The Price of Defense

M. Mavronicolas[*] , **V. Papadopoulou**[*],
L. Michael[¥], A. Philippou[*], P. Spirakis[§]

University of Cyprus, Cyprus[*]
University of Patras and RACTI, Greece[§]
Division of Engineering and Applied Sciences,
Harvard University, Cambridge[¥]

Motivation: Network Security

- Current networks are *huge* and *dynamic*

⇒vulnerable to Security risks (Attacks)

- *Attackers*:
  - viruses, worms, trojan horses or eavesdroppers
  - damage *a node* if it not secured
  - wish to avoid being caught by the security mechanism

Motivation: Network Security

- A *defense* mechanism:
  - a security software or a firewall
  - *cleans* from attackers a *limited part* of the network:
    - a *single link*
  - it wants to protect the network as much as possible

    ⇒ catches as many attackers as possible

A formal Model: A Strategic Game

- A non-cooperative strategic same *on a graph* with *two kinds* of *players*:
  - ⇒ the *vertex players* ↔ attackers
  - ⇒ the *edge player* ↔ defender
- An attacker *selects* a node *to* damage if unsecured
- The defender *selects* a single edge to clean from attackers on it

A formal Model: A Strategic Game (cont.)

- Attacker´s *(Expected) Individual Profit:*

  the probability not caught by the defender

- Defender´s *(Expected) Individual Profit*

  (expected) number of attackers it catches

A Strategic Game: Definition (cont.)

[Mavronicolas et al. ISAAC2005]

- Associated with G(V, E), is a strategic game:

$$\Pi(G) = \langle \mathcal{N}, \{S_i\}_{i\in\mathcal{N}}, \{\mathsf{IP}\}_{i\in\mathcal{N}} \rangle$$

- $\mathcal{N} = \mathcal{N}_{vp} \cup \mathcal{N}_{ep}$
- ν attackers (set $\mathcal{N}_{vp}$) or vertex players *vp*$_i$
  - *Strategy set* : S_{vp_i} = V
- a defender or the edge player *ep*
  - *Strategy set* : S_{ep} = E

Individual Profits

- *Pure* Profile: each player plays one strategy
- In a *pure* profile $\mathbf{s} = \langle s_1, \ldots, s_\nu, s_{ep} \rangle \in \mathcal{S}$
  - Vertex player vp$_i$´s Individual Profit:
    - $\text{IP}_i(\mathbf{s}) = 0 \; if \; s_i \in s_{ep} \;\; or \;\; 1 \; otherwise$

