A Sybil-Resistant Admission Control Coupling SybilGuard with Distributed Certification

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong
firstname.lastname@supelec.fr

Supélec, SSIR Group (EA 4039)

COPS, June 2008
Rome, Italy

What is the Sybil Attack ?

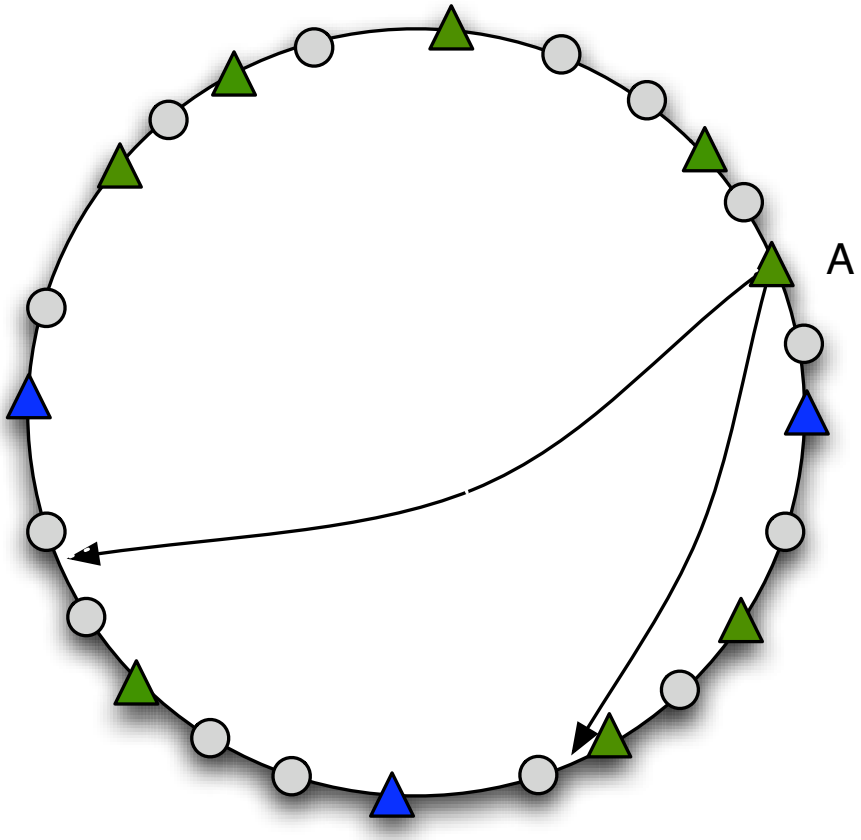
Honest network

1. Each user generates a random unique identifier
2. These identifiers are uniformly distributed

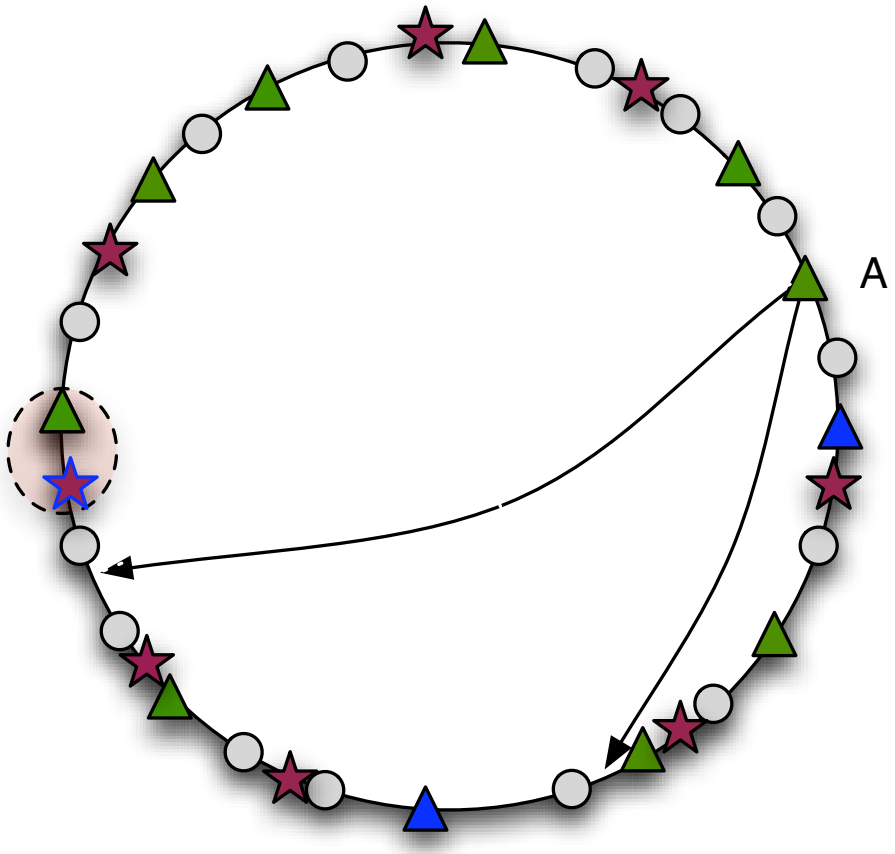
Network under Sybil Attack

