Adversary Games in Secure/Reliable Network Routing

Calinescu, Kapoor, Quinn, Shin
Presented by Gruia Calinescu

Sept. 28, 2011

Outline

1. Motivation
2. 2-player zero-sum game
3. (1 commodity , 1 edge) - game
4. (k commodities , 1 edge) - game
5. (2 commodities , c edges) - game
6. Attacker/designer games with costs
7. Conclusion

Motivation

- Utilizing single paths are prone to failures or malicious attacks.
- The fast growth of the Internet underscores the need for network security.
- Our approach allows to use multiple paths to avoid data stealing, security attacks or eavesdropping.
- Utilizing multiple paths implies minimizing the maximum congestion on the edges.

2-player zero-sum game

2-player zero-sum game requires

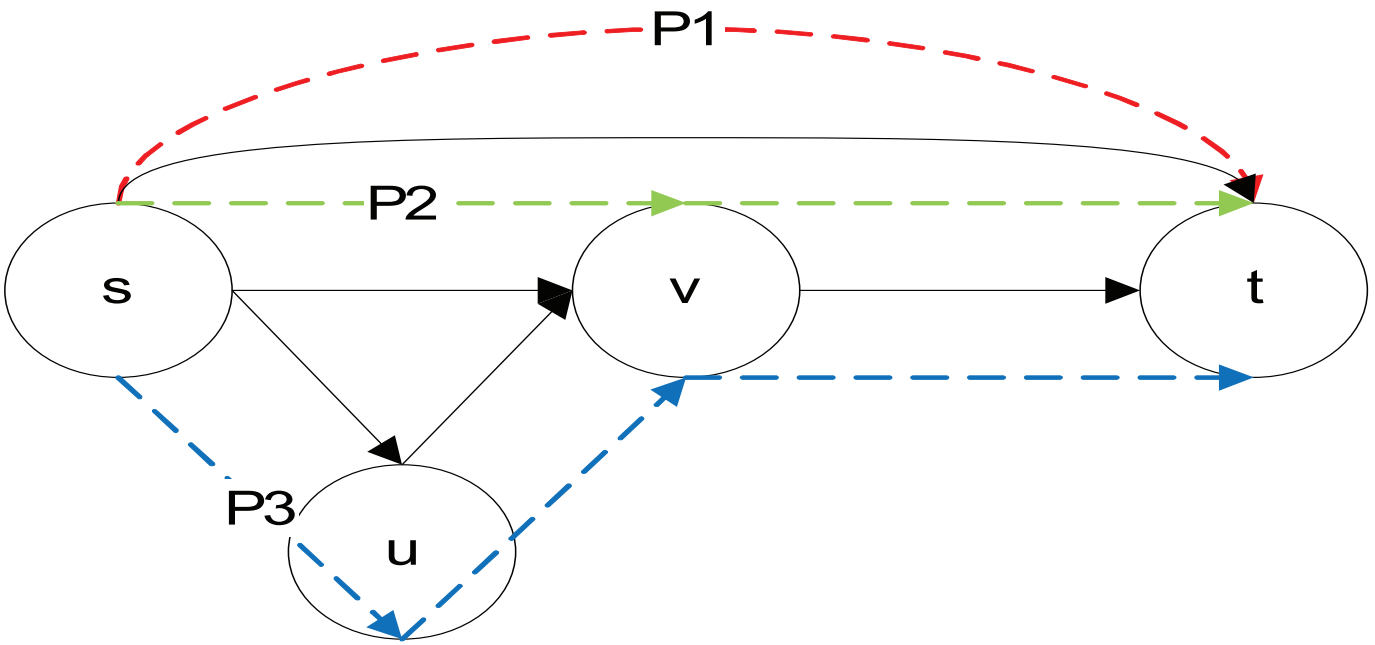
1. 2-players
2. Two sets of strategies, for each player
3. Payoff matrix. One player's payoff is the negation of the other player's payoff.

Network 2-player Zero-Sum $SG(k, c)$

Given graph $G = (V, E)$ and k source-destination pairs (s_i, t_i)

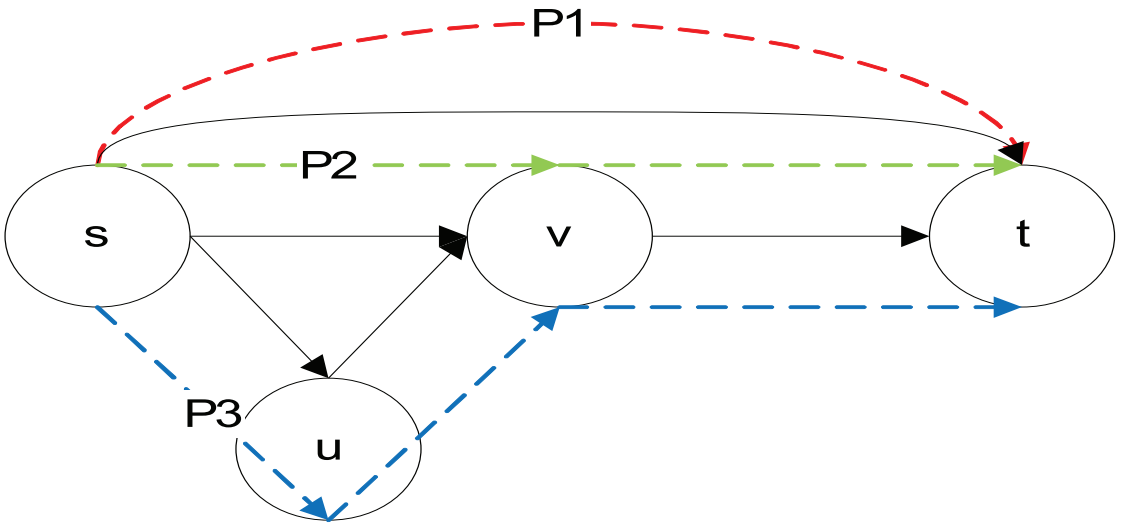
- 2-players: attacker and designer
- Strategies: attacker picks c edges, designer picks k paths, one from each s_i to corresponding t_i
- Attacker's payoff: number of intercepted paths
- Designer payoff: negation of attacker's payoff