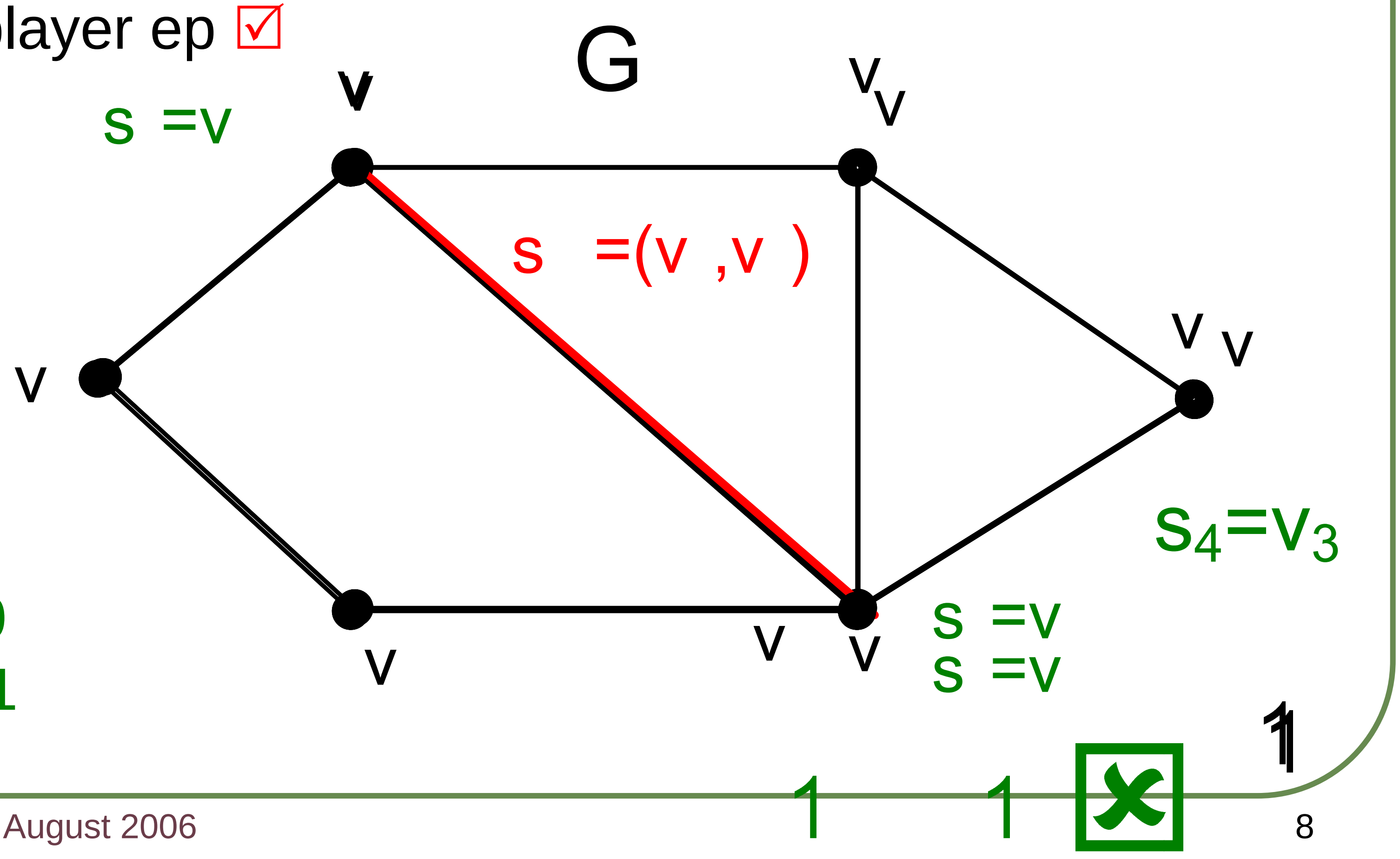
1 if it *selected* node is not incident to the edge selected by the edge player, and 0 otherwise

  - Edge player´s ep Individual Profit:
    - $\text{IP}_{ep}(\mathbf{s}) = |\{i : s_i \in s_{ep}\}|$

the number of attackers placed on the endpoints of its selected edge

Example

- a graph G
- ν=4 vertex players ☒
- edge player ep ☑



- $IP_s(ep)=3$
- $IP_s(vp_1)=0$
- $IP\mathbf{s}(vp_4)=1$

Mixed Strategies

- *Mixed strategy* s_i for player i
  - a probability distribution over its strategy set
- *Mixed profile* **s**
  - a collection of mixed strategies for all players
- *Support* (Support$_\mathbf{s}$(i)) of player i
  - set of pure strategies that it assigns *positive* probability

Nash Equilibria

- No player can unilaterally improve its Individual Profit by switching to another profile

Notation

In a profile **s**,

- **Support$_s$(vp)**= the supports of all vertex players
- P$_s$(Hit(υ)) $=$ Probability the edge player chooses an edge incident to vertex υ
- **VP$_s$(υ)** $=$ expected number of vps choosing vertex υ
- **VP$_s$(e)** $=$ VP$_s$(υ) $+$ VP$_s$(u), for an edge e$=$(u, υ)

Notation (cont.)

- Uniform profile:

  if each player uses a uniform probability distribution on its support. I.e., for each player i,

$$s_i(x) = \frac{1}{|\mathsf{Support_s}(i)|}, \text{ for any } x \in \mathsf{Support_s}(i).$$

- Attacker Symmetric profile:

  All vertex players use the same probability distribution

Expected Individual Profits

- vertex players *vp$_i$*:

$$\mathsf{IP}_{\mathbf{s}}(i) \;=\; \sum_{v \in V} s_i(v) \cdot (1 - P_{\mathbf{s}}(\mathsf{Hit}(v)))$$

- edge player *ep*:

$$\mathsf{IP}_{\mathbf{s}}(ep) \;=\; \sum_{e \in E} s_{ep}(e) \cdot \mathtt{VP}_{\mathbf{s}}(e)$$

where,

- **$s_i(\upsilon)$**= probability that vp$_i$ chooses vertex υ
- **$s_{ep}(e)$**= probability that the ep chooses edge *e*
- **Edges$_s$(υ)** ={edges $\in$ Support$_s$(ep) incident to vertex υ