1. An attacker *chooses* many identifiers
2. This attacker corrupts the uniform distribution

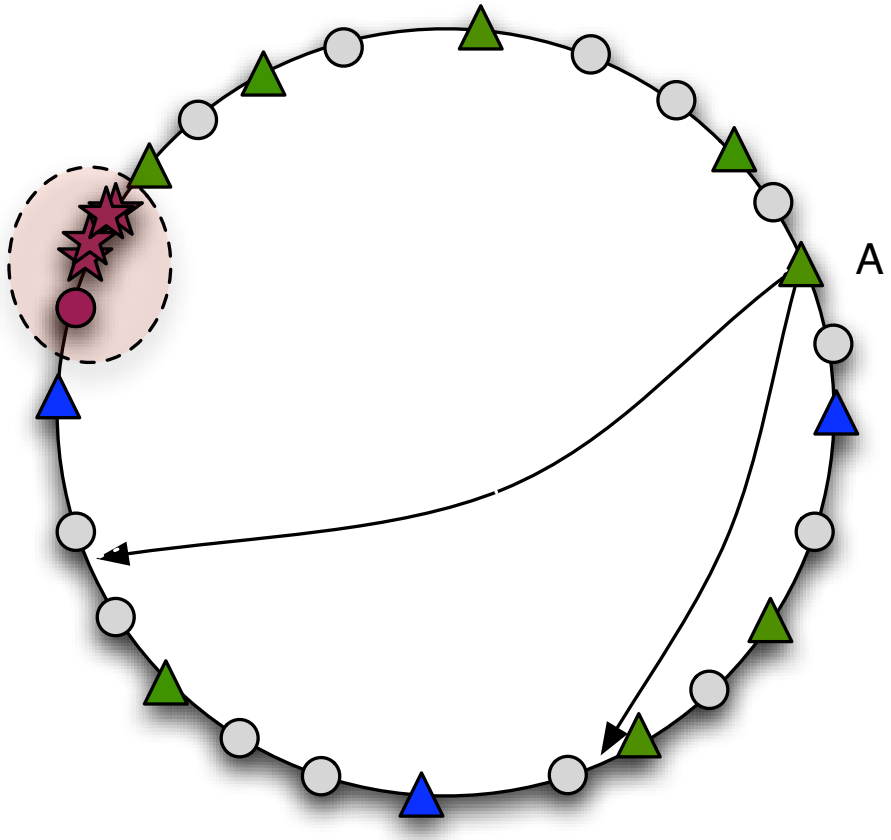
Routing Table of a Node (Chord)



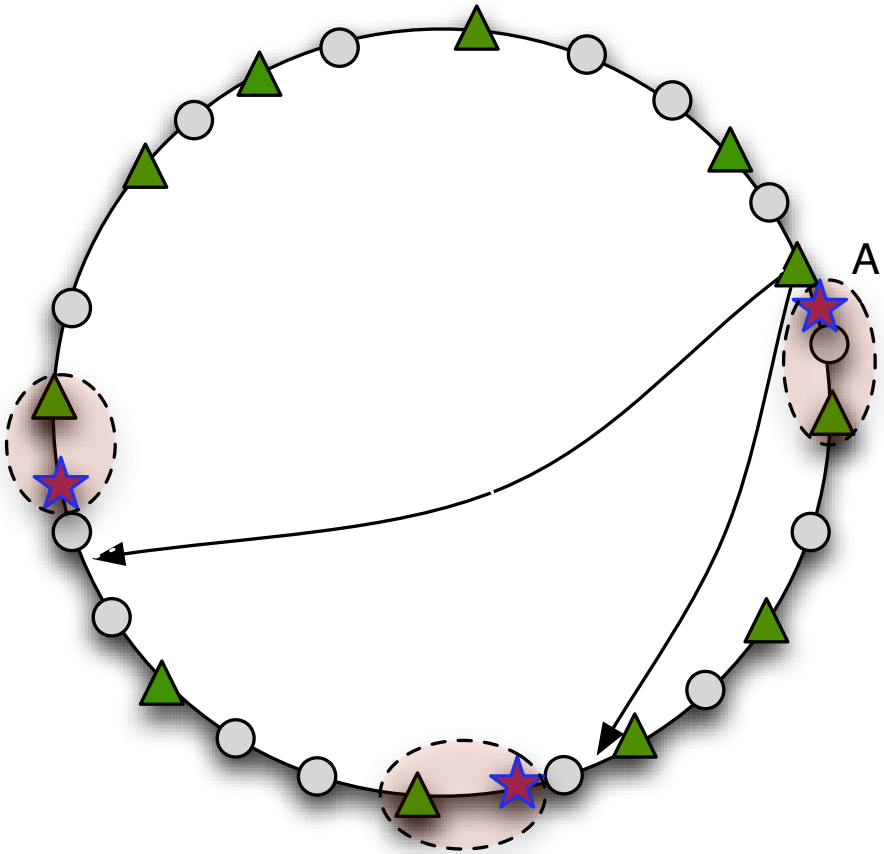
Global Attack



Attack of a Resource: Censorship



Attack of a Node: Filtering



Limiting the Sybil Attack

Limiting the Sybil Attack requires to

- Limit the number of identifiers of each physical person
- Constrain these identifiers to be randomly chosen

