



Informant: Detecting Sybils using Incentives

N. Boris Margolin
Brian Neil Levine

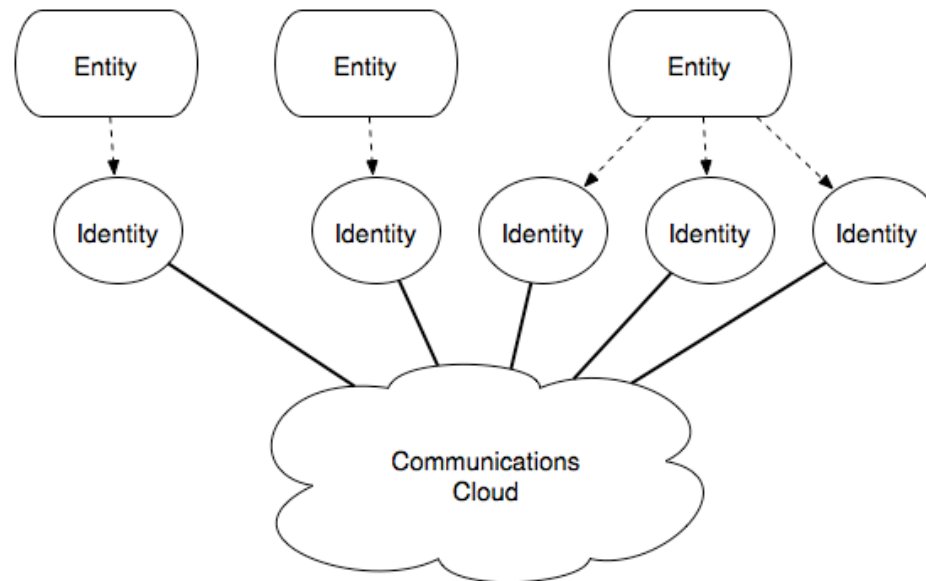
Dept. of Computer Science
University of Massachusetts, Amherst

NSF Grant 0133055



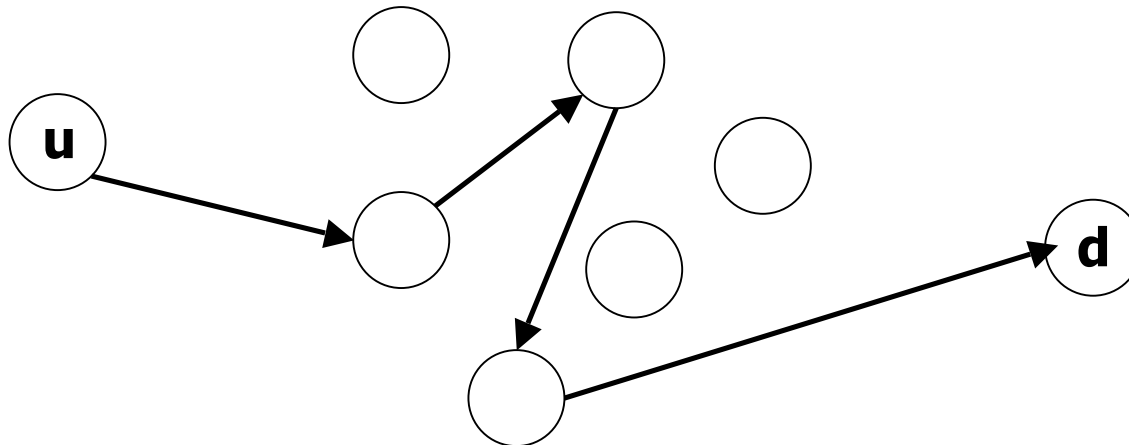
The Sybil Attack

- A single *Entity* uses many *Identities* in an attack
 - Very difficult to deduce the Entity
- (Douceur 2002)