Defense Ratio and Price of the Defense

- The Defense Ratio $DR_{\mathbf{s}}$ of a profile **s** is
  - the *optimal* profit of the defender (which is ν)
  - over its profit in profile **s**

$$= \frac{\nu}{\mathsf{IP}_{\mathbf{s}}(ep)}$$

- The Price of the Defense is
  - the worst-case (maximum) value, over all Nash equilibria **s**, of Defense Ratio DR

$$= \max_{\mathbf{s}\in\mathcal{S}} DR_{\mathbf{s}} = \max_{\mathbf{s}\in\mathcal{S}} \frac{\nu}{\mathsf{IP}_{\mathbf{s}}(ep)}$$

Algorithmic problems

- **CLASS** NE EXISTENCE

Instance: A graph G(V, E)

Question: Does Π(G) admit a **CLASS** Nash equilibrium?

- FIND **CLASS** NE

Instance: A graph G(V, E).

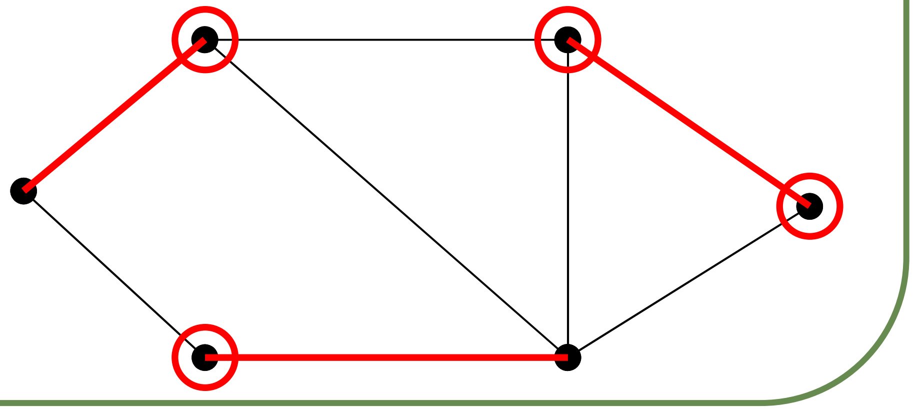
Output: A **CLASS** Nash equilibrium of Π(G) or No if such does not exist.

where,

CLASS : a class of Nash equilibria

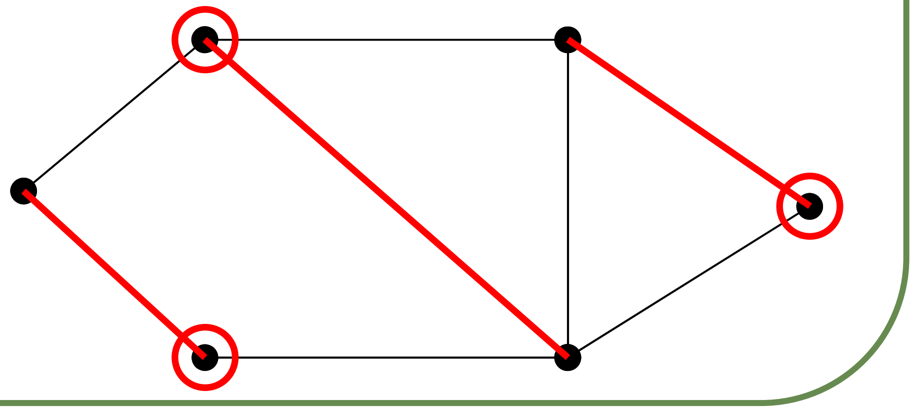
Background on Graph Theory

- **Vertex cover** of $\mathrm{G}(\mathrm{V},\mathrm{E})$
  - ⇒ set $V' \subseteq V$ that hits (incident to) *all* edges of *G*
  - ⇒ Minimum Vertex Cover size = $\alpha'(G)$
- **Edge cover**
  - ⇒ set $E' \subseteq E$ that hits (incident to) *all* vertices of *G*
  - ⇒ Minimum Edge Cover size = $\beta'(G)$



Background on Graph Theory

- **Independent Set**
  - ⇒ A set $IS \subseteq V$ of non-adjacent vertices of G
  - ⇒ Maximum Independent Set size = $\alpha(G)$
- **Matching**
  - ⇒ A set $M \subseteq E$ of non-adjacent edges
  - ⇒ Maximum Matching size = $\alpha'(G)$