$SG(1,1)$ Example with payoff matrix



P \ E	sv	su	uv	vt	st
P_1	0	0	0	0	1
P_2	1	0	0	1	0
P_3	0	1	1	1	0

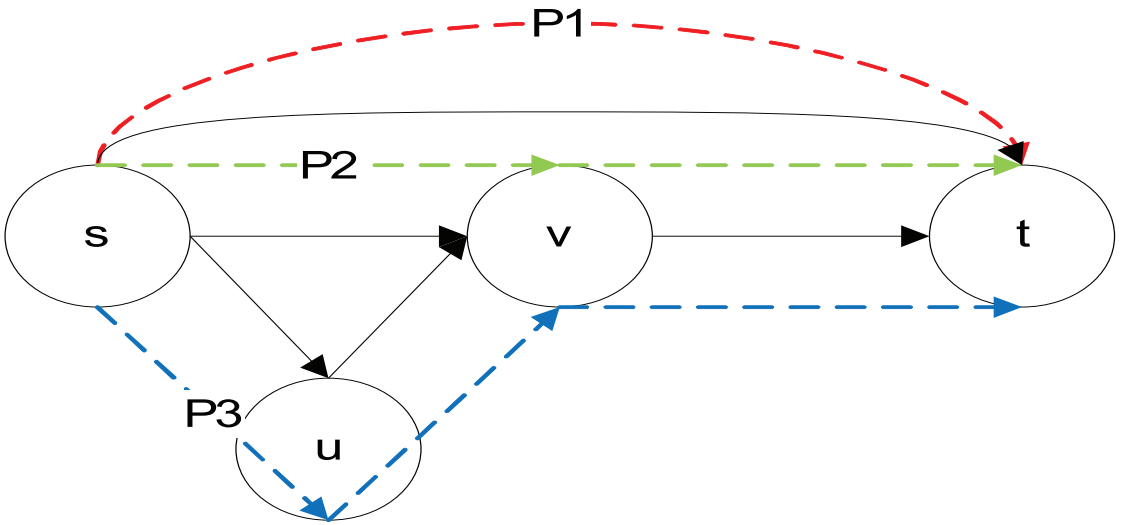
$SG(1,1)$ Pure strategies: no equilibrium



Designer uses P_1, attacker $st \implies$ designer switches to (say) P_2

Designer uses P_2, attacker $st \implies$ attacker switches to (say) vt

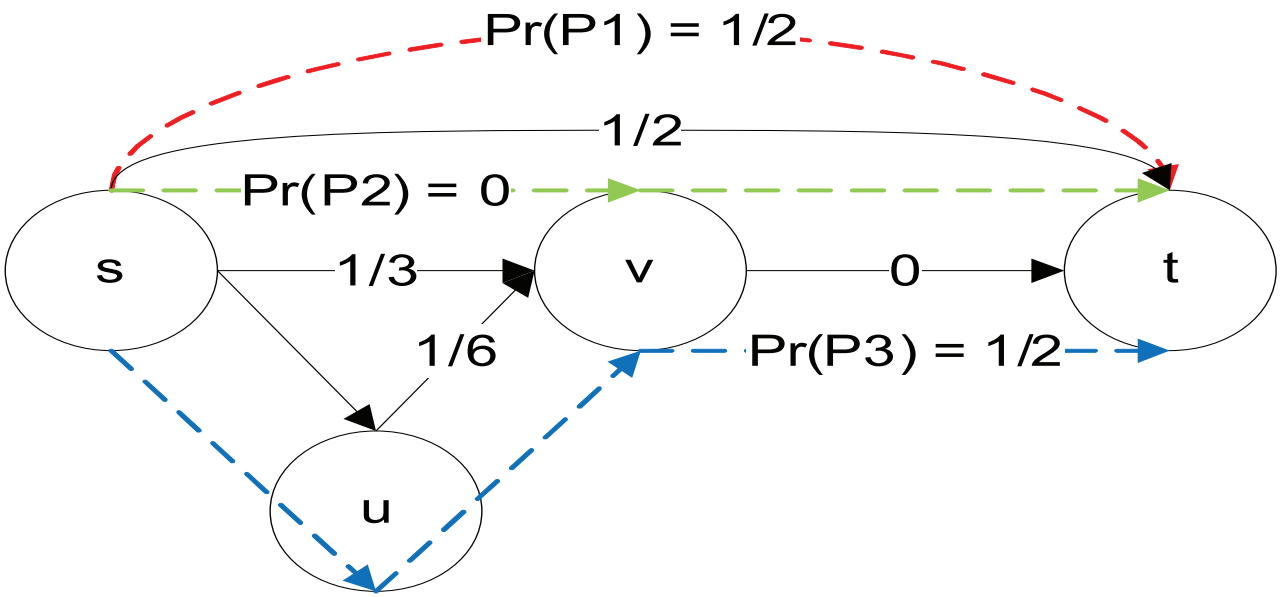
$SG(1,1)$ Pure strategies: no equilibrium