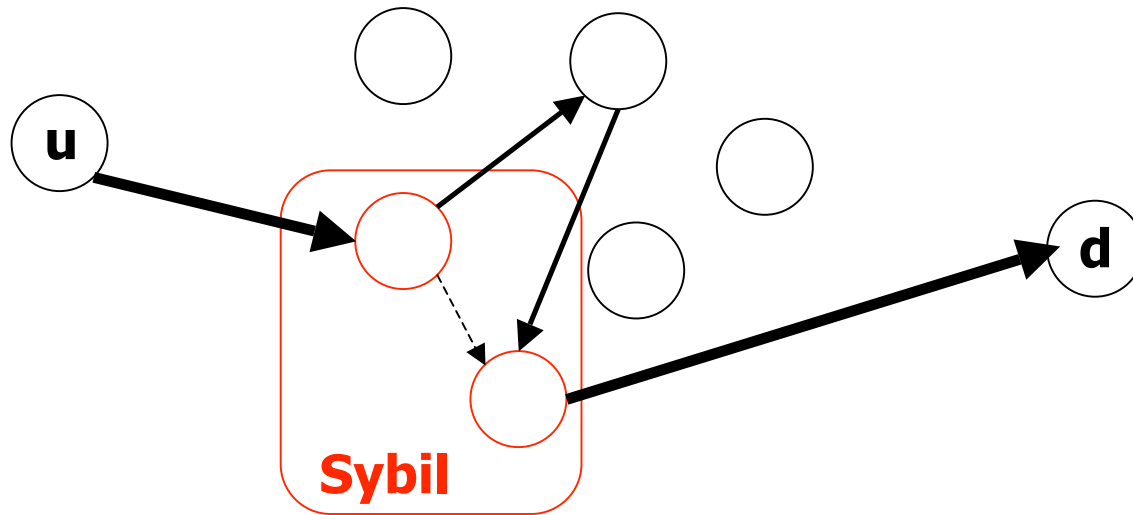
Example Scenario: TOR

- TOR: Onion routing, low latency anonymity
- TOR splits routing responsibility between nodes
- To ensure anonymity, nodes must be independent
 - *An Analysis of the Degradation of Anonymous Protocols* (Wright 2002)



Example Scenario: TOR

- A Sybil can break anonymity with as few as 2 nodes
 - First and last
 - Timing attacks to correlate messages
- More nodes lead to quicker breaks
 - Sybil nodes more likely as first and last hop



Sybil Prevention vs. Sybil Detection

- How do we deal with Sybil attacks?
- Prevention: only allow 1 identity per entity
 - Prevention is difficult (Douceur 2002)
 - Computational challenges, etc., usually ineffective
 - PKI works but is cumbersome and expensive
- Detection: notice that identities belong to a Sybil
 - Difficult by definition
 - Layered defense: shows problems, allows recovery
 - May be cheaper than a PKI

Related Work

- Detection on the link layer
 - Mac addresses
 - *Detecting the Sybil Attack in Ad hoc Networks* (Piro 2006)
 - Geographic position
 - Radio information
 - *The Sybil Attack in Sensor Networks: Analysis and Defenses* (Newsom 2004)
 - TCP timestamps & clock skew
 - *Hot or Not: Revealing Hidden Services by their Clock Skew* (Murdoch 2006)
 - & others...
- Our approach: Incentives
 - Sybils' economic incentives differ from ordinary users'
 - Our protocol exposes these differences

Outline

- Problem Statement
 - **Simple Example: Trust Game**
 - Participant's incentives
 - Sybil Game: more sophisticated game
 - Informant protocol
 - Conclusions
-

Trust Game: Introduction

- Simple approach to Sybil identity detection:

“Are you a Sybil identity?”

- A few problems...
 1. Why should they admit to being in a Sybil?
 - We pay them.
 - Only identities, not entities, revealed; little cost to Sybils
 2. Can we believe claims to be a Sybil?
 3. Will we encourage Sybils to join the application?

Trust Game: Participants

Two identities in the application:

- Informant



- Makes a Sybil claim, presenting another Sybil identity

- Target

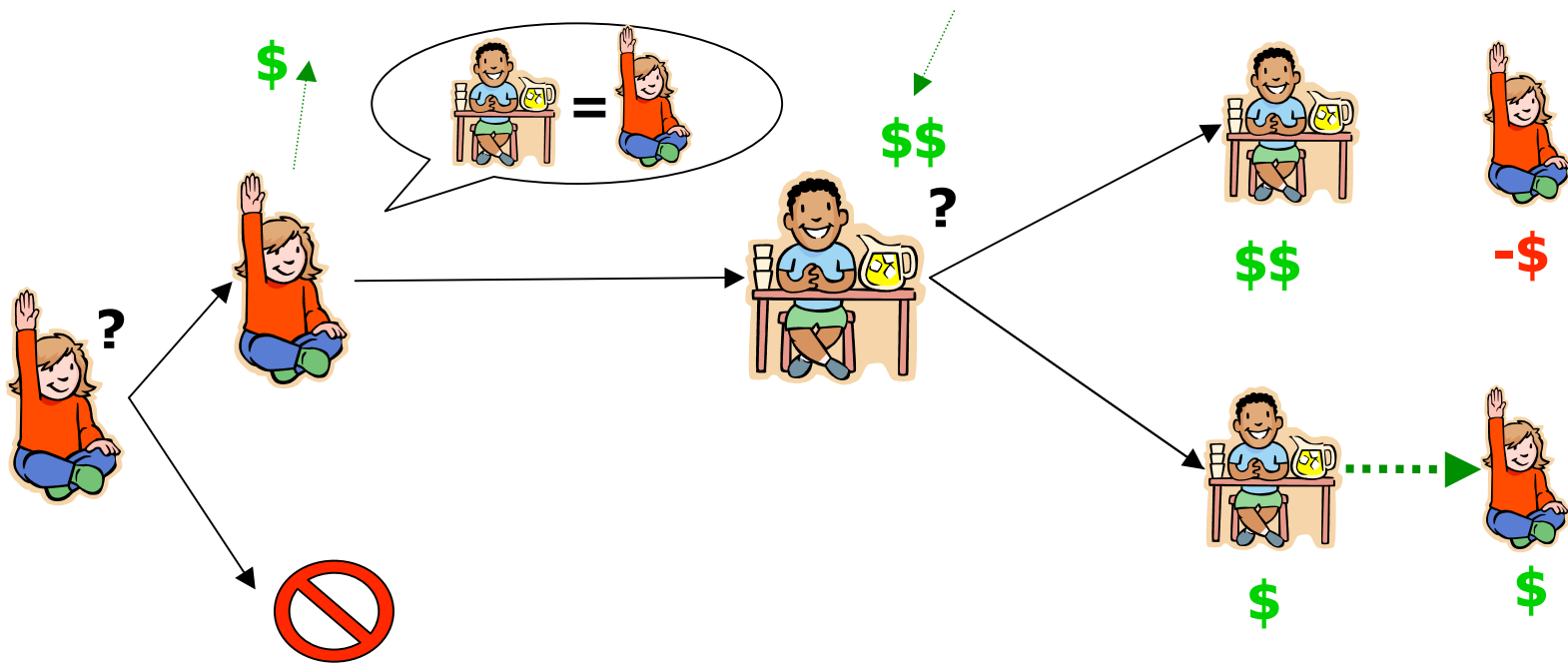


- The claimed other Sybil identity

- Goal: Informant makes a Sybil claim iff it is a Sybil

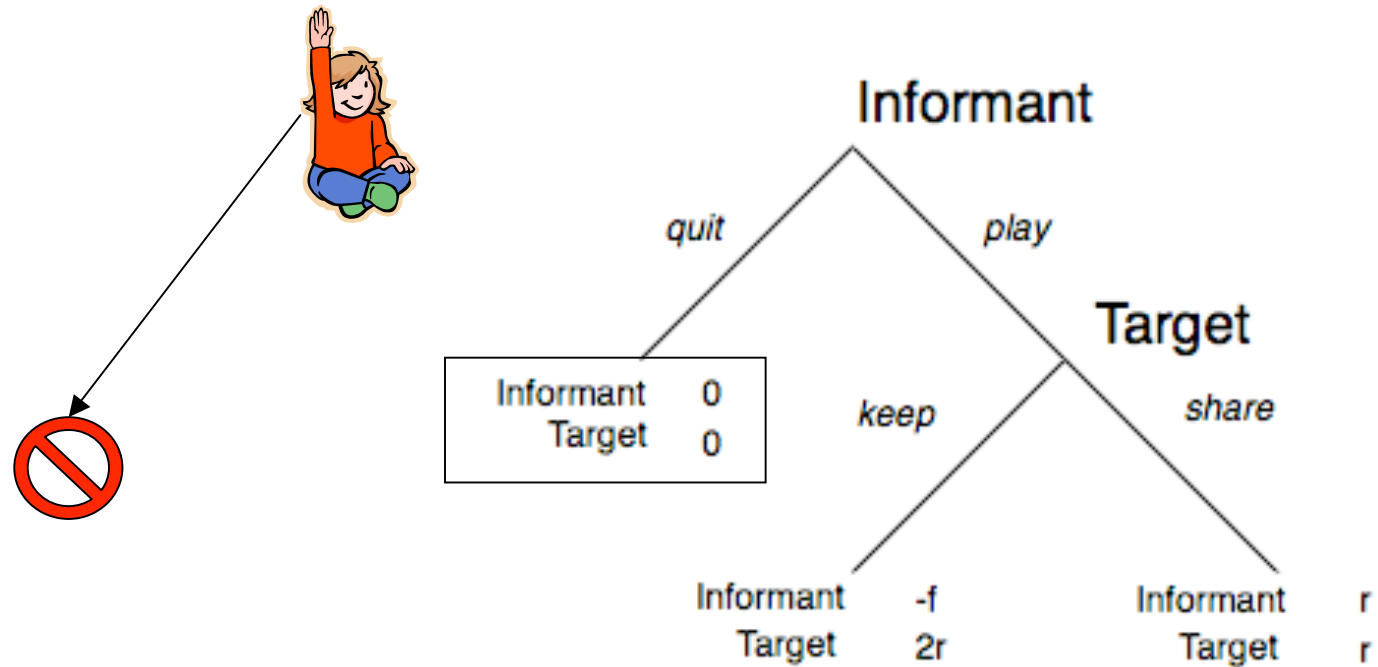
Trust Game: Basic Operation

1. Informant *may* make a claim of Sybil status by:
 1. Paying a security deposit, and
 2. Naming a TargetOr it may do nothing.
2. Target is paid a reward (only if it was named.)
3. Target may share this money, or keep it all.