Graph Theory Notation

- In a graph G,
  - α(G) $\leq$ β'(G)
  - A Graph G is König-Egenváry if α(G) = β'(G).
- For a vertex set U$\subseteq$ V,
  - $G(U)$ = the subgraph of G induced by vertices of U
- For the edge set $F\subseteq E$,
  - $G(F)$ = the subgraph of G induced by edges of F

Summary of Results

- Graph Theoretic
- Computational Complexity
- Game Theoretic

Summary of Results (1/6): Graph-Theoretic, Complexity Results

Useful Graph-Theoretic Results:

- Negative Results:
  - UNDIRECTED PARTITION INTO HAMILTONIAN CYRCUITS OF SIZE AT LEAST 6
    - is NP-complete.
- Positive Results
  - *KÖNIG-EGENVÁRY MAX INDEPENDENT SET can be solved in polynomial time.*
  - MAX INDEPENDENT SET EQUAL HALF ORDER *can be solved in polynomial time.*

Summary of Results (2/6): General Nash equilibria

- A general Nash equilibrium
  - can be computed in Polynomial time

But,

- No guarantee on the Defense Ratio of such an equilibrium computed.

Summary of Results (3/6): Structured Nash equilibria

Structured Nash equilibria:

⇒ Matching Nash equilibria [Mavronicolas et al. ISAAC05]

- A graph-theoretic characterization of graphs admitting them
- A polynomial time algorithm to compute them on any graph
  - using the KÖNIG-EGENVÁRY MAX INDEPENDENT SET problem
- The Defense Ratio for them is $\alpha(G)$

Summary of Results (5/6): Perfect Matching Nash equilibria

- Introduce Perfect Matching Nash equilibria
  - A graph-theoretic characterization of graphs admitting them
    - A polynomial time algorithm to compute them on any graph
      - using the MAX INDEPENDENT SET EQUAL HALF ORDER problem
  - The Defense Ratio for them is $|V| / 2$

Summary of Results (5/6): Defender Uniform Nash equilibria

- Introduce Defender Uniform Nash equilibria
  - A graph-theoretic characterization of graphs admitting them
  - The existence problem for them is NP-complete
  - The Defense Ratio them is $\left(\frac{\pi}{2}+1\right)\cdot|V|$ for some $1 \leq \pi \leq 1$.

Summary of Results (6/6): Attacker Symmetric Uniform Nash equilibria

- Introduce Attacker Symmetric Uniform Nash equilibria
  - A graph-theoretic characterization of graphs admitting them
  - The problem to find them *can be solved in polynomial time.*
  - The Defense Ratio for them is $\frac{|V|}{2}$ or $\alpha(G)$.

Complexity Results

Complexity Results (1/2):
A new NP-completeness proof

For the problem:

- UNDIRECTED PARTITION INTO HAMILTONIAN CIRCUITS OF SIZE AT LEAST 6

  Input: An undirected graph G(V,E)

  Question: Can the vertex set V be partitioned into disjoint sets V_1, Λ, V_k, such that each $|V_i| \geq 6$ and $G(V_i)$ is Hamiltonian?

Complexity Results (2/2):
A new NP-completeness proof

We provide the *first* published proof that:

- Theorem 1.

  UNDIRECTED PARTITION INTO HAMILTONIAN SUBGRAPHS OF SIZE AT LEAST 6 is NP-complete.

Proof.

Reduce from

- the *directed* version of the problem for circuits of size at least 3 which is known to be
  - NP-complete in [GJ79] □

Graph-Theoretic Results

Graph-Theoretic Results (1/3)

- KÖNIG-EGENVÁRY MAX INDEPENDENT SET

Instance: A graph G(V, E).

Output: A Max Independent Set of G is König-Egenváry ($\alpha(G) = \beta'(G)$) or No otherwise.

- Previous Results for König-Egenváry graphs
  - (Polynomial time) characterizations [Deming 79, Sterboul 79, Korach et. al, 06]
- Here we provide:
  - a new polynomial time algorithm for solving the KÖNIG-EGENVÁRY MAX INDEPENDENT SET problem.

Graph-Theoretic Results (2/3)

- Proposition 1.

  KÖNIG-EGENVÁRY MAX INDEPENDENT SET can be solved in polynomial time.

Proof.

- Compute a Min Edge Cover EC of G
- From EC construct a 2SAT instance ϕ such that
  - G has an Independent Set of size $|EC|=\beta'(G)$ (so, $\alpha(G) = \beta'(G)$) if and only if ϕ is satisfiable.

□

Graph-Theoretic Results (3/3)

- MAX INDEPENDENT SET EQUAL HALF ORDER

  Instance: A graph G(V, E).

