Tight Incentive Analysis on Sybil Attacks to Market Equilibrium of Resource Exchange over General Networks

Yukun Cheng[1], Xiaotie Deng[2], Yuhao Li[2], Xiang Yan[3]

[1]Suzhou University of Science and Technology, [2]Peking University, [3]Shanghai Jiao Tong University

ykcheng@amss.ac.cn, {xiaotie,yuhaoli.cs}@pku.edu.cn, xyansjtu@163.com

A Resource Exchange Model

Let's consider a P2P resource exchange system, which is modeled as an undirected graph $G = (V, E)$ with weight profile $\boldsymbol{w}$.

1. vertex (player) $v \in V$ represents a peer;
2. $w_v : V \to R_+$: the amount of divisible resource that agent v owns;
3. $\Gamma(v)$: the neighborhood of agent v;
4. x_{vu}: the amount of resource agent v uploads to its neighbor u;
5. $X = (x_{vu})_{(v,u)\in E}$: the resource allocation.

Given an allocation, the utility of each player is defined as the resources it received, i.e.,

$$U_v(X) = \sum_{u\in\Gamma(v)} x_{uv}.$$

Proportional Response Dynamics and Market Equilibrium

Proportional Response Dynamics [Wu and Zhang, STOC'07].

- At time 0, $x_{vu}(0) = w_v/d_v$.
- $x_{vu}(t+1) = \frac{x_{uv}(t)}{\sum_{k\in\Gamma(v)} x_{kv}(t)} \cdot w_v$.

Market Equilibrium is an important notion for characterizing efficient allocations in exchange economies.

A market equilibrium is a price vector along with allocation $(\boldsymbol{p}, X)$ with the following conditions:

- Market clearance: $\sum_{u\in\Gamma(v)} x_{vu} = w_v$;
- Budget constraint: $\sum_{u\in\Gamma(v)} \frac{x_{uv}}{w_u} p_u \le p_v$;
- Individual optimality: each player is optimally happy for its allocation at the current price. Formally, the solution $X = (x_{vu})$ maximizes utility $\sum_{u\in\Gamma(v)} x_{uv}$ for each player v, subject to $\sum_{u\in\Gamma(v)} \frac{x_{uv}}{w_u} p_u \le p_v$ and $w_u \ge x_{uv} \ge 0$.

Theorem [Wu and Zhang. STOC'07]. The proportional response dynamics converges, and it converges to a market equilibrium.

Bottleneck Decomposition

The market equilibrium can be represented by a combinatorial structure.

Bottleneck Decomposition. For a network $(G; w)$, start with $V_1 = V$, $G_1 = G$, and $i = 1$. Find the maximal bottleneck B_i of G_i and define the neighbor set of B_i in G_i is C_i, i.e., $C_i := \Gamma(B_i) \cap V_i$. Let G_{i+1} be the induced subgraph $G[V_{i+1}]$, where vertex set $V_{i+1} = V_i - (B_i \cup C_i)$. Repeat if $G_{i+1} \neq \emptyset$, and set $k = i$ and stop the procession if $G_{i+1} = \emptyset$. $\mathcal{B} = \{(B_1, C_1), \cdots, (B_k, C_k)\}$ is named as the bottleneck decomposition of G, in which (B_i, C_i) is the i-th bottleneck pair and $\alpha_i = w(C_i)/w(B_i)$ is the α-ratio of (B_i, C_i).

Sybil Attack

Sybil Attack. Consider a network $(G; w)$ and a strategic agent v. When v plays a Sybil attack, it would split itself into m fictitious nodes $\{v^1, \cdots, v^m\}$, and assigns amount w_{v^i} of resource to each node v^i, satisfying $0 < w_{v^i} \le w_v$ and $\sum_{i=1}^m w_{v^i} = w_v$. Each fictitious node may be adjacent to several neighbors of v's, but there are no connection between fictitious nodes.