Designer uses P_2, attacker $vt \implies$ designer switches to P_1

Designer uses P_1, attacker $vt \implies$ attacker switches to st

$SG(1,1)$ Mixed strategies example

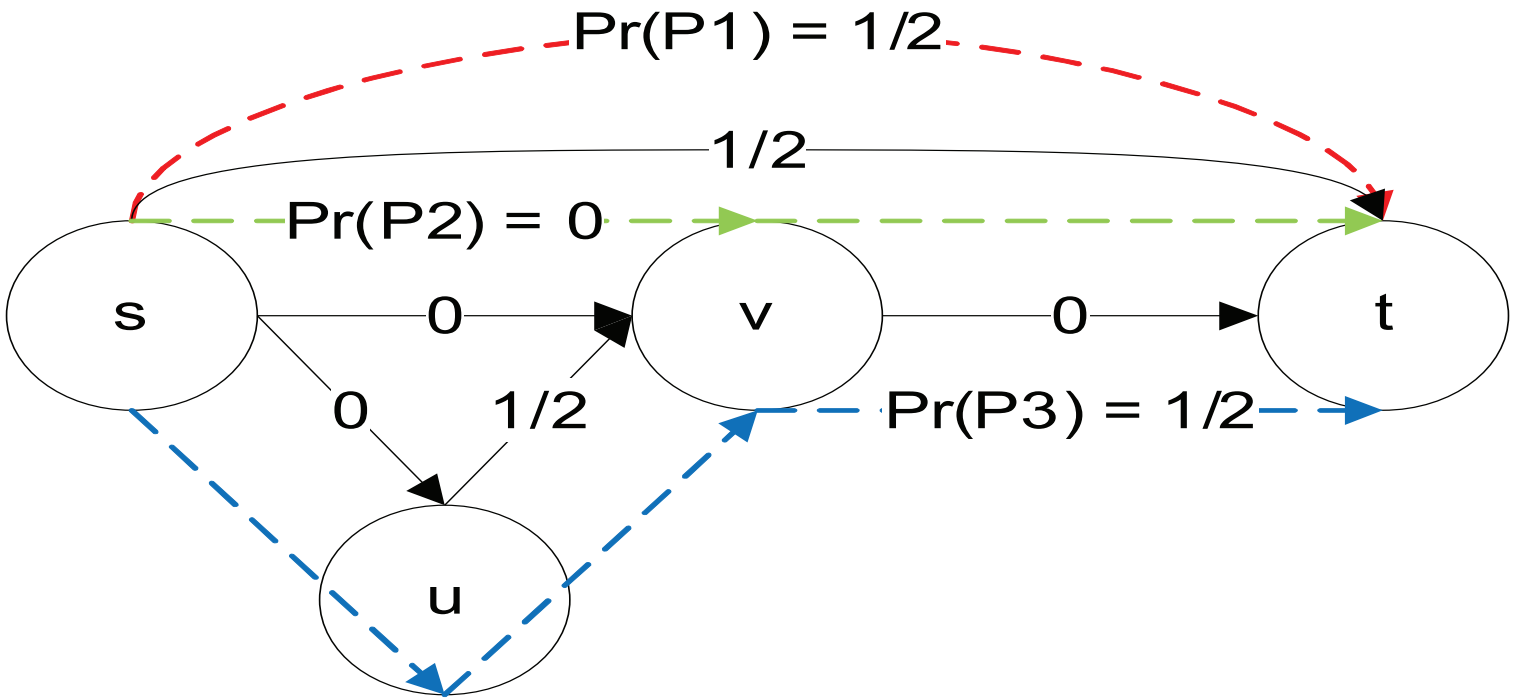


Attacker's (average) payoff:

$(1/2)(1/2) + (1/3) \cdot 0 + (1/6)(1/2) = 1/3$

Designer's payoff = $-1/3$

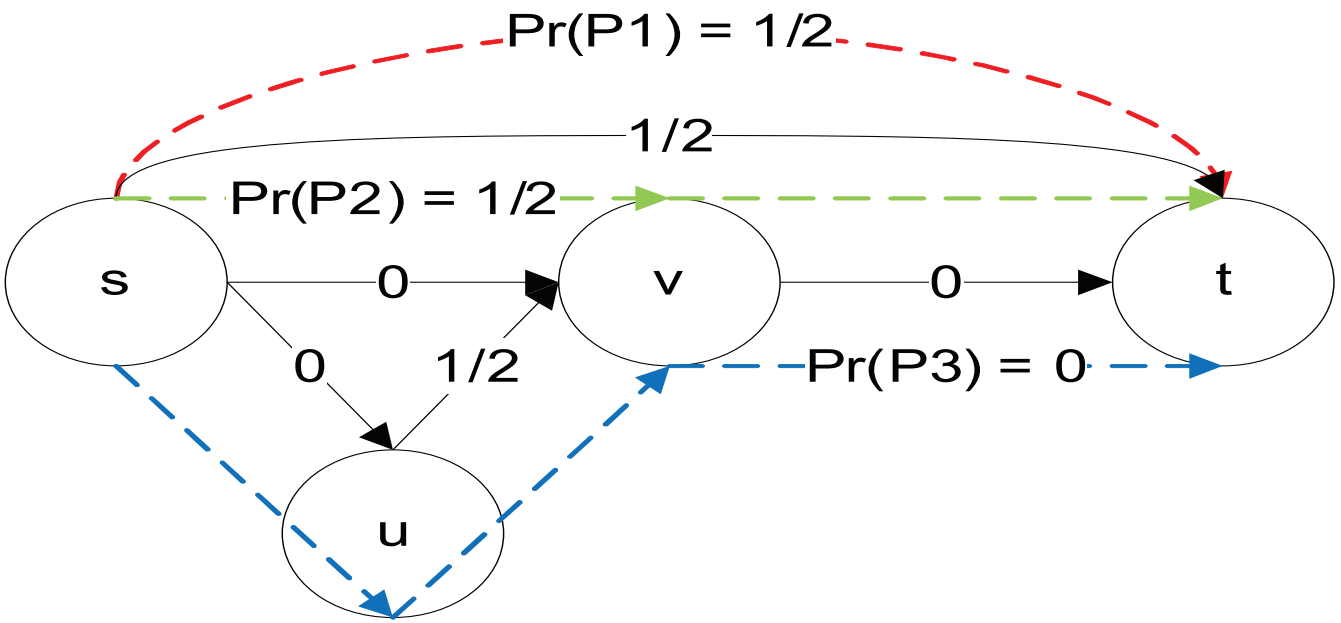
Mixed strategies - not an equilibrium



Attacker switched strategy. His new payoff:

$(1/2)(1/2) + (1/2)(1/2) = 1/2 > 1/3$

Mixed strategies - not an equilibrium

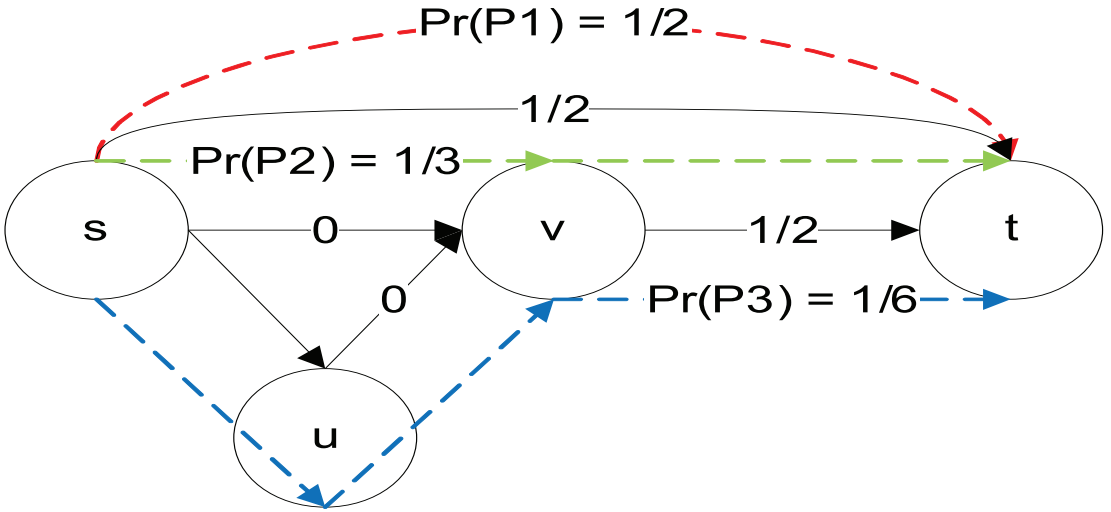


Designer switched strategy. Her new payoff:

$(-1)(1/2)(1/2) + (-1)(1/2) \cdot 0 + (-1) \cdot 0 \cdot (1/2) =$

$-1/4 > -1/2$

$SG(1,1)$ Mixed strategies - equilibrium



Designer pays at least $1/2$ no matter which path she picks.