  Output: A Max Independent Set of G of size $\frac{|V|}{2}$ if $\alpha(G) = \frac{|V|}{2}$, or No if $\alpha(G) \neq \frac{|V|}{2}$.

- Proposition 2.

  MAX INDEPENDENT SET EQUAL HALF ORDER can be solved in polynomial time.

  Proof.

  Similar to the KÖNIG-EGENVÁRY MAX INDEPENDENT SET problem. □

Game Theory- Previous Work

Game Theory - Previous Work (1/4)

Mavronicolas et al. ISAAC05:

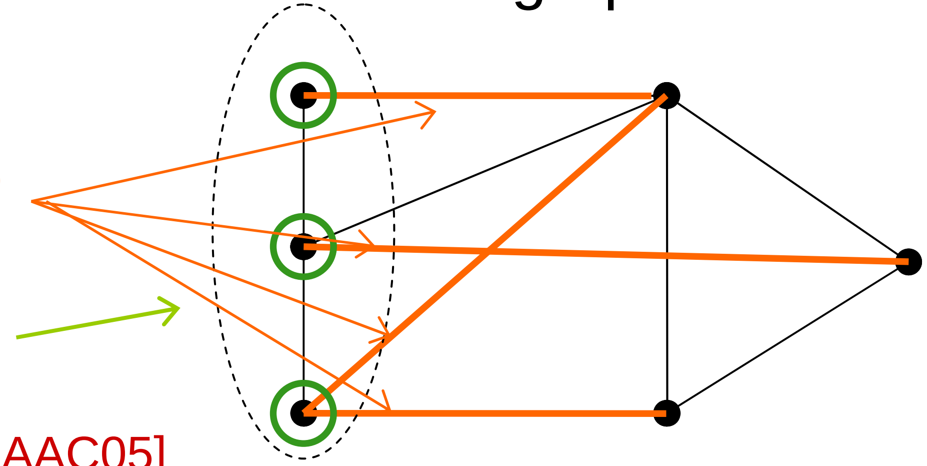
- Pure Nash Equilibria: The graph G admits no pure Nash equilibria (unless it is trivial).
- Mixed Nash Equilibria: An algebraic (non-polynomial) characterization.

Game Theory - Previous Work (3/5): Covering Profiles

- Definition. [Mavronicolas et al. ISAAC05]

  Covering profile is a profile **s** such that

  - $\text{Support}_s(\text{ep})$ is an Edge Cover of G
  - $\text{Support}_s(\text{vp})$ is a Vertex Cover of the graph $G(\text{Support}_s(\text{ep}))$.



$\text{Support}_s(\text{ep})$

$\text{Support}_s(\text{vp})$

- Proposition. [Mavr. et al. ISAAC05]

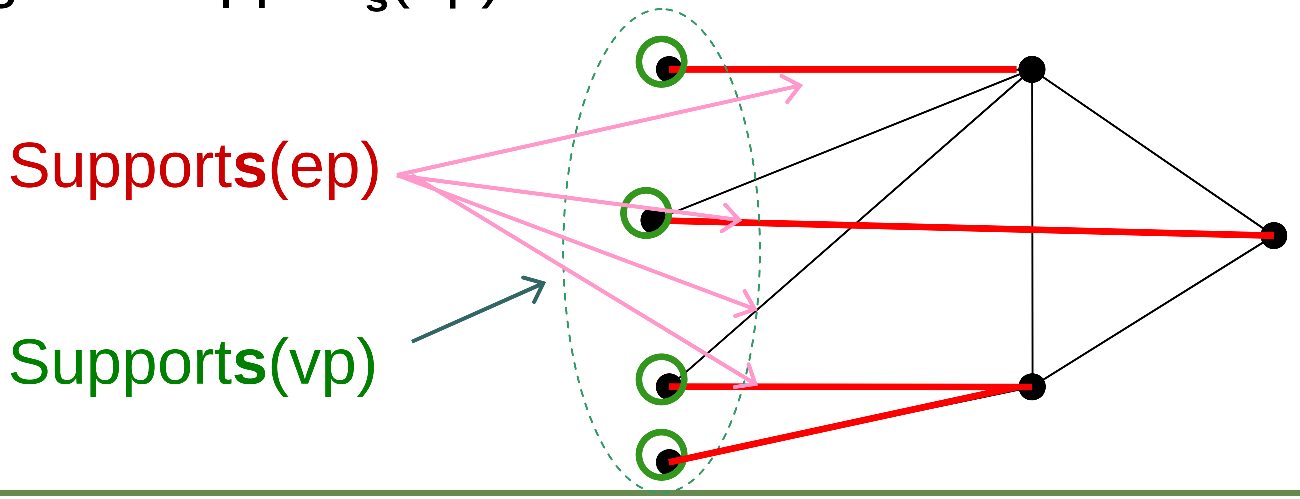
  A Nash equilibrium is a Covering profile.

