Optimal Smart Contracts with Costly Verification

Akaki Mamageishvili and Jan-Christoph Schlegel

P2PFISY, Frankfurt
July 26, 2019

Problem

Designing self-enforceable contracts

Smart contracts with deposits

Additional transaction (opportunity) costs

Careful analysis needed, e.g. we can't punish misbehavior too much

Example

A seller and a buyer

One item (file)

Buyer's valuation for item is higher than the seller's

Seller can send the item to buyer off-chain

(Abstract) costly verification procedure

Mechanism One: Seller-Only Communication

Seller sends item to buyer

Seller reports the status

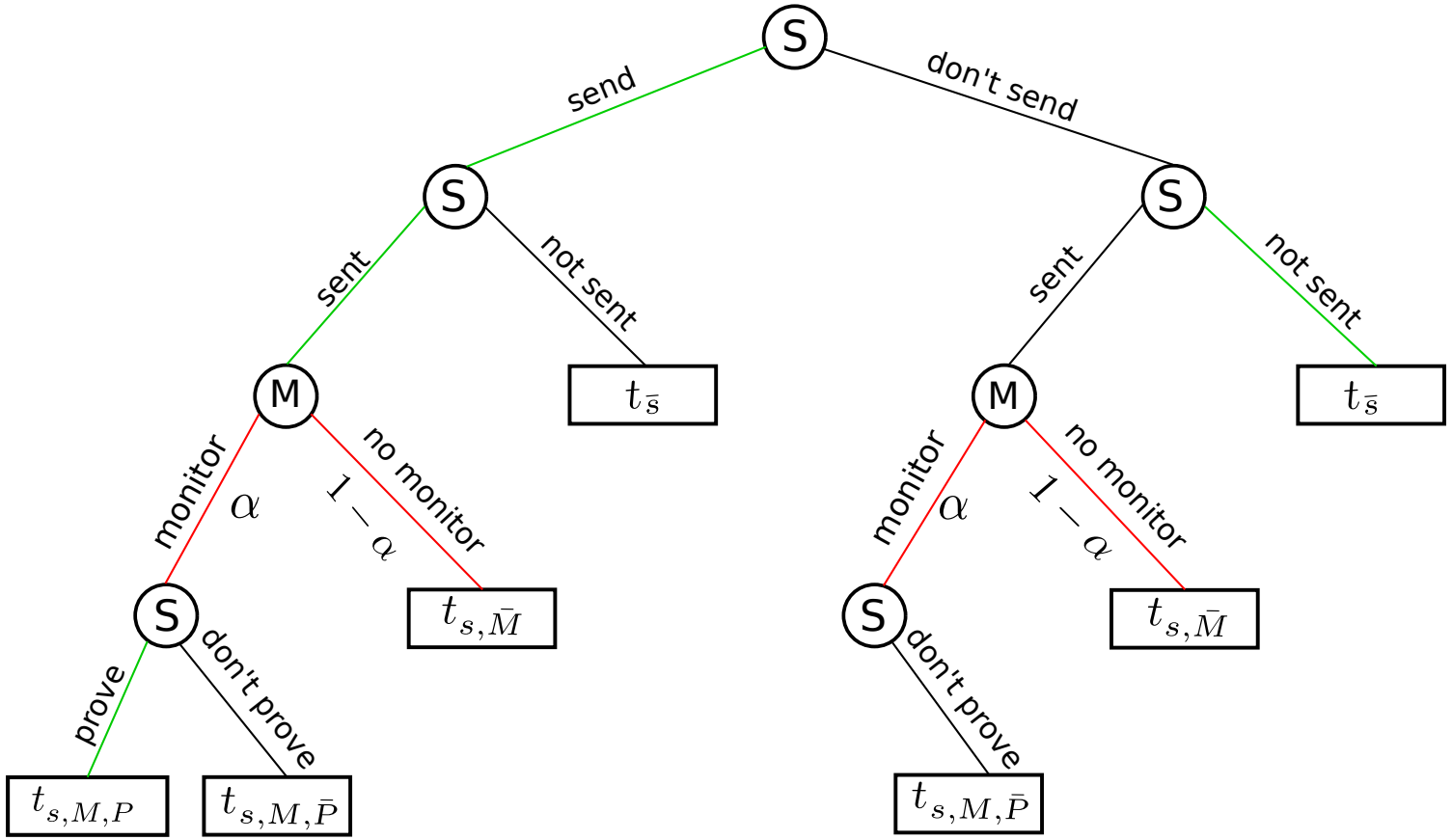
Contract asks seller to provide a proof with some probability