Attacker can't get more than $1/2$ no matter which edge he picks.

$SG(1,1)$ - Mixed strategies linear program

Payoff matrix: $a_{ij} = 1$ if $e_i \in P_j; 0$ otherwise.

$Attacker$: **LP1:** Maximize w s.t.

$$\sum_{i=1}^{m} x_i a_{ij} \geq w \quad \forall s-t \text{ path } P_j$$
$$\sum_{i=1}^{m} x_i = 1; \quad x_i \geq 0$$

$Designer$: **LP2:** Minimize λ s.t.

$$\sum_{j=1}^{q} a_{ij} y_j \leq \lambda \quad \forall e_i \in E$$
$$\sum_{j=1}^{q} y_j = 1; \quad y_j \geq 0$$

Exponentially large (primal/dual) linear programs.

- $SG(1, c)$ poly-time using maximum network flows - Washburn & Wood, 1995
- $SG(k, 1)$ NEW poly-time using concurrent flows
- $SG(2, c)$ with c at most the min-cut value in undirected graphs: NEW poly-time using Hu's two commodity flows
- $SG(3, c)$ with $2 \leq c \leq$ the global min-cut value in undirected graphs: left open. Separation oracle NP-Hard even for $SG(1, 2)$ (which can still be solved!). Poly-sized solution always exists.

Max-flow/Min-cut theorem

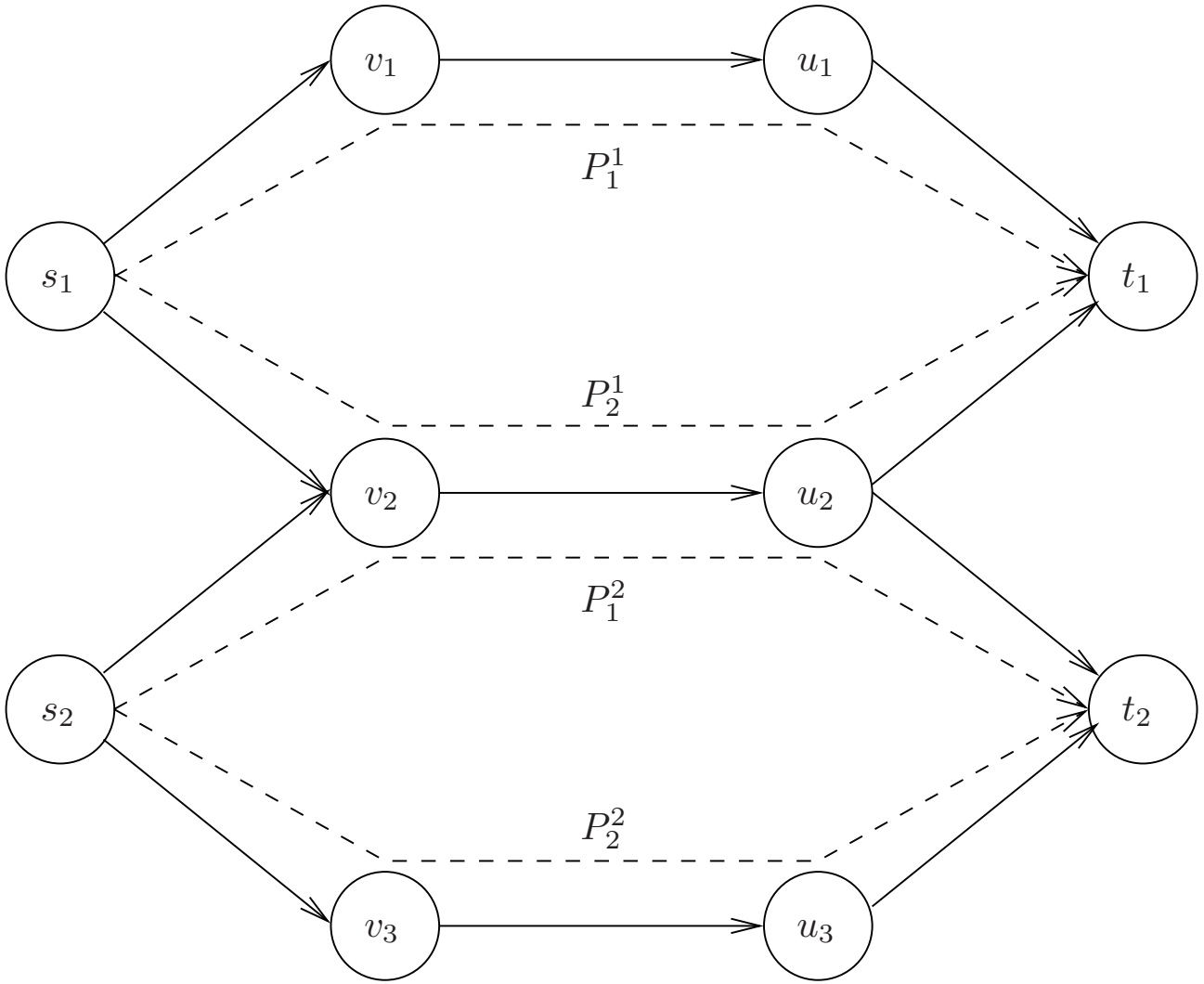
$SG(1,1)$ strategies for the attacker and the designer derives from max-flow and min-cut theorem. f is a max-flow. Nash equilibrium (KNOWN):

- Attacker: $\forall i, e_i \in C : x_i = 1/|C|$. C= min s-t cut
- Designer: $|f|$ disjoint paths $\forall j, P_j \in P_f : y_j = 1/|f|$
- Note that $|C| = |f|$. $w = \lambda = 1/|C| = 1/|f|$.

(k commodities , 1 edge)-game $SG(k, 1)$

- Max-flow/min-cut theorem does not hold in the case of multi-commodities.
- However, we achieve Nash equilibrium by solving (fractional) multi-commodity flow and (fractional) sparsest-cut.
- We will show examples in the following slides.