Game Theory - Previous Work (4/5): Independent Covering Profiles

- Definition. [Mavronicolas et al. ISAAC05]

An Independent Covering profile **s** is a *uniform*, *Attacker Symmetric Covering* profile **s** such that*:*

1. $\text{Support}_{\mathbf{s}}(\text{vp})$ is an Independent Set of G.
2. Each vertex in $\text{Support}_{\mathbf{s}}(\text{vp})$ is incident to exactly one edge in $\text{Support}_{\mathbf{s}}(\text{ep})$.



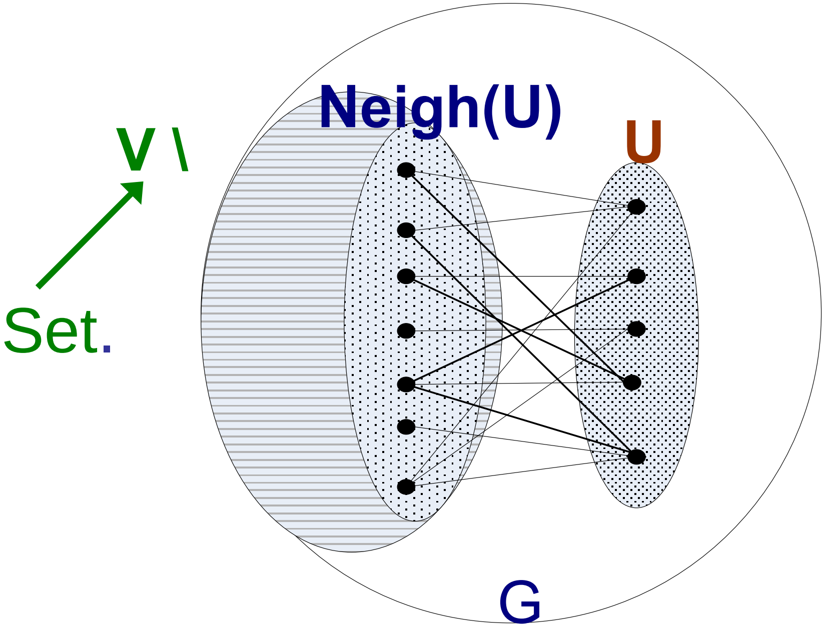
Game Theory - Previous Work (5/5): Matching Nash equilibria

- Proposition. [Mavronicolas et al. ISAAC05]

  An Independent Covering profile is a Nash equilibrium, called Matching Nash equilibrium

- Theorem. [Mavronicolas et al. ISAAC05]

  A graph G admits a Matching Nash equilibrium if and only if G contains an Expanding Independent Set.



Game Theoretic Results

General Nash Equilibria: Computation

- Consider a **two players** variation of the game Π(G):
  - ⇒ 1 attacker, 1 defender
- Show that it is a constant-sum game
- Compute a Nash equilibrium **s´** on the two players game (in polynomial time)
- Construct from **s´** a profile **s** for the many players game:
  - ⇒ which is Attacker Symmetric
  - ⇒ show that it is a Nash equilibrium

Theorem 2.

FIND GENERAL NE can be solved in polynomial time.

Matching Nash Equilibria: Graph Theoretic Properties

- Proposition 3.

  In a Matching Nash equilibrium ***s****,*

  - *$Support_s(vp)$ is a Maximum Independent Set of G.*
  - *$Support_s(ep)$ is a Minimum Edge Cover of G.*

A new Characterization of Matching Nash Equilibria

- Theorem 3. *The graph G admits a Matching Nash equilibrium if and it is* König-Egenváry *graph (*$\alpha(G) = \beta'(G)$*).*

Proof.

- Assume that $\alpha(G) = \beta'(G)$
- IS = Max Independent Set
- EC= Min Edge Cover
- Construct a Uniform, Attackers Symmetric profile **s** with:
  - $\text{Support}_{\mathbf{s}}(vp)$ = IS and $\text{Support}_{\mathbf{s}}(ep)$ = EC.
- We prove that **s** is an Independent Covering profile

  $\Rightarrow$ a Nash equilibrium.

