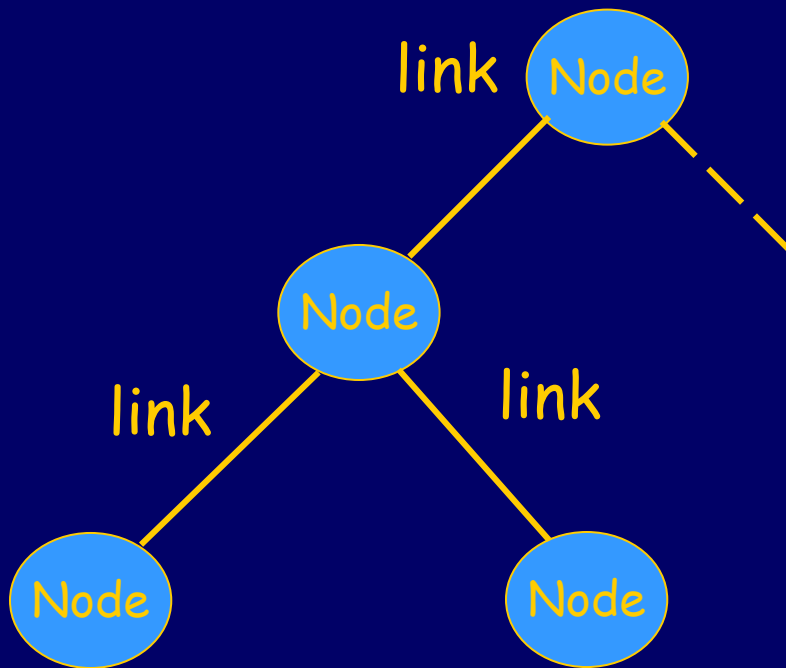


Distributed Mechanism Design and Computer Security

John Mitchell Vanessa Teague
Stanford University

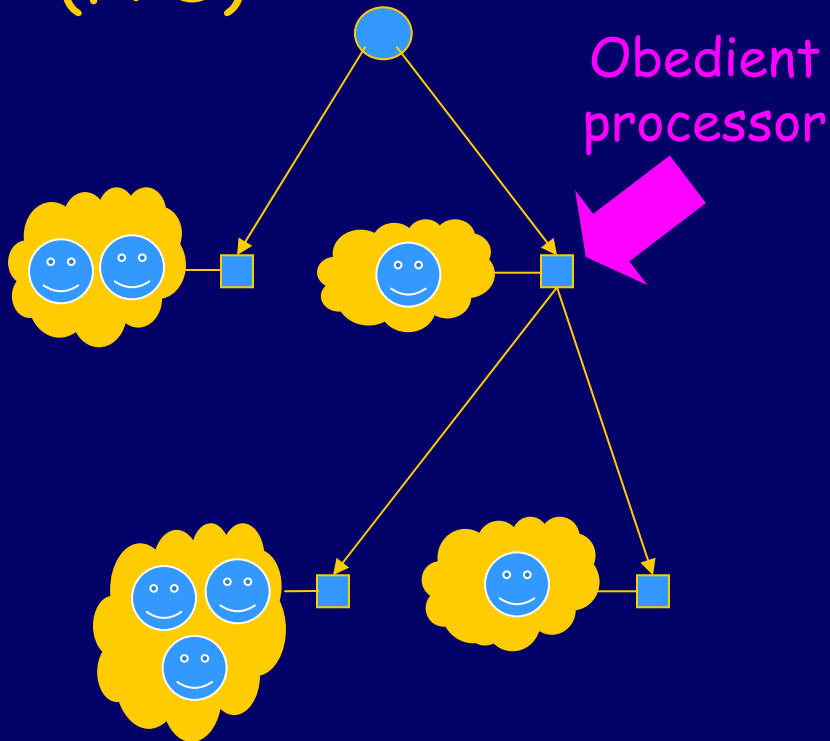
Multicast cost sharing



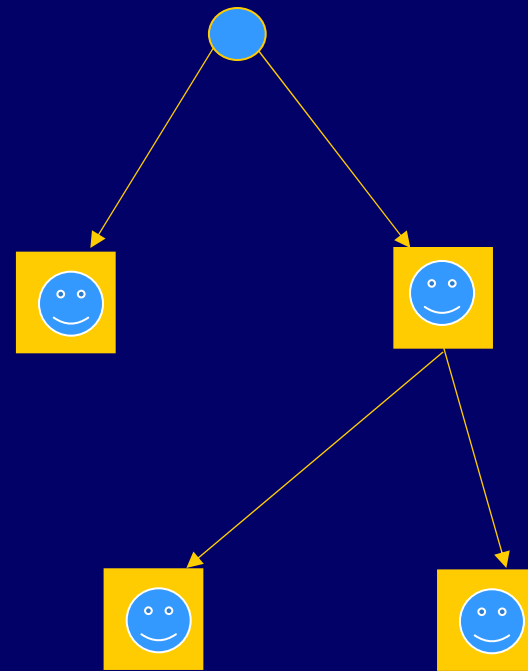
- Distribute some good
- Each node has some utility for the good
- Each link has some cost
- Which nodes get the transmission?

Two models

◆ Tamper-proof nodes (FPS)



◆ Strategic nodes



Acknowledgements: J. Feigenbaum, R. Sami, A. Scedrov ...

FPS Pricing Mechanism

◆ Motivation