In our proposition

- Number of identifiers is limited using social SybilGuard
- Random identifiers are hashed from certificates

Related Work

Crypto-puzzles

Huge disparities among users

Social protections (SybilGuard)

No constraints on node identifiers

Certification Authorities

Expensive and centralized

$\Rightarrow$ Combination of Social and CA

Outline

1. Presentation of the two Combined Sybil Protections
2. Combination of SybilGuard with Distributed Certification

Presentation of the two Combined Sybil Protections

SybilGuard: a Social-Based Protection

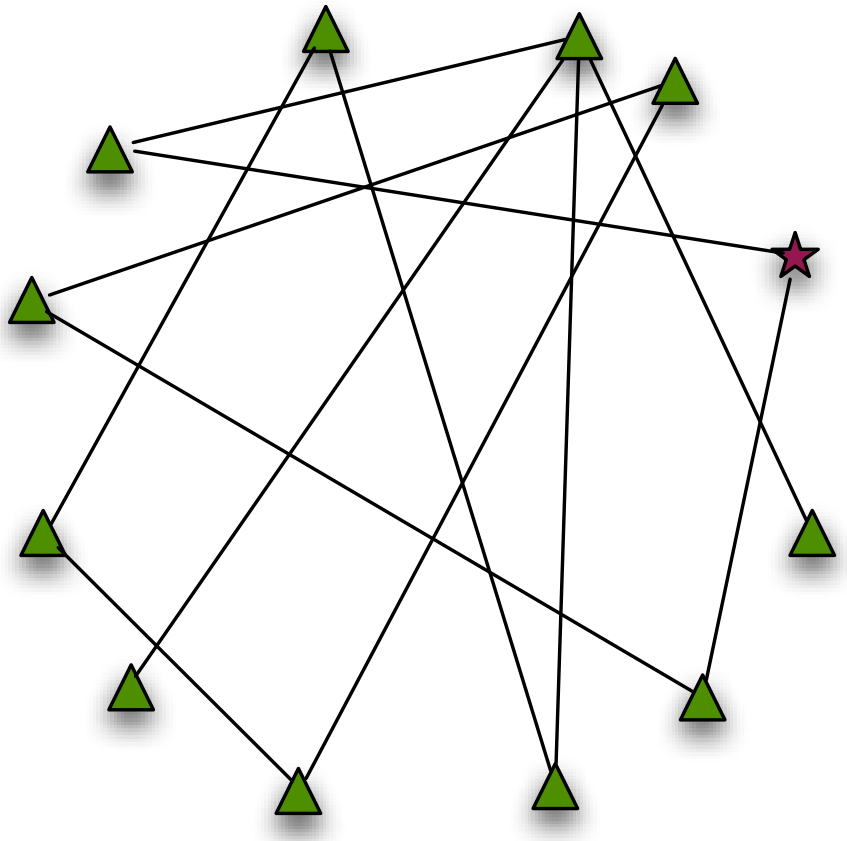
Principle

- Each member manually creates edges to friends
- Each member automatically creates random convergent routes
- A member accepts another one if routes intersect