The resulting network, called a Sybil network, is denoted by $\tilde{G} = (\tilde{V}, \tilde{E})$, in which the fictitious nodes set is $\Lambda = \{v^1, \cdots, v^m\}$. After playing Sybil attack, v obtains new utility, which is the sum of utilities from all fictitious nodes in $\tilde{G}$. The utility of v is defined as $U_v(\tilde{G}; w_{v^1}, \cdots, w_{v^m}, w_{-v}) := \sum_{i=1}^m U_{v^i}(\tilde{G}; w_{v^1}, \cdots, w_{v^m}, w_{-v})$.

Non-Strategyproofness.

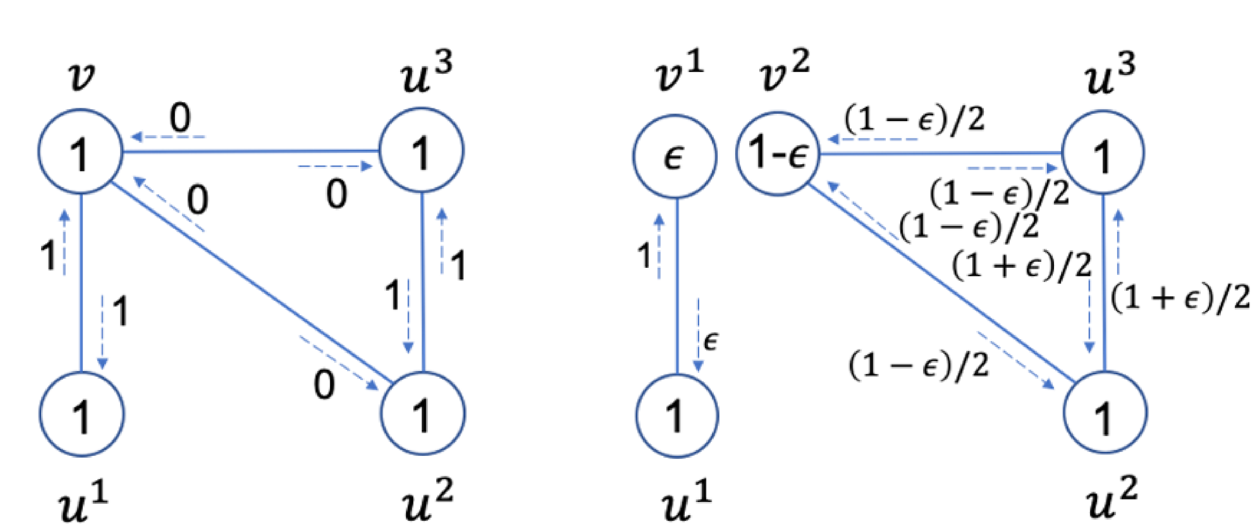

Fig. 1: An example for which a strategic agent could gain more by Sybil attack.

Incentive Ratio

Incentive Ratio [Chen, Deng, and Zhang ESA'11] is a solution concept of approximate strategyproofness, which is defined as the ratio of one's maximum utility by a strategic behavior to the utility when it plays truthfully. A smaller incentive ratio means how close our solution is for an agent not to manipulate the system.

Incentive ratio of agent v under Proportional Response Mechanism against Sybil attack is

$$\zeta_v = \max_{\substack{1\le m\le d_v \\ w_{v^i}\in[0,w_v], i=1,2,\ldots,m \\ \sum_{i=1}^m w_{v^i}=w_v; G'}} \frac{U_v'(G'; w_{v^1}, \ldots, w_{v^m}, w_{-v})}{U_v(G; w)}$$

The incentive ratio of Proportional Response Mechanism in a bandwidth resource sharing game against Sybil attack is

$$\zeta = \max_{\substack{G=(V,E), v\in V \\ w=(w_1,\ldots,w_n)}} \zeta_v.$$

Main Theorem

Main Theorem. The incentive ratio of Proportional Response Mechanism against Sybil attack is exactly two.

The proof is to show that for any network and any strategic agent, by launching Sybil attacks, the incentive ratio is upper bounded by two. Combining with the lower bound, we can get this theorem.

Future Works

While the proof is based on analyzing the bottleneck decomposition, it opens up the possibility may the result be further extended to other market scenarios. The equilibrium solutions always face threats from participating agents' possible strategic behaviors, so it would be of great interest to study the corresponding incentive analysis.