An example of $SG(2,1)$ instance

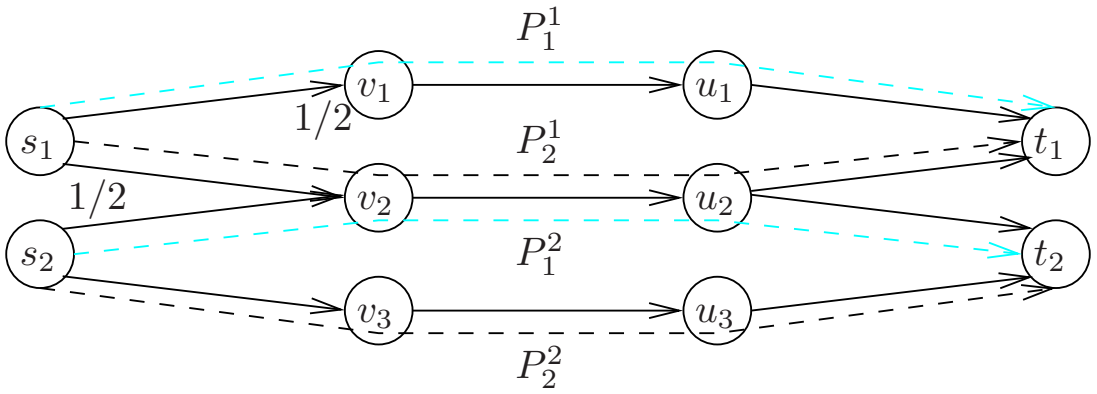


Payoff Matrix

P \ E	$s_1 v_1$	$s_1 v_2$	$s_2 v_2$	$s_2 v_3$	$v_1 u_1$	$v_2 u_2$
$P_1^1 P_1^2$	1	0	1	0	1	1
$P_1^1 P_2^2$	1	0	0	1	1	0
$P_2^1 P_1^2$	0	1	1	0	0	2
$P_2^1 P_2^2$	0	1	0	1	0	1

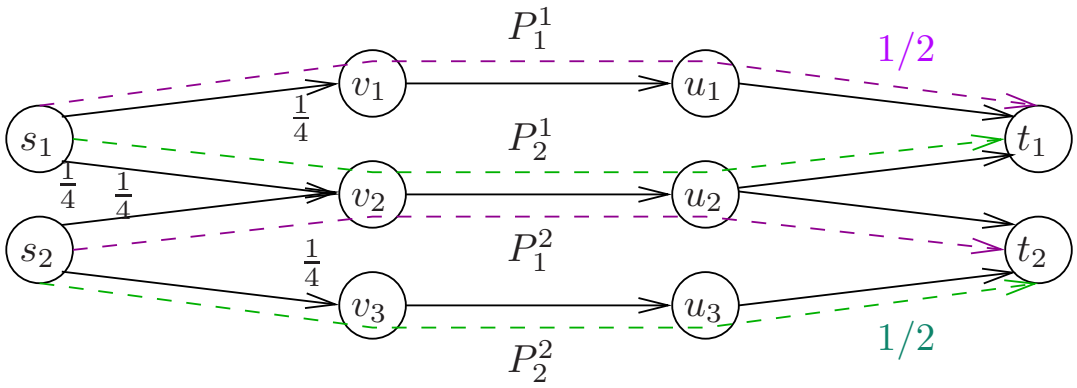
P \ E	$v_3 u_3$	$u_1 t_1$	$u_2 t_1$	$u_2 t_2$	$u_3 t_2$
$P_1^1 P_1^2$	0	1	0	1	0
$P_1^1 P_2^2$	1	1	0	0	1
$P_2^1 P_1^2$	0	0	1	1	0
$P_2^1 P_2^2$	1	0	1	0	1

$SG(2,1)$ - mixed strategy example



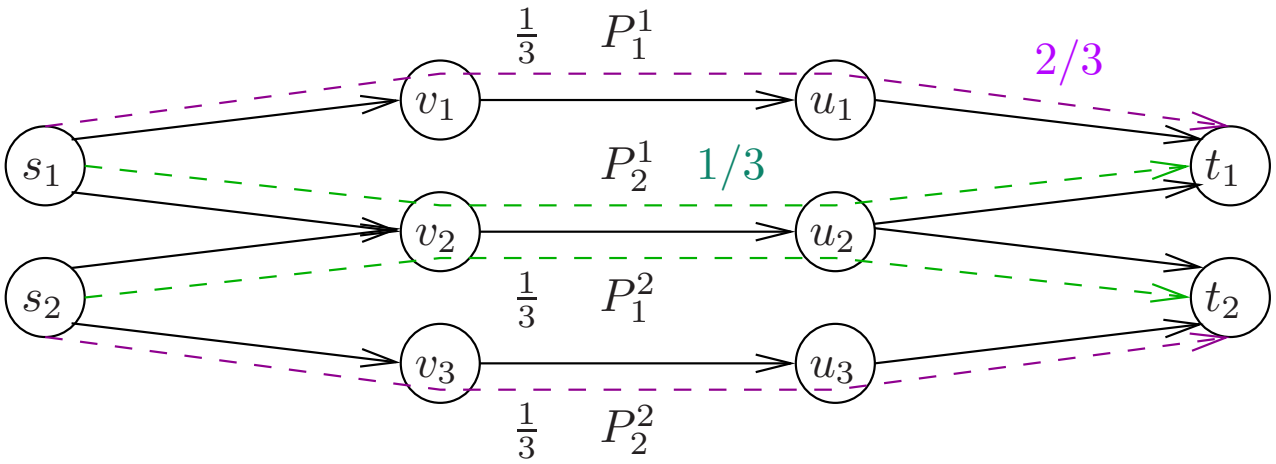
- Designer: $P_1^1 P_1^2$ with prob. 1
- Attacker: $s_1 v_1$ and $s_2 v_2$ each with prob. $1/2$,
- Attacker's payoff is $1(1/2) + 1(1/2) = 1$
- Not an equilibrium; designer can switch to $P_2^1 P_2^2$ with resulting payoff 0

$SG(2,1)$ - mixed strategy example



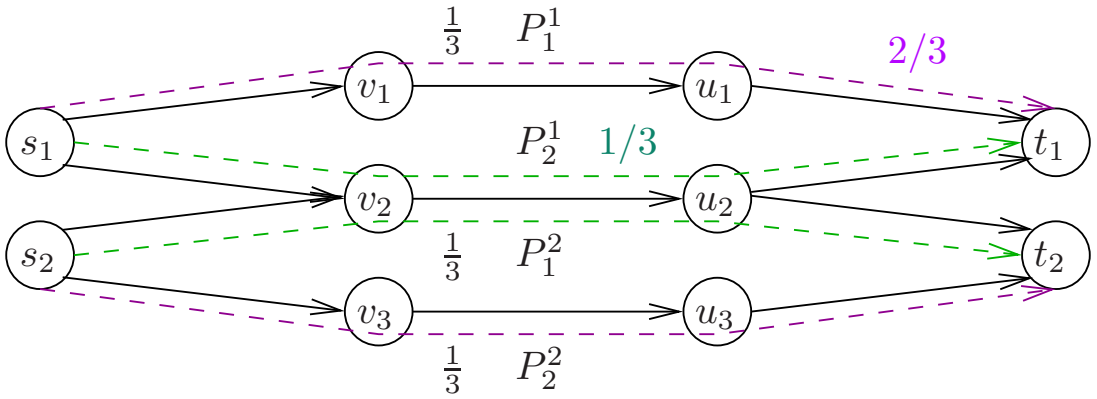
- Designer: $P_1^1 P_1^2$ and $P_2^1 P_2^2$ each w.p. $1/2$
- Attacker: s_1v_1, s_1v_2, s_2v_2, s_2v_3, each w. p. $1/4$
- Attacker's payoff $\frac{1}{2}(\frac{1}{4}+\frac{1}{4})+\frac{1}{2}(\frac{1}{4}+\frac{1}{4})=1/2$
- Not an equilibrium; attacker can switch to v_2u_2 with resulting payoff $\frac{1}{2}\cdot 1+\frac{1}{2}\cdot 1=1$