- Want agents to reveal true utility so we can decide which agents get transmission

◆ Distribution

- Transmission goes into every subtree with non-negative welfare (utilities minus link costs)

◆ Payments

- If agent doesn't receive the good, it pays nothing
- If agent receives the good, it pays:
the minimum bid needed to get the transmission,
given the other players' bids

This is a VCG mechanism

Strategyproof and Efficient

◆ Efficient (max welfare) by construction

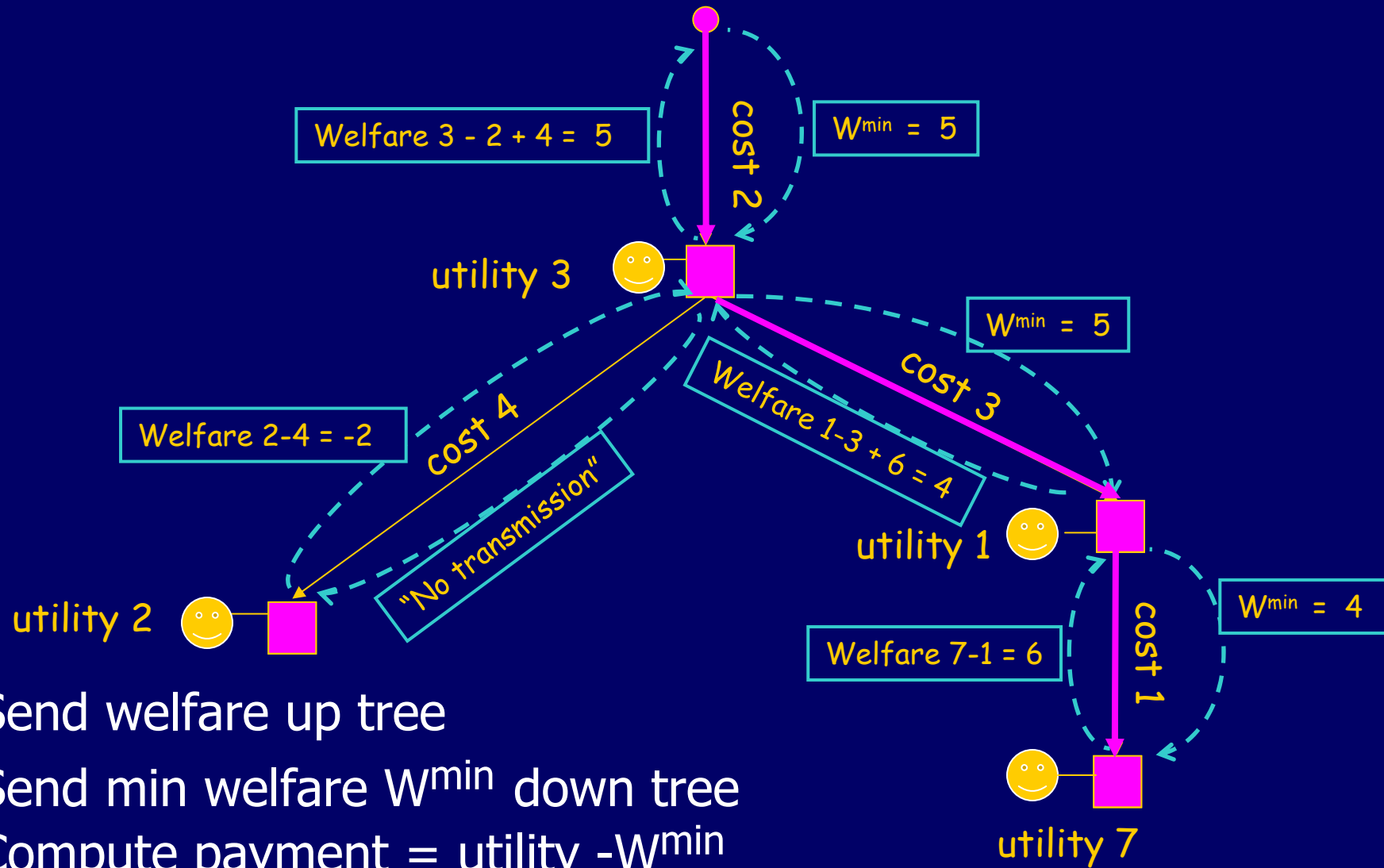
- Add omitted subtree \rightarrow decrease welfare
- Remove routed subtree \rightarrow decrease welfare