If monitoring does not happen, transfers are realized

If monitoring happens, seller provides a proof if possible

Transfers are realized

Mechanism One: Seller-Only Communication



Mechanism Two: Buyer-Seller Communication

Seller sends item to buyer

Buyer reports the status

If buyer says received, transfers are realized

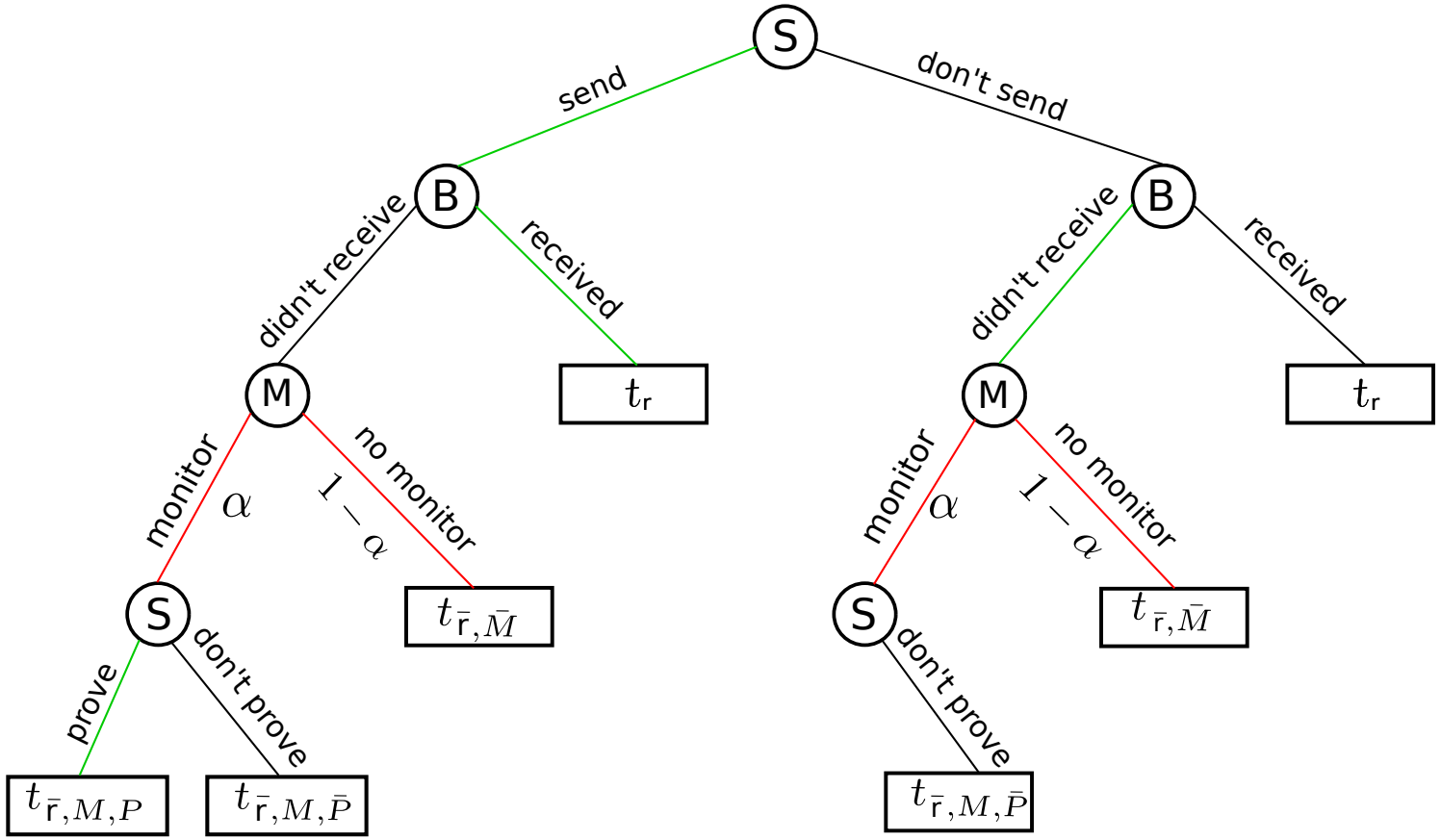
If buyer says he has not received, contract asks seller to provide a proof with some probability

If monitoring does not happen, transfers are realized

If monitoring happens, seller provides a proof if possible

Transfers are realized

Mechanism Two: Buyer-Seller Communication



Game Theoretical Approach

Incentive compatibility constraints

Individual rationality constraints

Honest behavior should correspond to (subgame-perfect) Nash equilibrium

Gains from trade is maximized

Opportunity Costs Matter

In mechanism one, optimal monitoring probability depends on discount factor

In mechanism two, monitoring probability should be higher than a certain threshold

Mechanism two dominates mechanism one

Possible Extensions

We consider risk neutral players

One could consider risk-averse players, e.g. insurance contracts

Other types of problems and optimal mechanisms with self-enforceable contracts

Thank You!

Questions?

Suggestions?