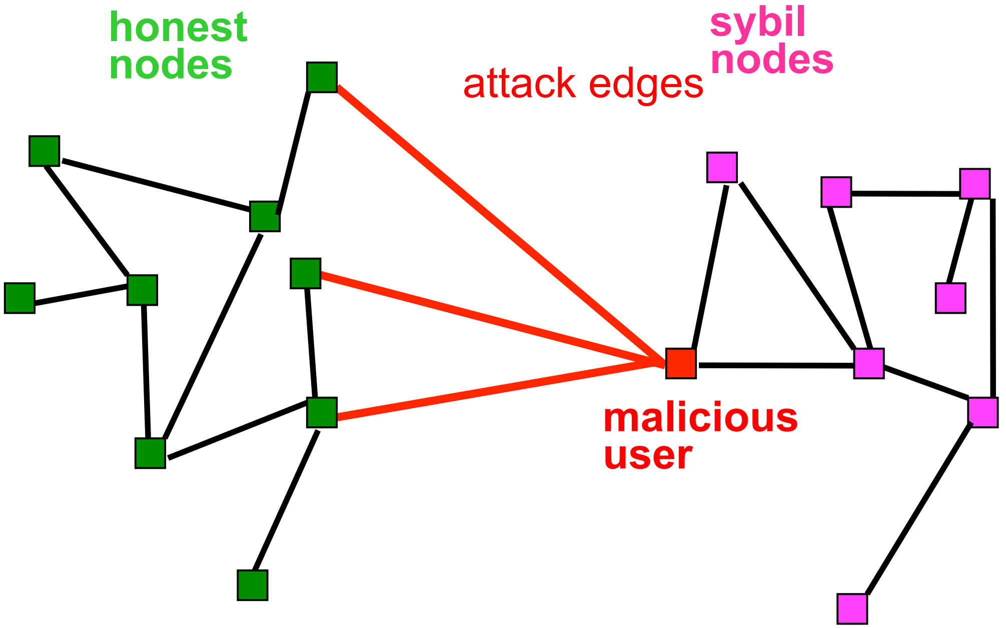
Our Social Network Definition



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

SybilGuard Basic Insight

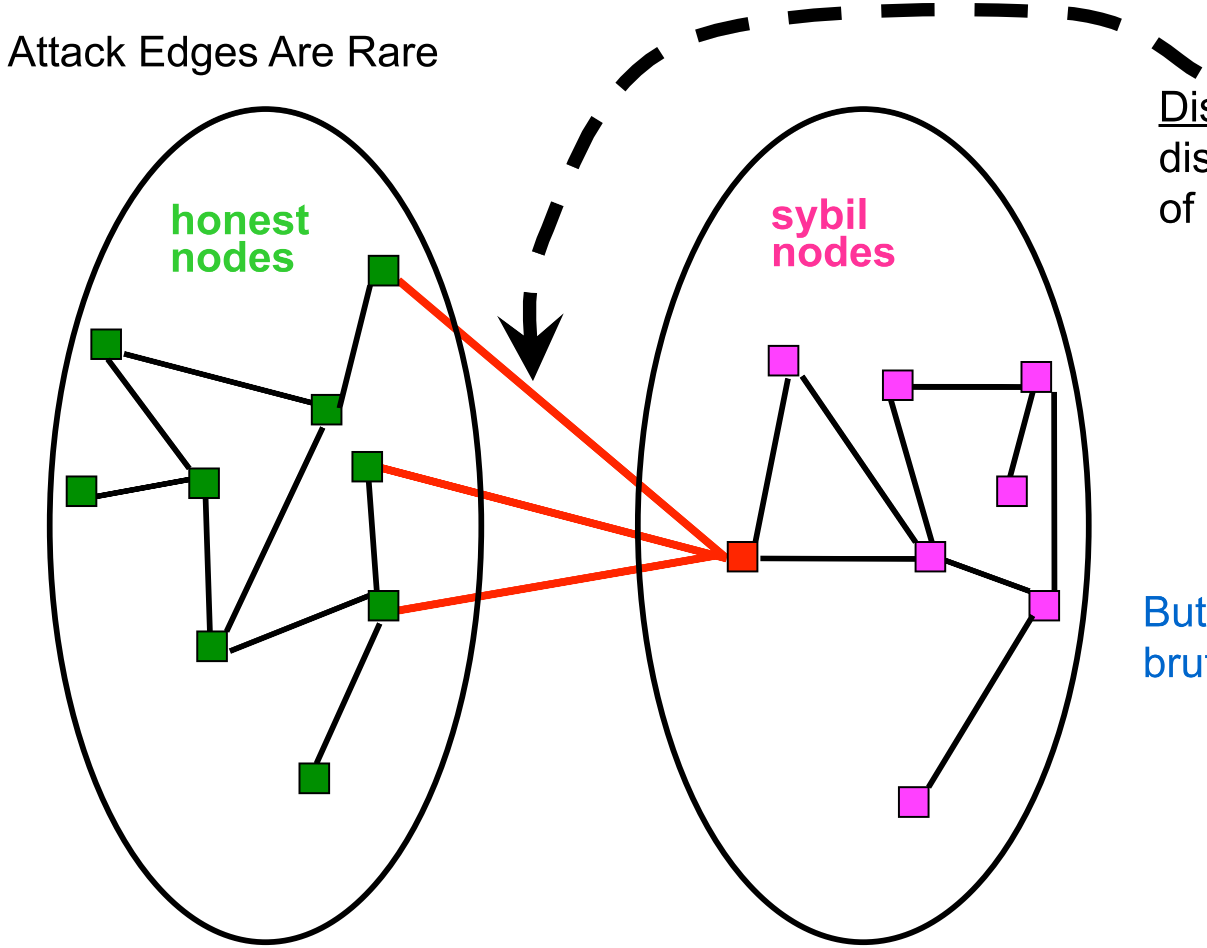
- *n* honest users: One identity/node each
- Malicious users: Multiple identities each (sybil nodes)