$SG(2,1)$ instance - Nash equilibrium



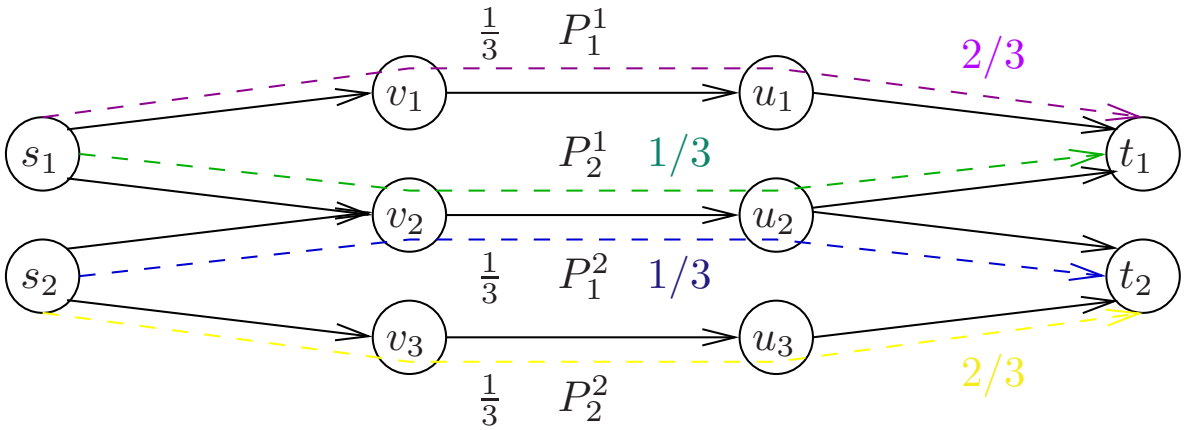
- Designer: $P_1^1 P_2^2$ w.p. $2/3$ and $P_2^1 P_1^2$ w.p. $1/3$
- Attacker: v_1u_1, v_2u_2, v_3u_3, each w.p. $1/3$
- Attacker's payoff is $\frac{2}{3}(\frac{1}{3}+\frac{1}{3})+\frac{1}{3}\cdot\frac{1}{3}\cdot 2=\frac{6}{9}=\frac{2}{3}$
- Attacker not switching: any edge gets $\leq 2/3$

$SG(2,1)$ instance - Nash equilibrium



- Designer: $P_1^1 P_2^2$ w.p. $2/3$ and $P_2^1 P_1^2$ w.p. $1/3$
- Attacker: v_1u_1, v_2u_2, v_3u_3, each w.p. $1/3$
- Attacker's payoff is $2/3$
- Designer would not switch: any single path must pay $1/3$ (and there are two paths)

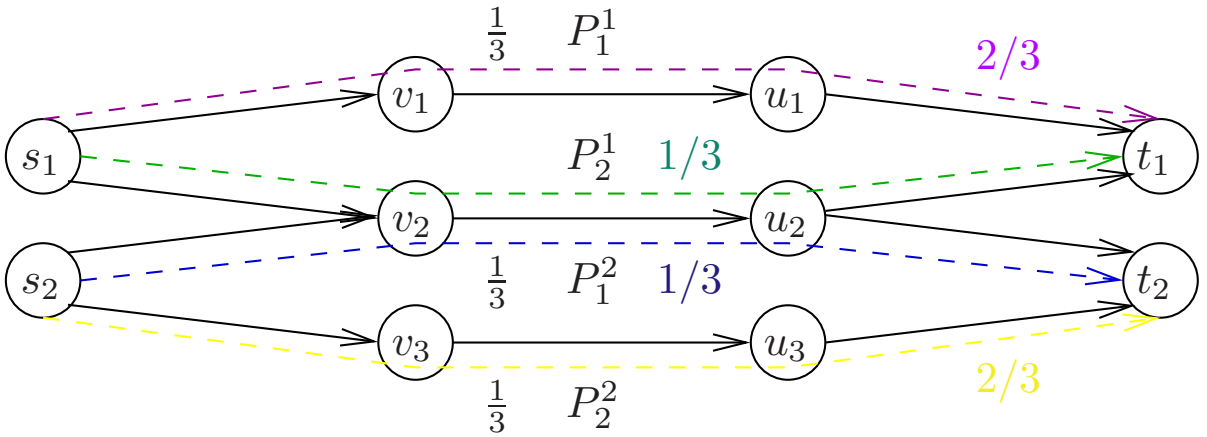
$SG(2,1)$ instance - second equilibrium



- Designer: $P_1^1 P_1^2$, $P_2^1 P_2^2$ each w.p $2/9$, $P_2^1 P_1^2$ w.p. $1/9$, $P_1^1 P_2^2$ w.p. $4/9$ ("decomposable paths")
- Attacker: v_1u_1, v_2u_2, v_3u_3, each w.p. $1/3$
- Attacker's payoff is