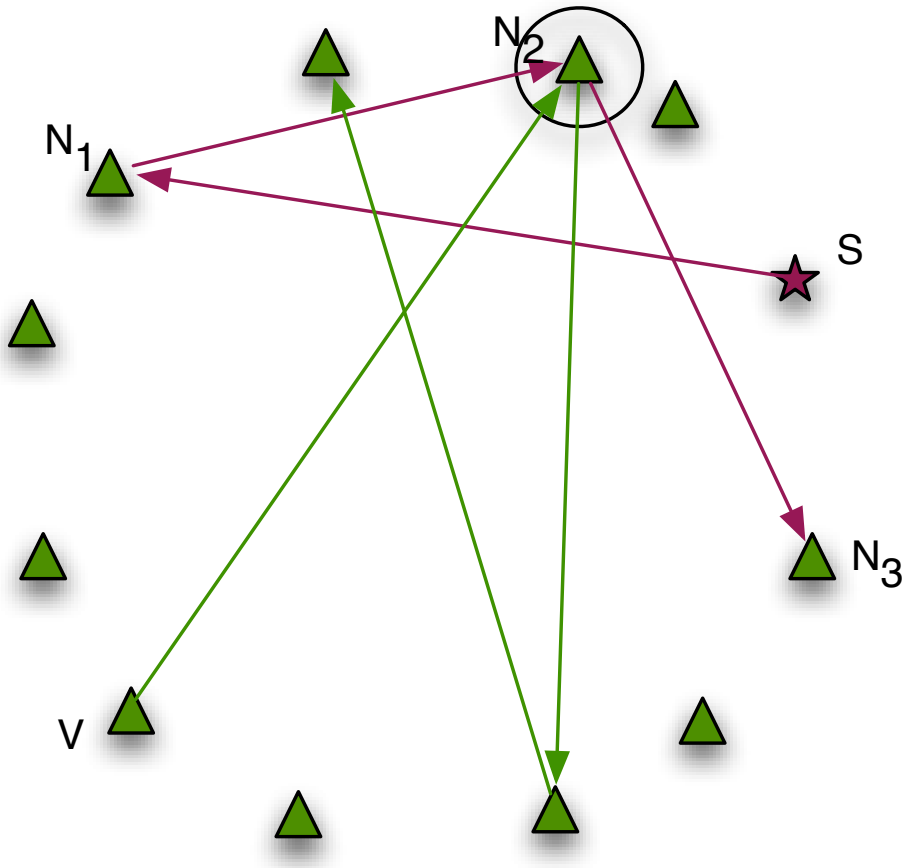
For us...