This argument assumes agents tell truth

◆ Agent can bid true utility

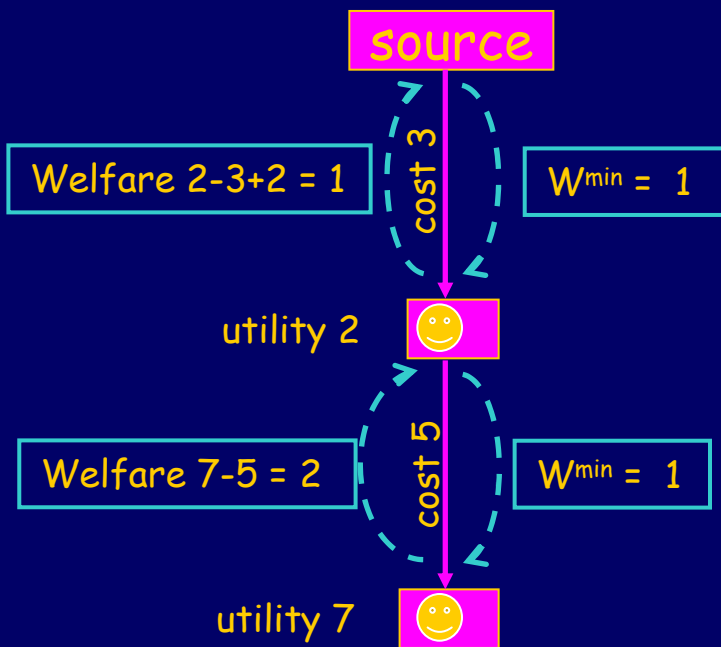
- Payment is independent of bid, given outcome
- Bid more than utility \Rightarrow
 - doesn't help, or pay too much
- Bid less than utility \Rightarrow
 - doesn't help, or don't get the transmission

Distributed implementation (tamper-proof nodes model)



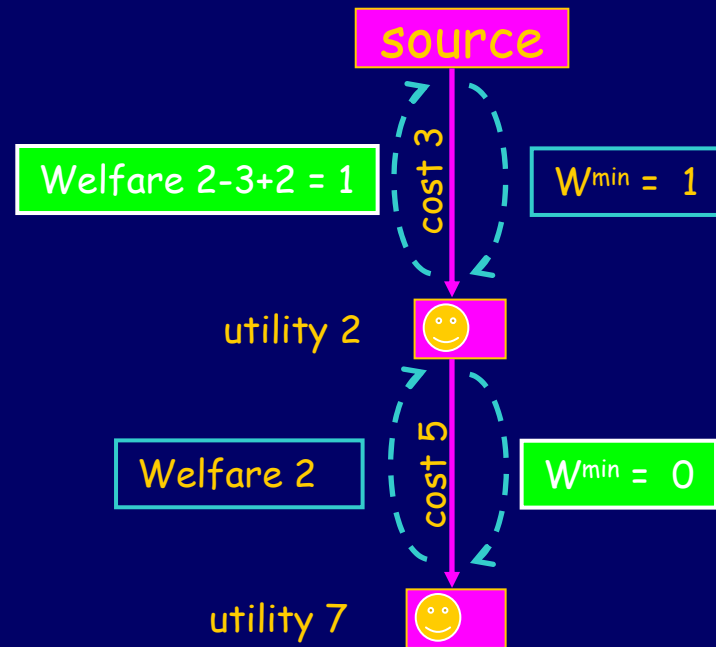
Node can cheat its children (strategic nodes model)