- Edges to honest nodes are "human established"
- Attack edges are difficult for Sybil nodes to create
- Sybil nodes may collude – the adversary

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

SybilGuard Basic Insight



Dis-proportionally small cut disconnecting a large number of identities

But cannot search for such cut brute-force…

SybilGuard's Model

- A social network exists containing honest nodes and Sybil nodes
- Honest nodes provide a service to or receive a service from nodes that they "accept"

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:

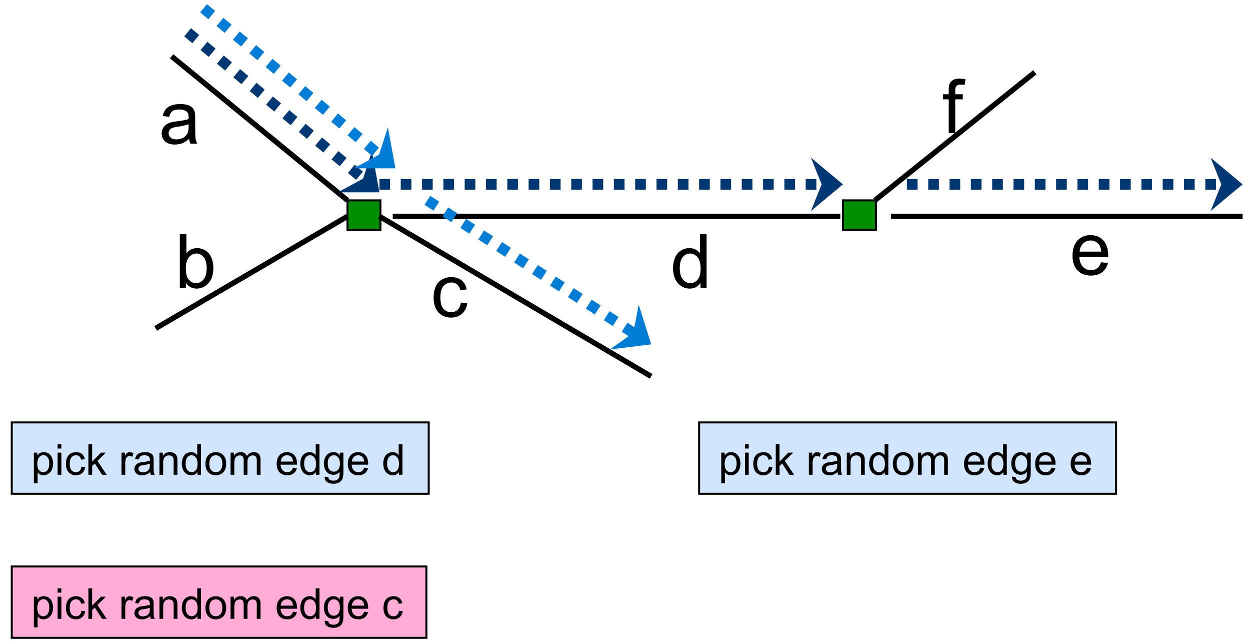
- Bounds the number of sybil nodes accepted
- Guarantees are with high probability
- Accepts and is accepted by most honest nodes
- Approach: Acceptance based on random route intersection between verifier and suspect