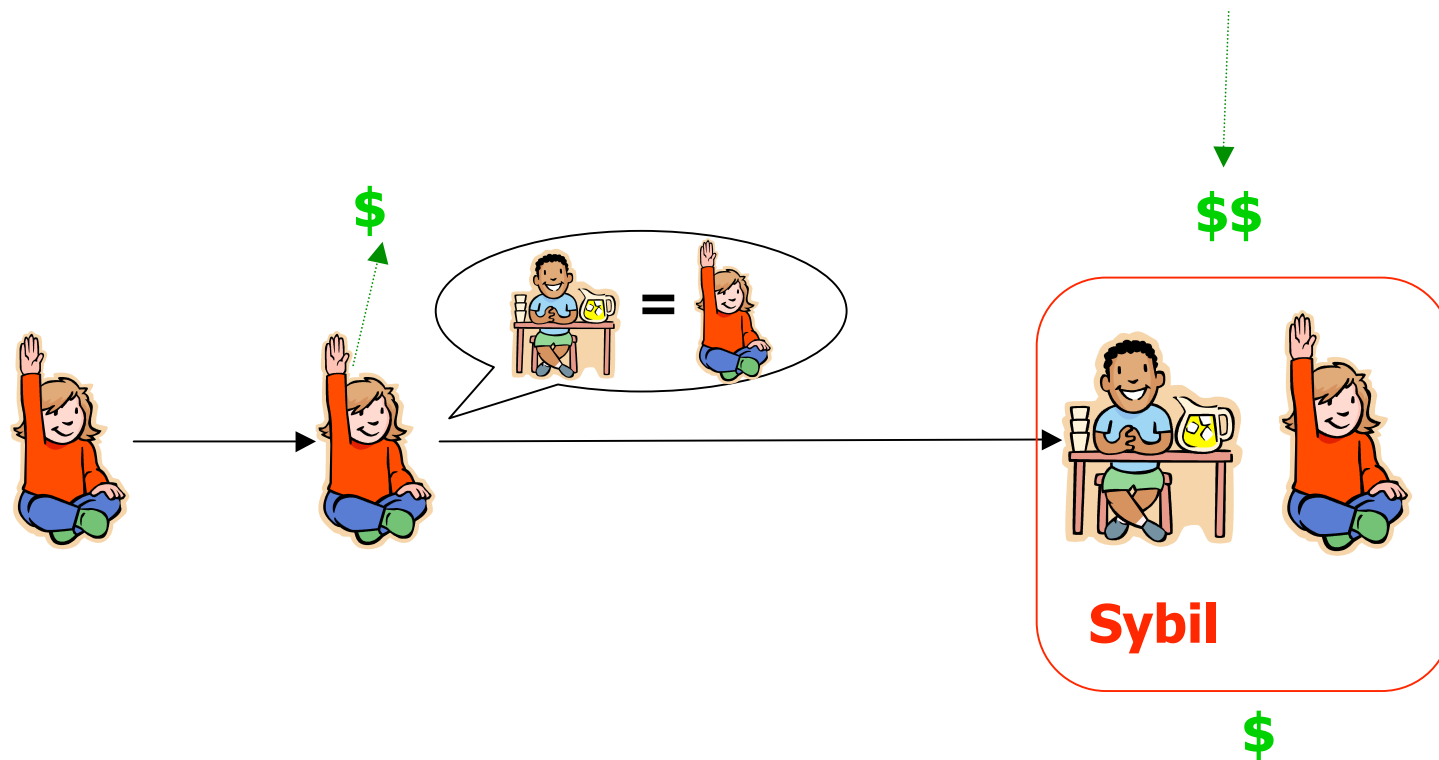
Trust Game: Non-Sybil Case

- Target will not share the money...
- So the Informant will not name a target



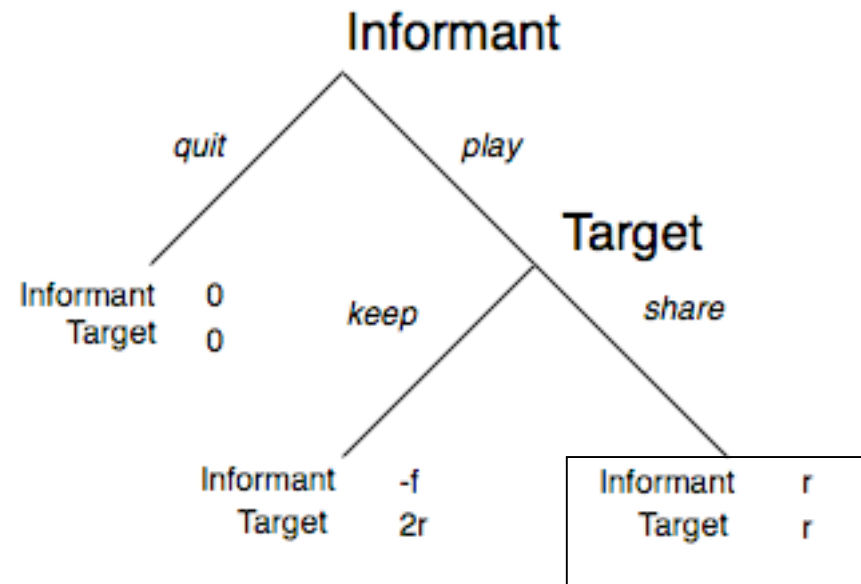
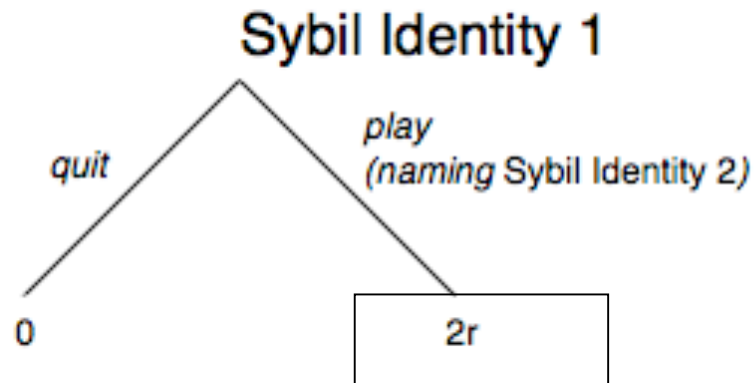
Trust Game: Sybil case

- What if the Target and Informant are in a Sybil?
 - Target always “shares” the money
 - So the Informant profits from naming the target



Trust Game: Sybil case

- Sybil's view of the game:



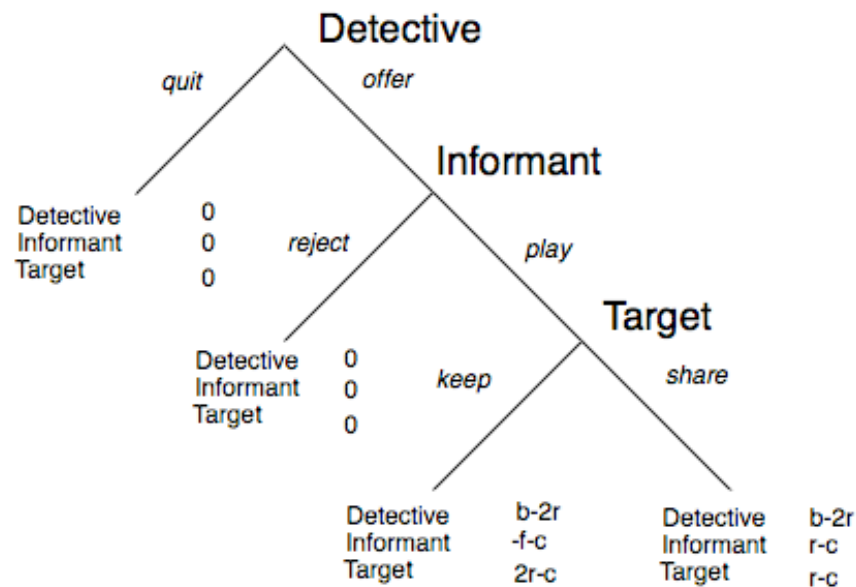
Trust Game vs. Sybil Game

- Trust Game limitations
 - Sybils may have some cost for revealing themselves
 - We need someone who to pay the reward
- Sybil Game addresses these issues
 - Sybil has an opportunity cost
 - Adds a Detective who:
 - Takes the security deposit
 - Offers the reward



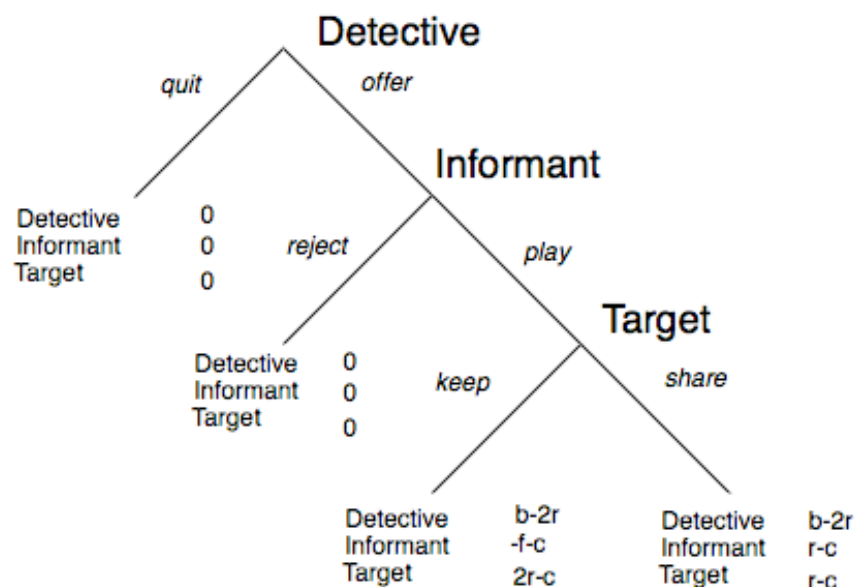
Sybil Game

- Detective, Informant, and Target
 - b: benefit of learning of Sybils
 - f: entry fee
 - c: opportunity cost of Sybil claims
 - r: reward



Sybil Game: Optimal Strategies

- Detective: Offer the game if reward paid is less than value of Sybil information
- Informant: Play if a Sybil, and reward exceeds opportunity cost in revealing
- Target: always keep reward