The truth



Parent pays 1
Child pays 6

The cheat



Parent pays 0
Child pays 7

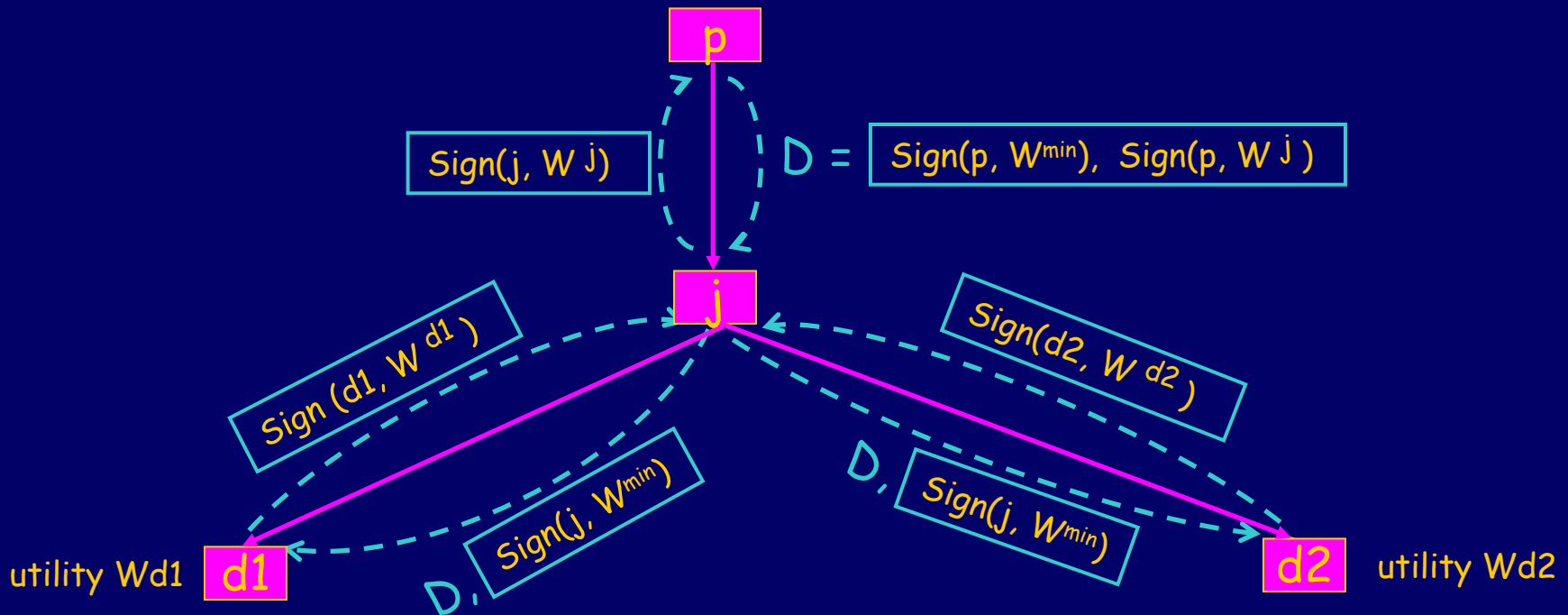
Child can't see that parent doesn't pay

Authenticated protocol

- ◆ Assume public-key infrastructure
 - Each node has verifiable signature
- ◆ Augment messages
 - Sign data from FPS algorithm
 - Parent returns signed W to child
- ◆ Nodes send payment, proof to content source
 - Proof: signed data, payment calculated correctly
 - If nobody cheated, transmission is sent
 - Otherwise, cheater is fined; no transmission
- ◆ Make punishment high enough so benefit of cheating is negative

Preventing mischief

Node J passes on parent's data



Children verify j 's calculation of W^{\min}

Security in FPS model

◆ Let the adversary be node A

◆ Lemma

- Case 1: A wasn't going to receive the transmission by bidding zero
 - then it can't reduce the group welfare by more than it pays
- case 2: A was going to receive the transmission by bidding zero
 - then it can't reduce the group welfare

Security of anti-mischief protocol

- ◆ Assume malicious node has honest neighbours
- ◆ Theorem: Security "Almost as good" as in FPS model
- ◆ Denial-of-service attacks easy
 - Don't send any messages, so protocol doesn't terminate
 - Detected cheating stops the protocol

Conclusion

- ◆ Pricing function provides incentive
- ◆ Distributed algorithm computes price
- ◆ Techniques to encourage compliance
 - Nodes save signed confirmation of msgs
 - Randomized auditing incents compliance
- ◆ Security against irrational agent
 - Close to model with tamper-proof algorithm