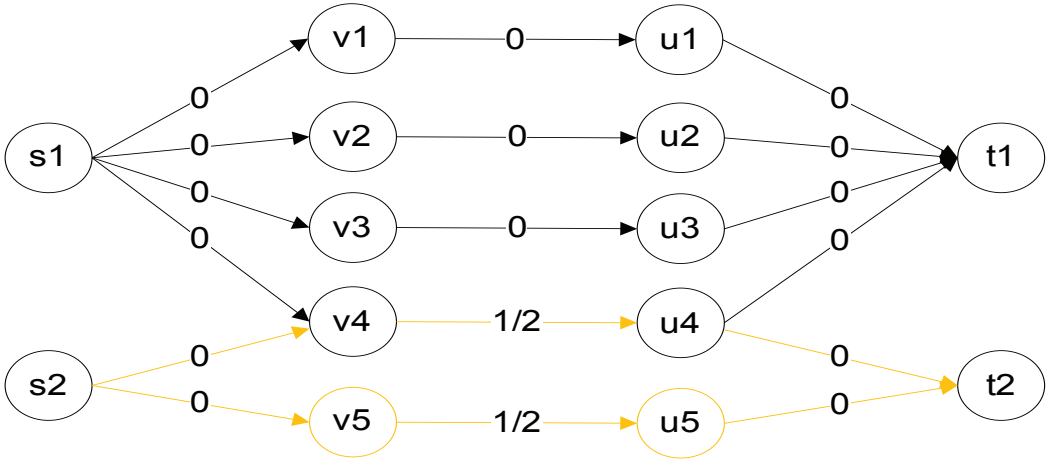
$$\frac{2}{9}\left(\frac{1}{3}+\frac{1}{3}\right)+\frac{2}{9}\left(\frac{1}{3}+\frac{1}{3}\right)+\frac{1}{9}\left(\frac{1}{3}\right)\cdot 2+\frac{4}{9}\left(\frac{1}{3}+\frac{1}{3}\right)=\frac{4+4+2+8}{27}=\frac{2}{3}$$

$SG(2,1)$ instance - second equilibrium



- Designer's paths decomposed: P_1^1 w.p. $2/3$, P_2^1 w.p $1/3$, and P_2^2 w.p. $2/3$, P_1^2 w.p $1/3$,
- Attacker: any single edge pays at most $\frac{2}{3}$
- Designer would not switch: any single path must pay $1/3$ (and there are two paths)

Another $SG(2,1)$ instance + equilibrium



- Designer: Two yellow $s_2 - t_2$ paths each w.p. $1/2$, upper three $s_1 - t_1$ paths each w.p. $1/3$
- Attacker: v_4u_4 and v_5u_5 each w.p. $1/2$
- Attacker's payoff is $\frac{1}{2}\frac{1}{2} + \frac{1}{2}\frac{1}{2} = 1/2$

$SG(k,1)$ Payoff Matrix A

$q_i :=$ number of $s_i - t_i$ paths.

A has $q := \Pi_{i=1}^{k} q_i$ rows and $|E|$ columns.

Let P_j^i be the j^{th} path from s_i to t_i Let r be some correspondence from $\{1, 2, \ldots, q\}$ to $\{1, 2, \ldots, q_1\} \times \{1, 2, \ldots, q_2\} \times \cdots \times \{1, 2, \ldots, q_k\}$, with $r_i(j)$ giving the i^{th} component of $r(j)$

A_{je} represents the number of commodities going through e $(= |\{i \in \{1, 2, \ldots, k\} \mid e \in P^i_{r_i(j)}\}|)$

$SG(k,1)$ Primal and Dual Linear Programs

LP3: Maximize w s.t. $\sum_{e \in E} A_{je} x_e \geq w \quad \forall 1 \leq j \leq q$

$$\sum_{i=1}^{m} x_e = 1; \qquad x_e \geq 0 \; \forall e \in E.$$

LP4: Minimize λ s.t. $\sum_{j=1}^{q} A_{je} y_j \leq \lambda \qquad \forall e \in E$

$$\sum_{j=1}^{q} y_j = 1; \qquad y_j \geq 0 \; \forall j \in \{1, \ldots, q\}$$

$$A_{je} = |\{i \in \{1, 2, \ldots, k\} \mid e \in P^i_{r_i(j)}\}|$$

$SG(k,1)$ - Auxiliary Primal and Dual LPs

LP5: Minimize α s.t. $\sum_{P \in \mathcal{P} \mid e \in P} f_P \leq \alpha \quad \forall e \in E$

$$\sum_{j=1}^{q_i} f_{P_j^i} = 1 \ \ \forall i; \qquad f_P \geq 0 \qquad \forall P \in \mathcal{P}$$

LP6: Maximize $\sum_{i=1}^{k} d_i$ s.t. $d_i \leq \sum_{e \in P_j^i} l_e \quad \forall i \wedge \forall j$

$$\sum_{e \in E} l_e = 1; \qquad l_e \geq 0 \qquad \forall e \in E$$

Concurrent flow - Fractional Sparsest Cut LPs.

$SG(k,1)$ - Solving auxiliary LP5

Polynomial-sized **LP7:** Minimize γ s.t.

$$\begin{aligned}
\textstyle\sum_{e\in\delta^-(u)} f_e^i = \sum_{e\in\delta^+(u)} f_e^i & \qquad \forall i \wedge \forall u \in V \setminus \{s_i, t_i\} \\
\textstyle\sum_{e\in\delta^+(s_i)} f_e^i - \sum_{e\in\delta^-(s_i)} f_e^i = 1 & \qquad \forall i \in \{1,\ldots,k\} \\
\textstyle\sum_{i=1}^{k} f_e^i \leq \gamma & \qquad \forall e \in E \\
f_e^i \geq 0 & \qquad \forall e \in E \wedge \forall i
\end{aligned}$$

$SG(k,1)$ equilibrium solution

Let $w = \sum_{i=1}^{k} d_i$ and $x_e = l_e$ (magic fails for $SG(k,2)$)

Claim 1 *The above w and x_e are feasible for LP3.*

Let $\lambda = \alpha^*$ and $y_j = \Pi_{i=1}^{k} f^*_{P^i_{r_i(j)}}$ (decomposable)

Claim 2 *The above λ and y_j are feasible for LP4.*

Same objective $\Longrightarrow$ primal/dual feasible solutions are optimal

$SG(2, c)$ game

- We did not solve more general problems, i.e. $SG(k, c)$ since primal/dual type relation does not hold for multicommodities
- In undirected graphs, for two commodites, Hu's Max-Flow Min-Multicut theorem holds
- It is natural to assume $c \leq q$, where q is the number of edges in a global min-cut (otherwise attacker does more than break the network)

for $SG(2, c)$: Max-Flow/Min-Multicut setup

- Let $C_1 \subseteq E$ be the min-cut separating s_1 from t_1
- Let $C_2 \subseteq E$ be the min-cut separating s_2 from t_2
- Let $C_3 \subseteq E$ be the minimum cut separating both $s_i - t_i$ pairs

for $SG(2, c)$: Max-Flow/Min-Multicut

Let $C_{min} = \min(|C_1|, |C_2|)$.

Hu's Theorem (1963) :

- If $C_{min} \leq |C_3|/2$, then $\exists\ |f_1| = |f_2| = C_{min}$.
- If $C_{min} > |C_3|/2$, then $\exists\ |f_1| = |f_2| = |C_3|/2$.

Moreover, these two-commodity flows can be found in time polynomial in the size of G.