Informant Protocol

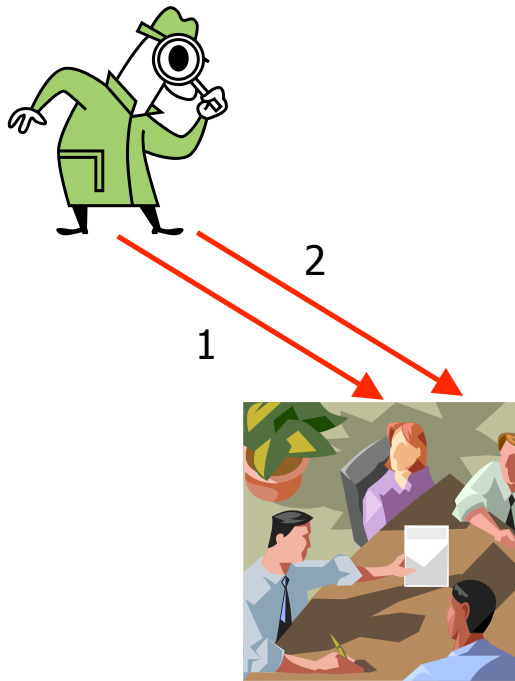
- Iterative version of the Sybil Game
 - Reverse Dutch auction
 - Minimizes the reward that the detective pays
 - Serialize Sybil revelations
 - Detective can learn of larger Sybils

Informant Requirements

- Public/private keys for each identity
- Broadcast mechanism within application community
- Trusted Detective
 - Otherwise, the Detective can steal Informant's money
 - Detective not anonymous, can be held responsible
- Electronic cash
- Recurring entry fees
 - payment each round of an application
 - Can be cash, CAPTCHAs, tokens

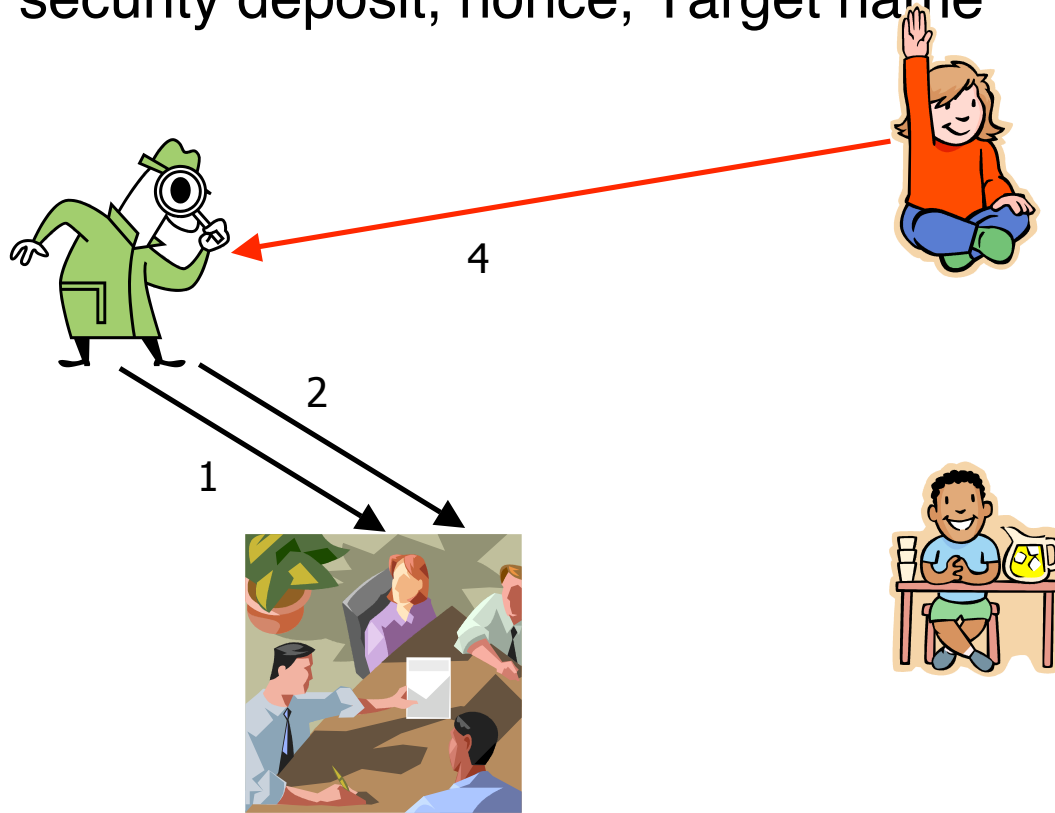
Steps in Informant

1. Detective announces Informant run
 - Auction id, time between rounds, security deposit
2. Detective announces Informant round
 - reward, round nonce