A "simple" oracle for sybil-detection

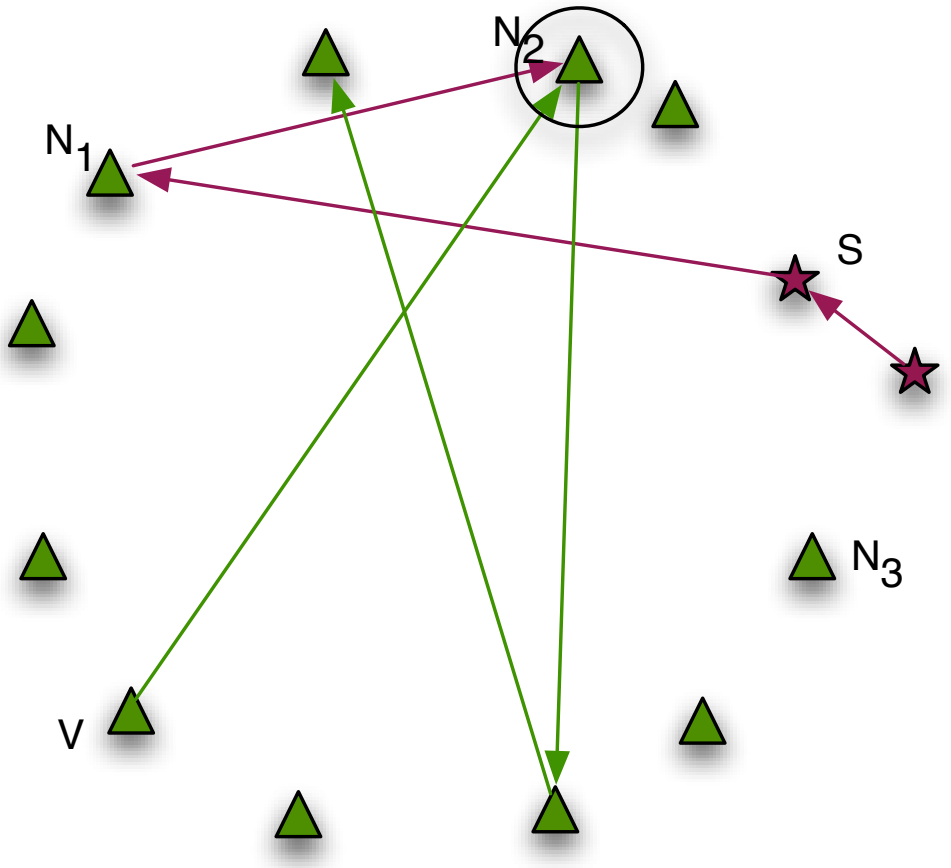
Example



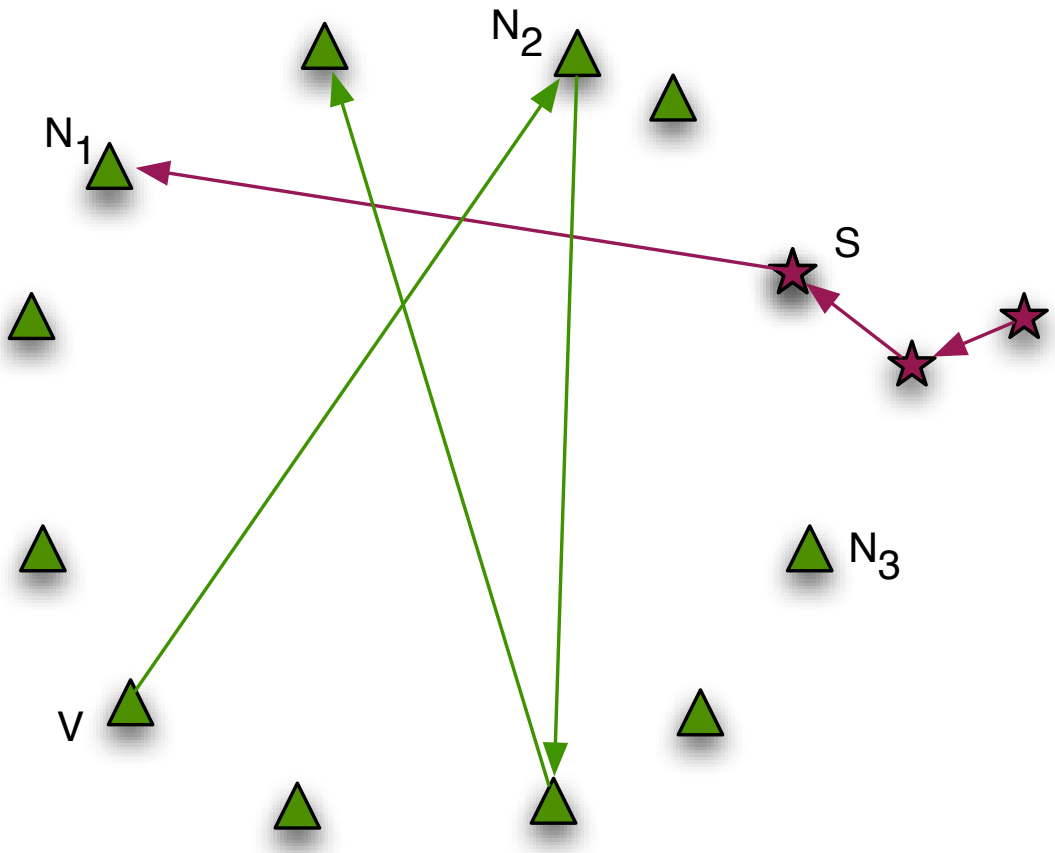
Example



Example



Example



Strengths & Weaknesses

Strengths

- Social-based sybil protection
- Easy deployment

Weaknesses

- No control on the node identifier

Certification Authorities

Principle

- Each member registers with the CA
- The CA checks the identity of newcomers
- A genuine newcomer receives a signed membership certificate

Strengths

- Truly random node identifiers

Weaknesses

- Hard deployment
- Associated cost
- Contrary to P2P philosophy

Combining SybilGuard and CA

Two functionalities in a CA

- Deciding whether to accept the newcomer
- Signing his certificate

Combining SybilGuard and CA

Two functionalities in a CA

- Deciding whether to accept the newcomer
  $\Rightarrow$ SybilGuard on each node (social cost, easy deployment)
- Signing his certificate
  $\Rightarrow$ Distributed certification (truly random node identifiers)