Proof of Theorem 7 (cont.)

- Assume now that G admits a Matching Nash equilibrium **s**.
- By Proposition 3,

  ⇒ $|\text{Support}_{\mathbf{s}}(vp)| = |\text{Support}_{\mathbf{s}}(ep)|$

- by the definition of Matching Nash equilibria

⇒ $\alpha(G) = \beta'(G)$.

□

Since *KÖNIG-EGENVÁRY MAX INDEPENDENT SET* $\in \mathcal{P}$

⇒ Theorem 4.

FIND MATCHING NE can be solved in time

$$O\left(\sqrt{|V|}|E| \cdot \log_{|V|} \frac{|V|^2}{|E|}\right).$$

The Defense Ratio

- Proposition 5.

  In a Matching Nash equilibrium, the Defense Ratio is $\alpha(G)$.

Perfect Matching Nash Equilibria: Graph Theoretic Properties

- A Perfect Matching Nash equilibrium **s** is a Matching NE s.t. $\text{Support}_{\mathbf{s}}(\text{ep})$ is a Perfect Matching of G.

- Proposition 6.

  For a Perfect Matching Nash equilibrium ***s****,*

$$|\text{Support}_{\mathbf{s}}(vp)| = \frac{|V|}{2}.$$

Perfect Matching Nash Equilibria: Graph Theoretic Properties

- Theorem 5.

  A graph G admits a Perfect Matching Nash equilibrium if and only if it

  - *it has a Perfect Matching and*
  - *$\alpha(G) = |V|/2$.*

Proof.

Similarly to Matching Nash equilibria. □

Computation and the Defense Ratio

- Since MAXIMUM INDEPENDENT EQUAL HALF ORDER $\in \mathcal{P}$,

$\Rightarrow$ Theorem 6.

FIND PERFECT MATCHING NE can be solved in polynomial time

$$O\left(\sqrt{|V|}|E| \cdot \log_{|V|} \frac{|V|^2}{|E|}\right).$$

- Proposition 7. *In a Perfect Matching Nash equilibrium, the Defense Ratio is |V| / 2.*

Defender Uniform Nash Equilibria: A Characterization

- Theorem 7. *A graph G admits a Defender Uniform Nash equilibrium if and only if there are non-empty sets* $V' \subseteq V$ *and* $E' \subseteq E$ *and an integer* $r \geq 1$ *such that:*

  (1/a) For each $v \in V'$, $d_{G(E')}(v) = r$.

  (1/b) For each $v \in V \setminus V'$, $d_{G(E')}(v) \geq r$.