Random Routes

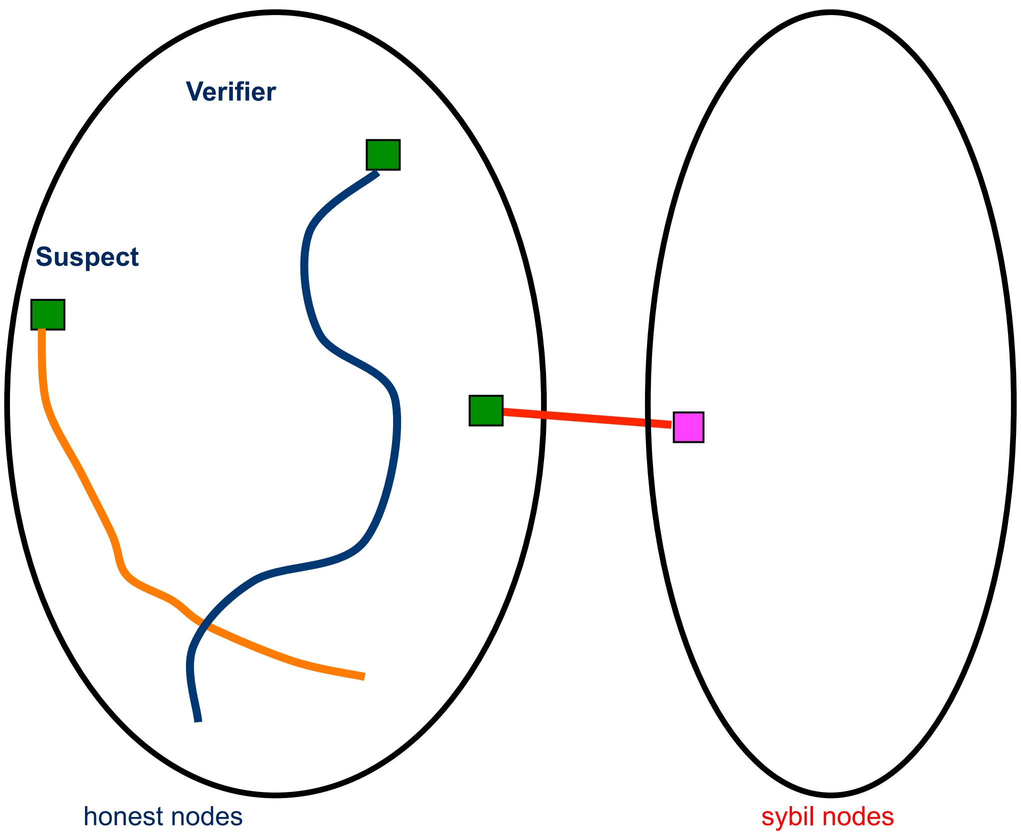
- Every node picks a random routing from input to output edges
- A directed edge is in exactly one route of unbounded length
- A directed edge is in at most w routes of length w

Clever Use of Random Routes

- Each node finds all the length w random routes that start at the node itself
- Honest node V accepts node S if most of V's random routes intersect a random route of S