Combination of SybilGuard with Distributed Certification

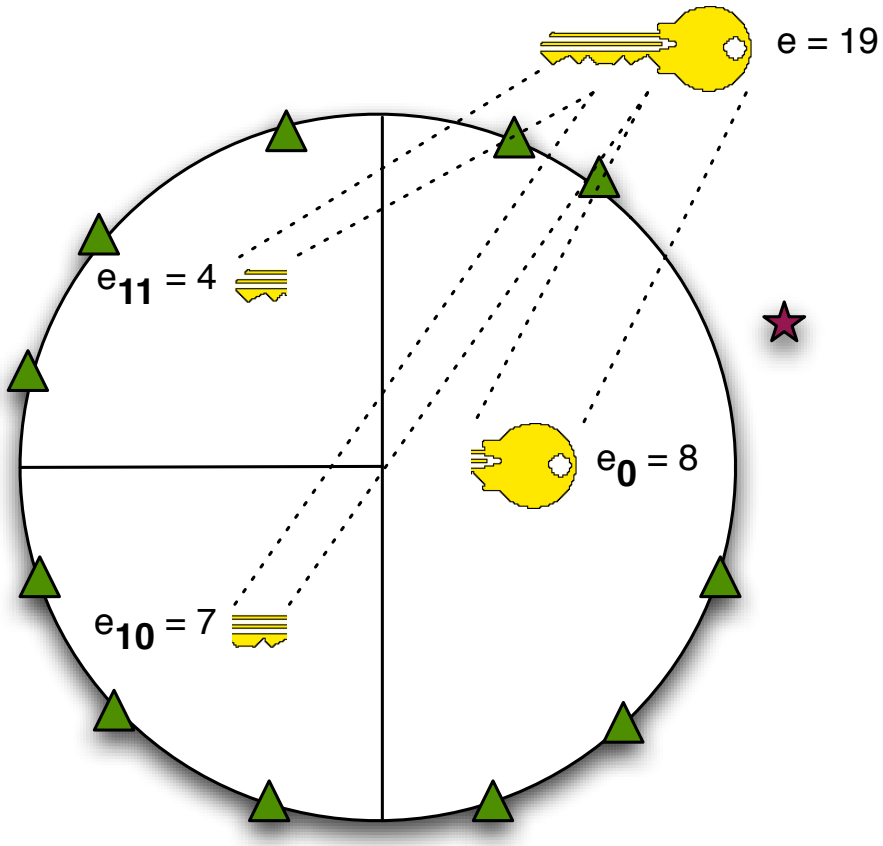
Distributed Admission Control

Principle

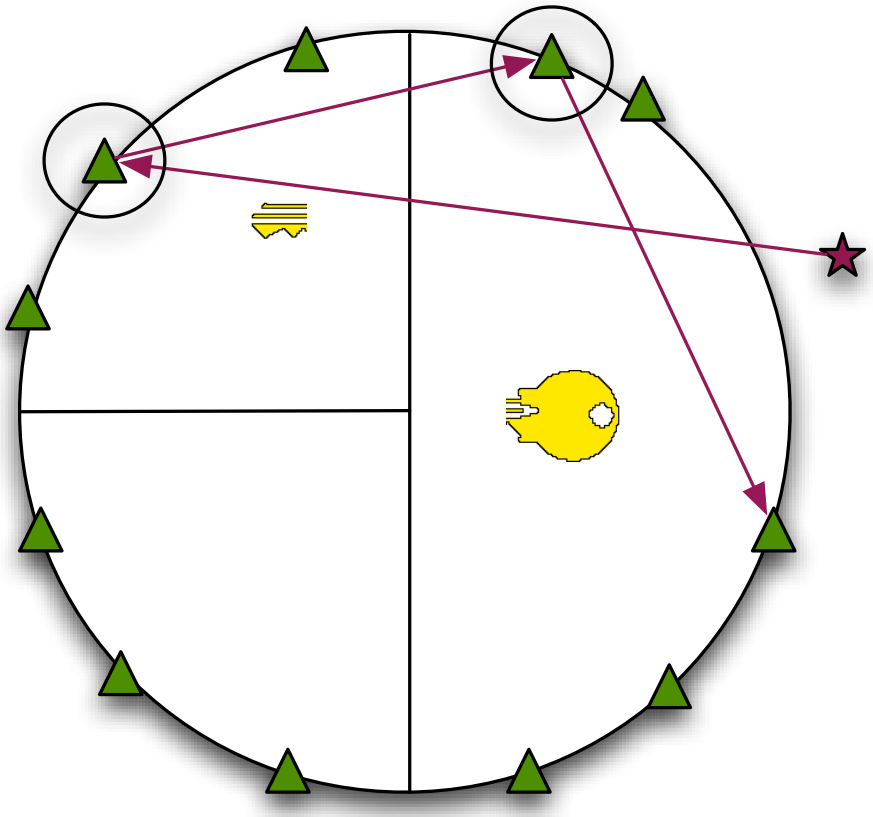
- Membership is proved by a certificate
- Signature of this certificate requires the cooperation of t% of the nodes
- Each node cooperates if its SybilGuard detects the newcomer as genuine
- Node identifier is derived from the certificate (unpredictable)

$\Rightarrow$ A newcomer obtains his certificate only if t% of the nodes detect him as genuine