  (2) V' can be partitioned into two disjoint sets V'_i *and* V'_r *such that:*

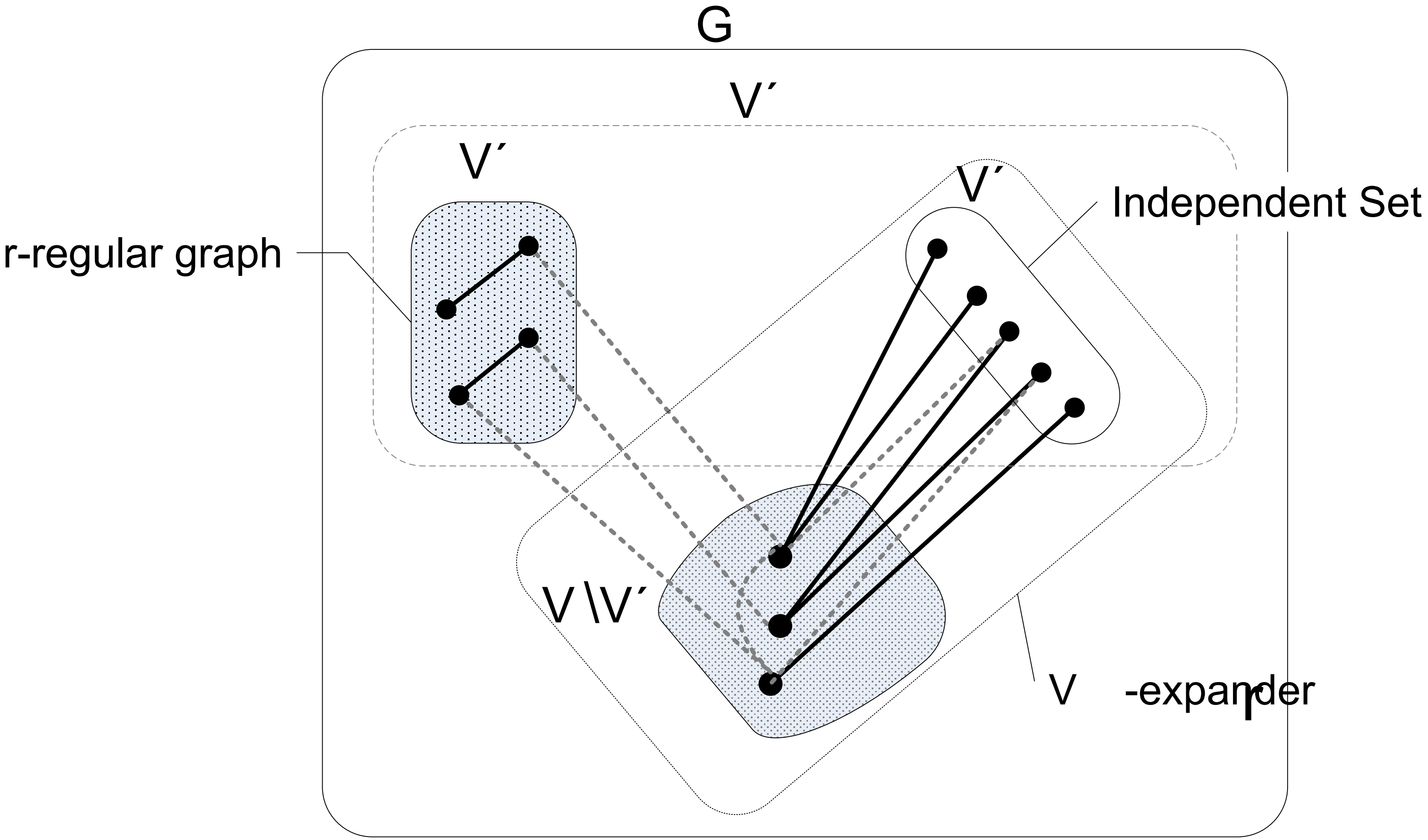
  (2/a) *For each* $v \in V'_i$, *for any* $u \in \mathrm{Neigh}_G(v)$, *it holds that* $u \notin V'$.

  (2/b) *The graph* $\langle V'_r, \mathrm{Edges}_G (V'_r)$ Å $E' \rangle$ *is an r-regular graph.*

  (2/c) *The graph* $\langle V'_l \cup (V \setminus V'), \mathrm{Edges}_G V'_l \cup (V \setminus V'))$ Å$E' \rangle$ *is a* $(V'_i , V \setminus V')$*-bipartite graph.*

  (2/d) *The graph* $\langle V'_i \cup V \setminus V‘), \mathrm{Edges}_G(V'_i \cup V \setminus V‘)$ Å$E' \rangle$ *is a* $(V \setminus V')$ *- Expander graph.*

Characterization of Defender Uniform Nash Equilibria



Complexity anf the Defense Ratio

- Theorem 8.

DEFENDER UNIFORM NE EXISTENCE is NP-complete.

Proof.

Reducing from

- UNDIRECTED PARTITION INTO HAMILTONIAN CYRCUITS

□

- Theorem 9. *In a Defender Uniform Nash equilibrium, the Defense Ratio is* $\left(\frac{\pi}{2}+1\right)\cdot|V|$ *for some* $0 \leq \pi \leq 1$.

Attacker Symmetric Uniform Nash Equilibria: A characterization

- Theorem 10.

  A graph G admits an Attacker Symmetric Uniform Nash equilibrium if and only if:

1. *There is a probability distribution* p:E → [0,1] *such that:*

   a) $\sum_{e \in \mathsf{Edges}_G(v)} p(e) = \sum_{e' \in \mathsf{Edges}_G(v')} p(e'),$
   $\forall v, v' \in V$

   b) $\sum_{e \in \mathsf{Edges}_G(v)} p(e) > 0 \forall\, v \in V$

OR

2. α*(G) =* β*'(G).*

Computation and the Defense Ratio

- Computation

Theorem 11. *FIND ATTACKER SYMMETRIC UNIFORM NE can be solved in polynomial time.*

- Defense Ratio

Theorem 12. *In a Attacker Symmetric Uniform Nash equilibrium, the Defense Ratio is*

$$\frac{|V|}{2} \text{ or } \alpha(G).$$

Thank you !