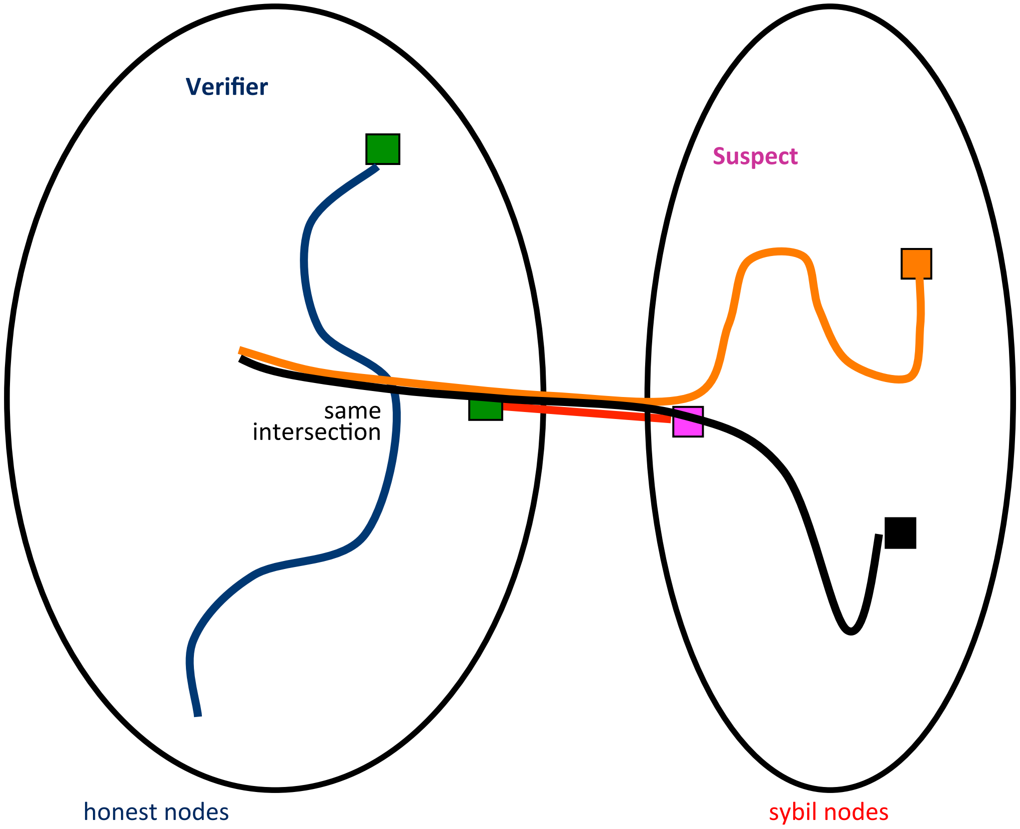


Random Route Intersection: Honest Nodes



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

Random Route Intersection: Sybil Nodes



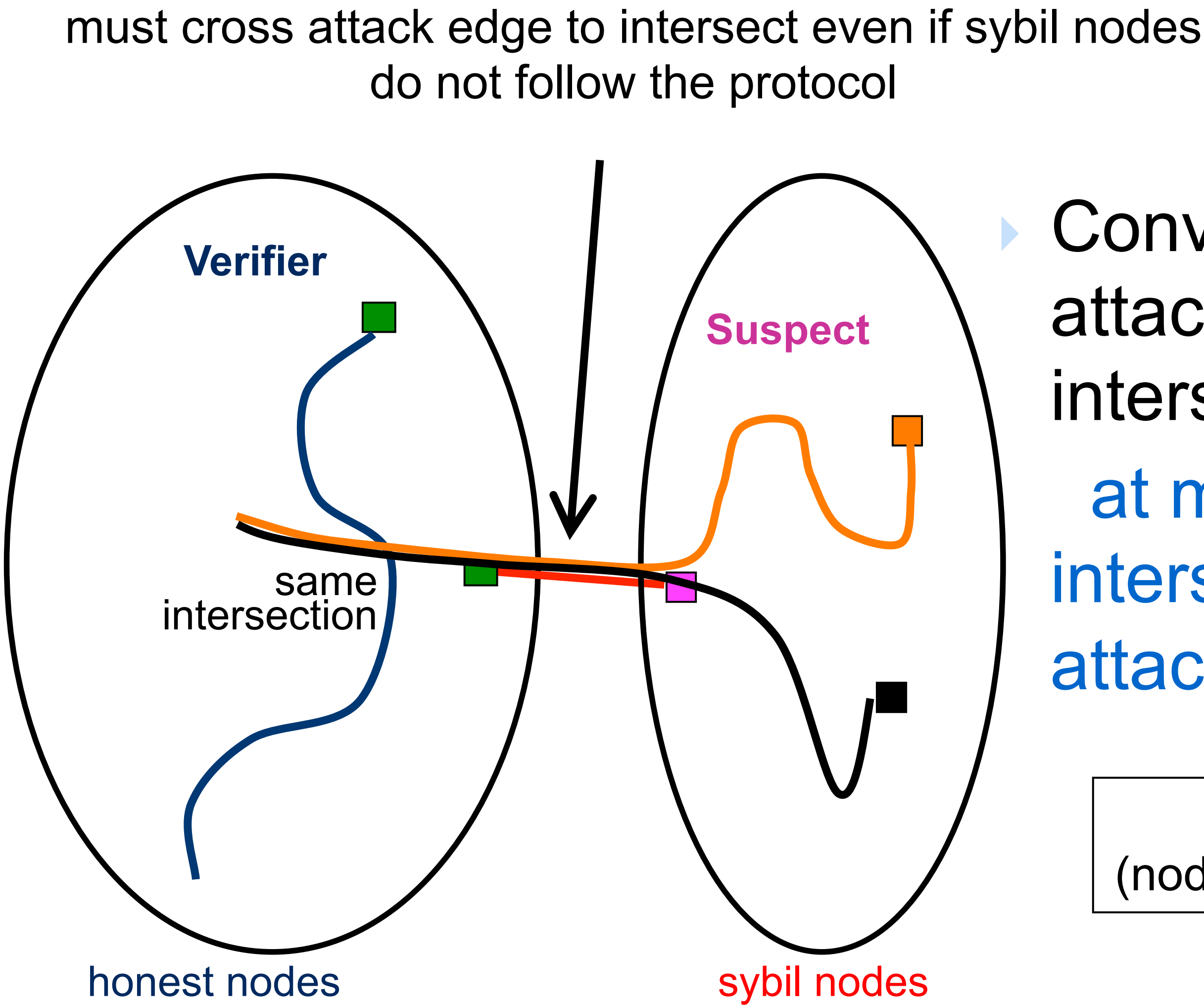
- Each attack edge gives one intersection
- Intersection points are SybilGuard's equivalence sets