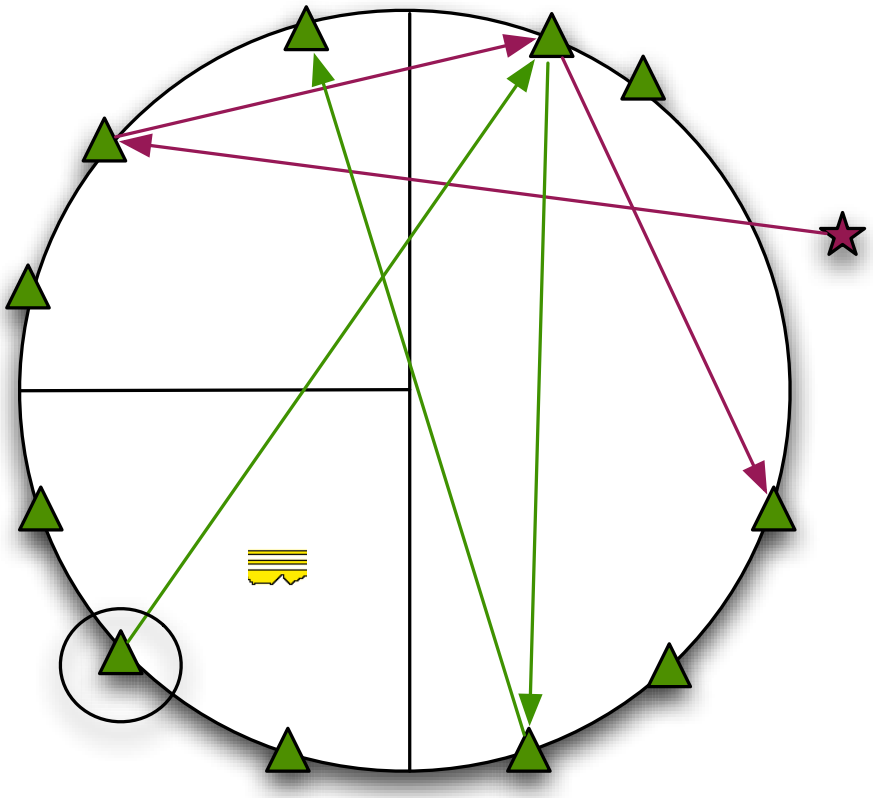
Example



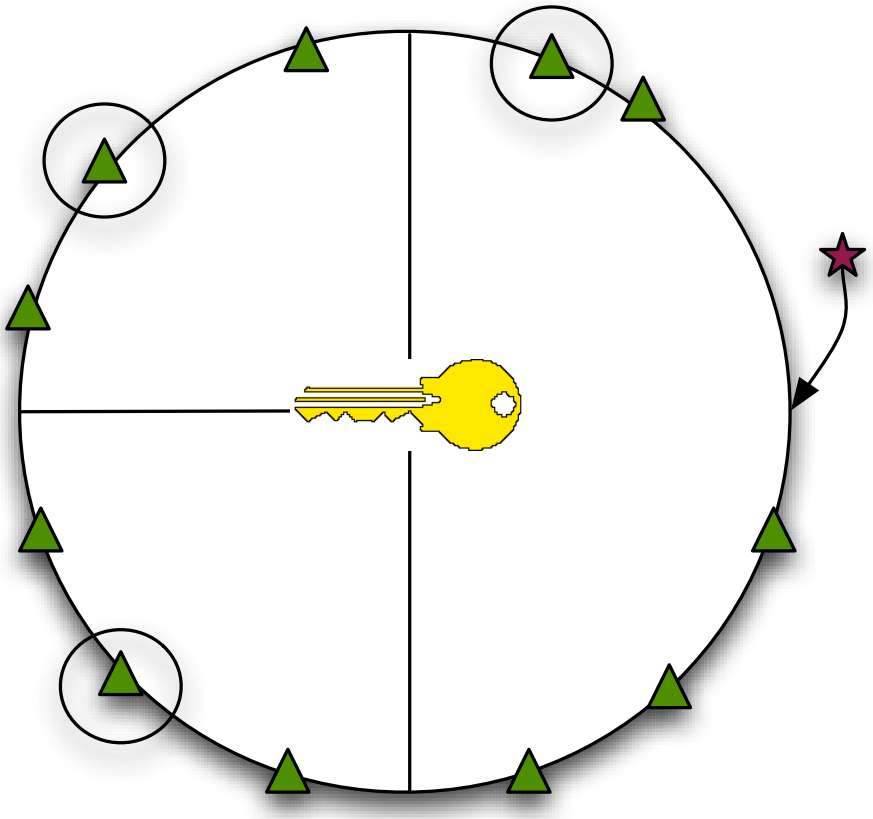
Example



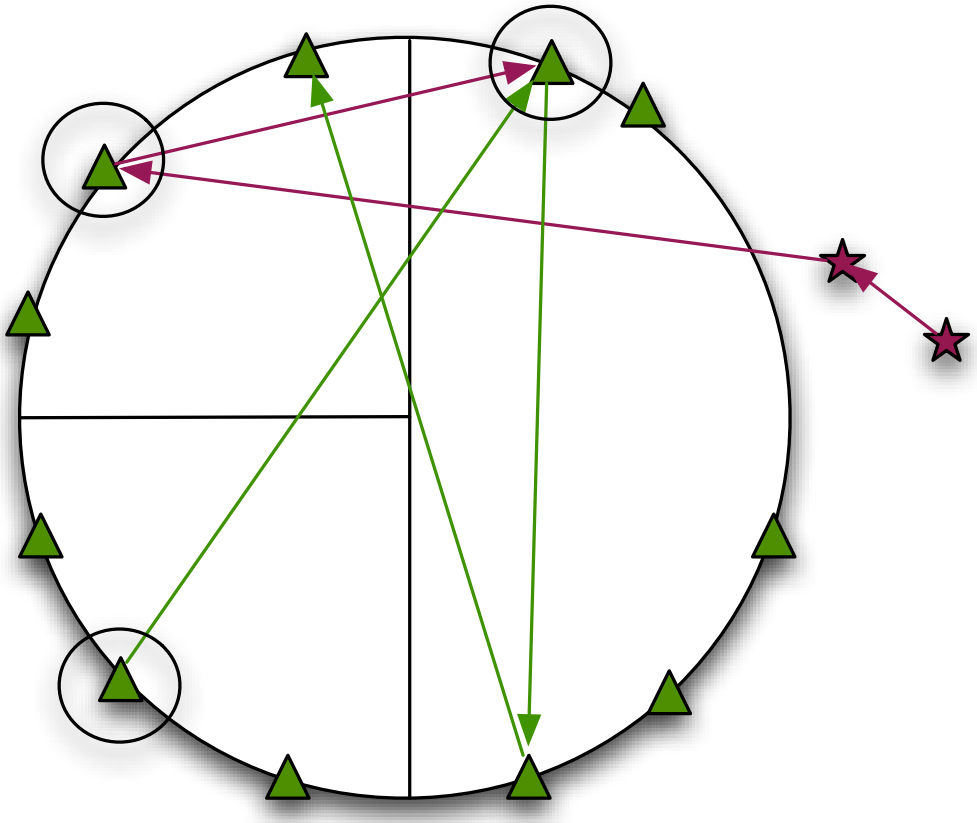
Example



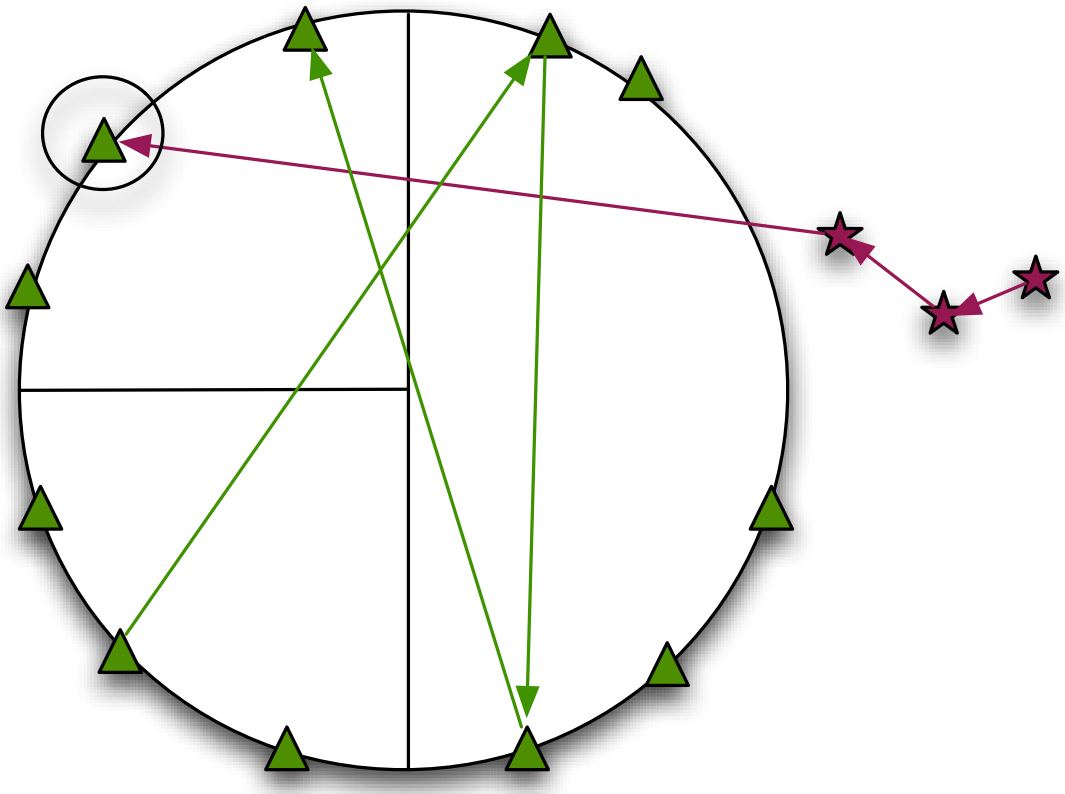
Example



Example



Example



Results

10,000 nodes, SybilGuard alone

- $w = 45$ to accept every honest node
- 67 sybil nodes per attacker

10,000 nodes, SybilGuard with Distributed Certification

- $w = 37$ to accept every honest node
- 38 sybil nodes per attacker

Conclusion and Future Work

Conclusion

- Social-based sybil protection
- Random node identifiers
- Less sybil nodes than SybilGuard alone
- Theoretical analysis with constant degrees

Future Work

- Theoretical analysis with distribution of degrees
- Optimizations and deployment on PlanetLab
- Simulations on real social networks ?

A Sybil-Resistant Admission Control Coupling SybilGuard with Distributed Certification

François Lesueur, Ludovic Mé, Valérie Viet Triem Tong
firstname.lastname@supelec.fr

Supélec, SSIR Group (EA 4039)

COPS, June 2008
Rome, Italy