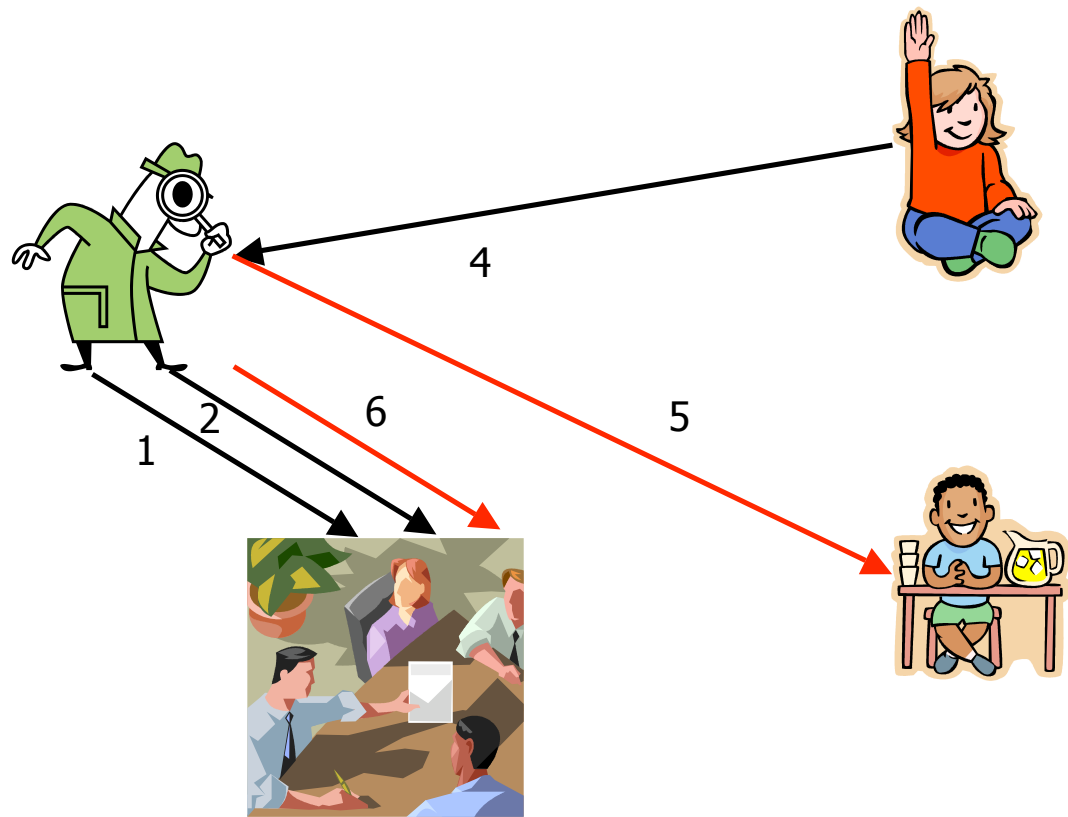
Steps in Informant

- 3. If no responses within τ seconds, go to next round
 - increment reward by a small amount; quit if at max
- 4. Detective receives a response from an Informant
 - security deposit, nonce, Target name



Steps in Informant

- 5. Pay the named target the reward and deposit
 - 6. Announce common control of Informant & Target
- End of Protocol



Opportunistic Sybils

- Goal is to detect Sybils
- But some could join just for the reward!
- Per-round application entry fee must be higher than Informant reward
 - Can amortize, offer Informant infrequently.
- Only malicious Sybils will join
 - Already benefit from making a Sybil attack
 - Reward just increases the benefit
 - Could still encourage slightly malicious

Setting the values properly

- Determined Sybils require high rewards
- Detective finds as many as she is willing to pay for
- Balance of several values required:

amortized reward $<$

application entry fee $<$

legitimate users' application valuation

Sybil's opportunity cost $<$

non-amortized reward $<$

Detective's valuation of Sybil knowledge

Miscellaneous Issues

- Are Sybil attackers rational?
 - goals are neither rational or irrational, behavior may be
 - Some evidence that p2p app. participants are rational
 - Shneidman & Parkes 2003
- Legal
 - Informant only works if Sybils don't face prosecution
- Collaborators vs. Sybils
 - Not distinguished by this protocol
 - Collaborators' incentives are different than Sybils

Summary

- Detect Sybils with observed behavior and incentives
- Informant protocol
- Beware of opportunistic Sybils
- Limitations:
 - Requires electronic cash
 - Trusted Detective
 - Detecting some Sybils may be too expensive
- Informant details and proofs of optimal strategies are in the paper.