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

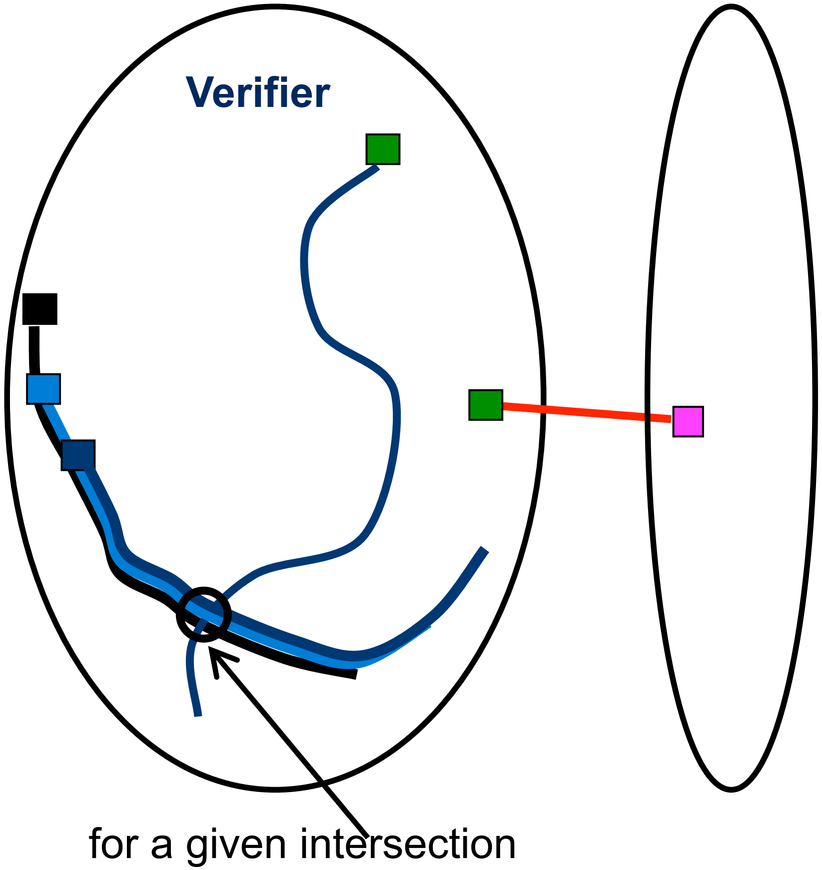
Bound # Intersections Within *g*



- Convergence: Each attack edge gives one intersection
  at most *g* intersections with *g* attack edges

Intersection =
(node, incoming edge)

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

Conclusions

- 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
    -

- Future work: (Already Done)
  - Local Partitioning using PageRank
  - Evaluation using real and large-scale social networks

Thank you – Enjoy the rest of your night