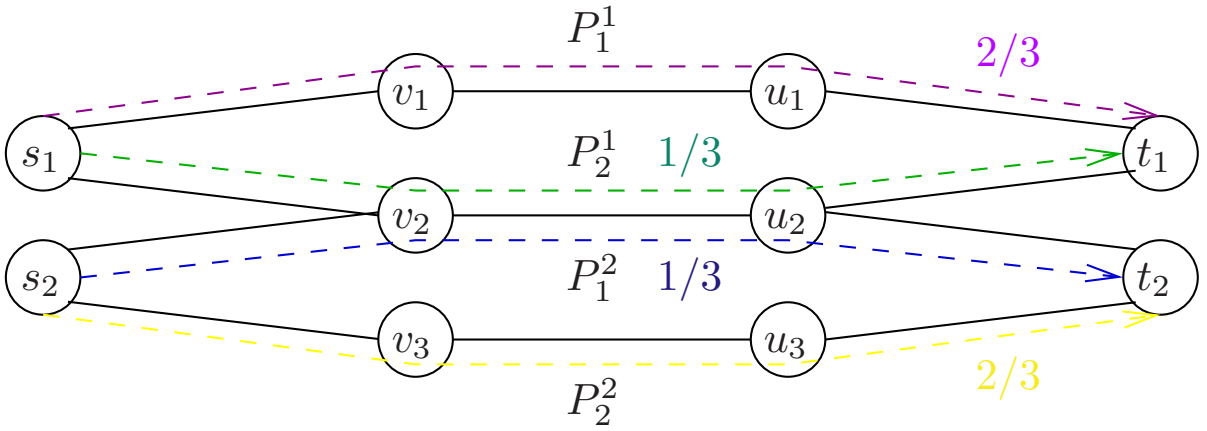
for $SG(2, c)$: Computing Nash Equilibrium

If $\min(|C_1|, |C_2|) \leq |C_3|/2$, attacker uniformly at random picks c edges from the cut achieving $\min(|C_1|, |C_2|)$

Otherwise ($|C_3|/2 < |C_1|$ and $|C_3|/2 < |C_2|$), attacker uniformly at random picks c edges from C_3

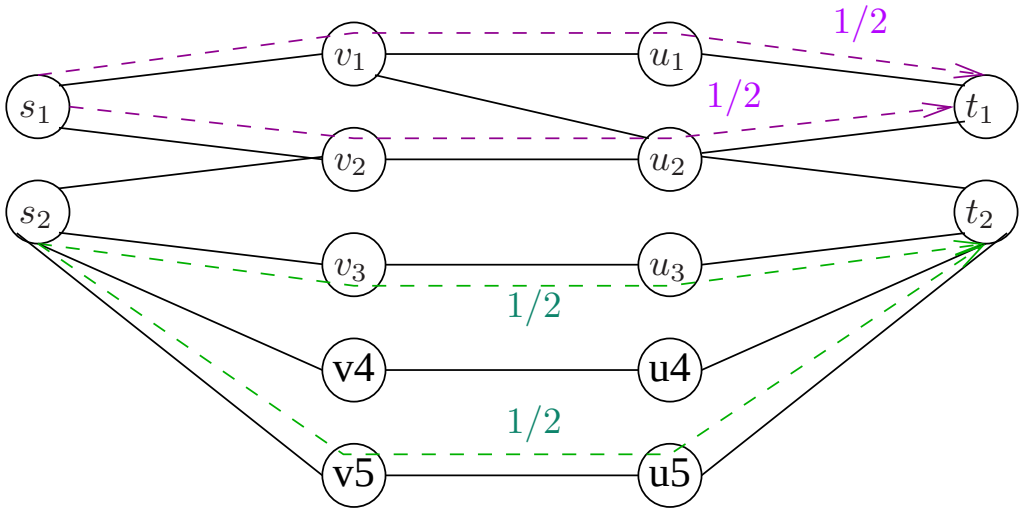
Designer's strategy: independently for the two commodities, routed as in the theorem and scaled down such that each flow is 1

$SG(2,2)$: example



- Here $|C_1| = |C_2| = 2$ and $|C_3|/2 = 3/2$.
- Attacker picks two out of v_1u_1, v_2u_2, v_3u_3 with payoff $\frac{1}{3}(1+1/3)+\frac{1}{3}(1+1/3)+\frac{1}{3}(2/3+2/3) = 4/3$
- Designer's decomposable solution shows attacker can't get more ($2/3$ flow "escapes")

$SG(2,2)$ - another example



- Here $|C_1| = 2$, $|C_2| = 4$ and $|C_3|/2 = 5/2$.
- Attacker picks $\{s_1v_1, s_1v_2\}$ with payoff $\frac{c}{|C_1|} = 1$.
- Designer's decomposable solution shows attacker can't get more (1 flow "escapes")

Edges have costs - two commodities

- The attacker incurs a cost for each edge attacked, gains 1 for every intercepted path
- The designer chooses two paths, from given s_1 to t_1 and s_2 to t_2

With $c(S) = \sum_{e \in S} c(e)$, for $S \subseteq E$, the payoff matrix is

$$A_{jS} = |\{i \in \{1,2\} \mid P^i_{r_i(j)} \cap S \neq \emptyset\}| - c(S)$$

Game with edge costs

LP11: Maximize w subject to

$$\sum_{S \in \mathcal{T}} A_{jS} x_S \geq w \quad \forall 1 \leq j \leq q \tag{1}$$

$$\sum_{S \in \mathcal{T}} x_S = 1 \tag{2}$$

$$x_S \geq 0 \qquad \forall S \in \mathcal{T}. \tag{3}$$

LP12: Minimize λ subject to

$$\sum_{j=1}^{q} A_{jS} y_j \leq \lambda \quad \forall S \in \mathcal{T} \tag{4}$$

$$\sum_{j=1}^{q} y_j = 1 \tag{5}$$

$$y_j \geq 0 \qquad \forall j \in \{1, 2, \ldots, q\} \tag{6}$$

Game with edge costs

- With C_1, C_2, C_3 being Hu's cuts, assign
  $\lambda = w = \max(0 - c(\emptyset), 1 - c(C_1), 1 - c(C_2), 2 - c(C_3))$.
- The attacker picks as his strategy the set of edges above achieving the maximum.
- For the designer, we use a second result of Hu.

Conclusion

New poly-time computation of Nash equilibrum:

- $SG(k, 1)$ using concurrent flows
- $SG(2, c)$ with c at most the min-cut value in undirected graphs: using Hu's two commodity flows
- with costs, two commodities in undirected graphs

$SG(3, c)$ with $2 \leq c \leq$ the global min-cut value in undirected graphs: left open.