Coevolutionary Approach to Sequential Stackelberg Security Games

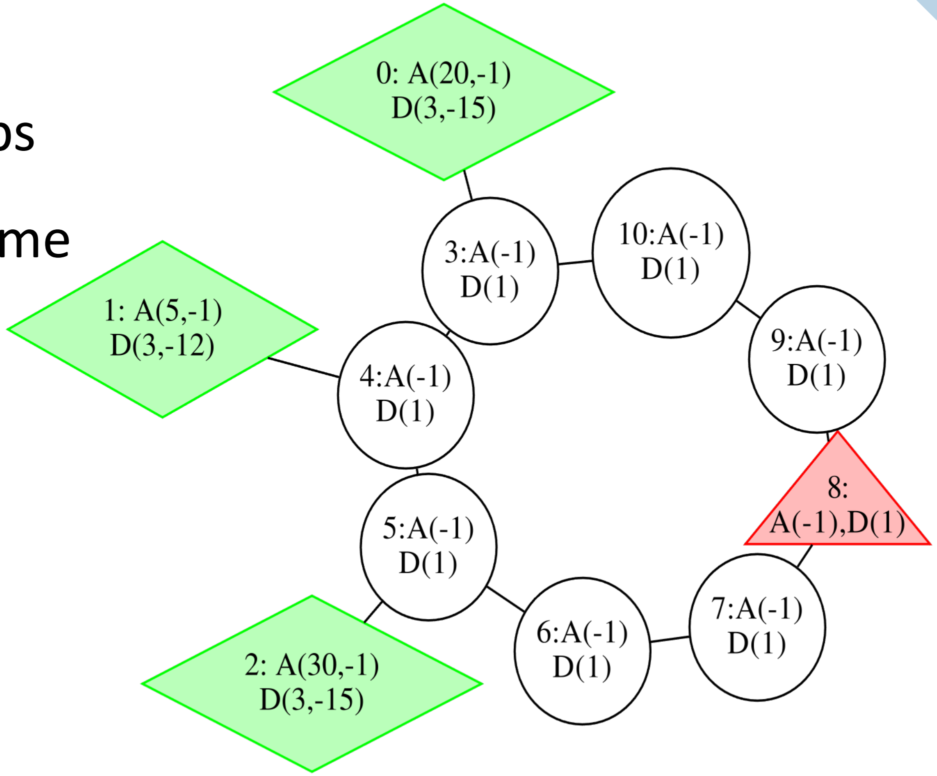
Adam Żychowski, Jacek Mańdziuk

Faculty of Mathematics and Information Science
Warsaw University of Technology

June 2022

Sequential Stackelberg Security Games

- Two players: the Leader/Defender (D) and the Follower/Attacker (A)
- A list of targets with payoffs: attack successful (U_{D-} , U_{A+}), attack unsuccessful (U_{D+} , U_{A-})
- *n* rounds (time steps)
- Player's pure strategy: list of actions in subsequent time steps
- Players commit to their strategies at the beginning of the game and cannot change them later on
- Non-zero sum games



Stackelberg equilibrium

- Defender commits to his/her strategy first
- Attacker, knowing the Defender's strategy, chooses his/her strategy
- Defender always commits to a mixed strategy

- **Stackelberg equilibrium**: a pair of players' strategies, for which strategy change by any of the players leads to his/her result deterioration.

$$(\pi_D^*, R(\pi_D^*)) \in \Pi_D \text{ x } \Pi_A$$

$$\pi_D^* = \operatorname{argmax}_{\pi_D \in \Pi_D} U_D(\pi_D, R(\pi_D))$$

$$R(\pi_D) = \operatorname{argmax}_{\pi_A \in \Pi_A} U_A(\pi_D, \pi_A)$$

$G \in \{D, A\}$ – *players (Defender, Attacker)*
Π_G – a set of player's G all mixed strategies
U_G – payoff of player G

Additional assumption: ties from Attacker's perspective (strategies with equal Attacker's payoff) are broken in favour of the Defender (**Strong Stackelberg equilibrium - SSE**)

Real-life applications

Federal Air Marshal Service

US Coast Guard in Boston Harbor

Los Angeles Airport

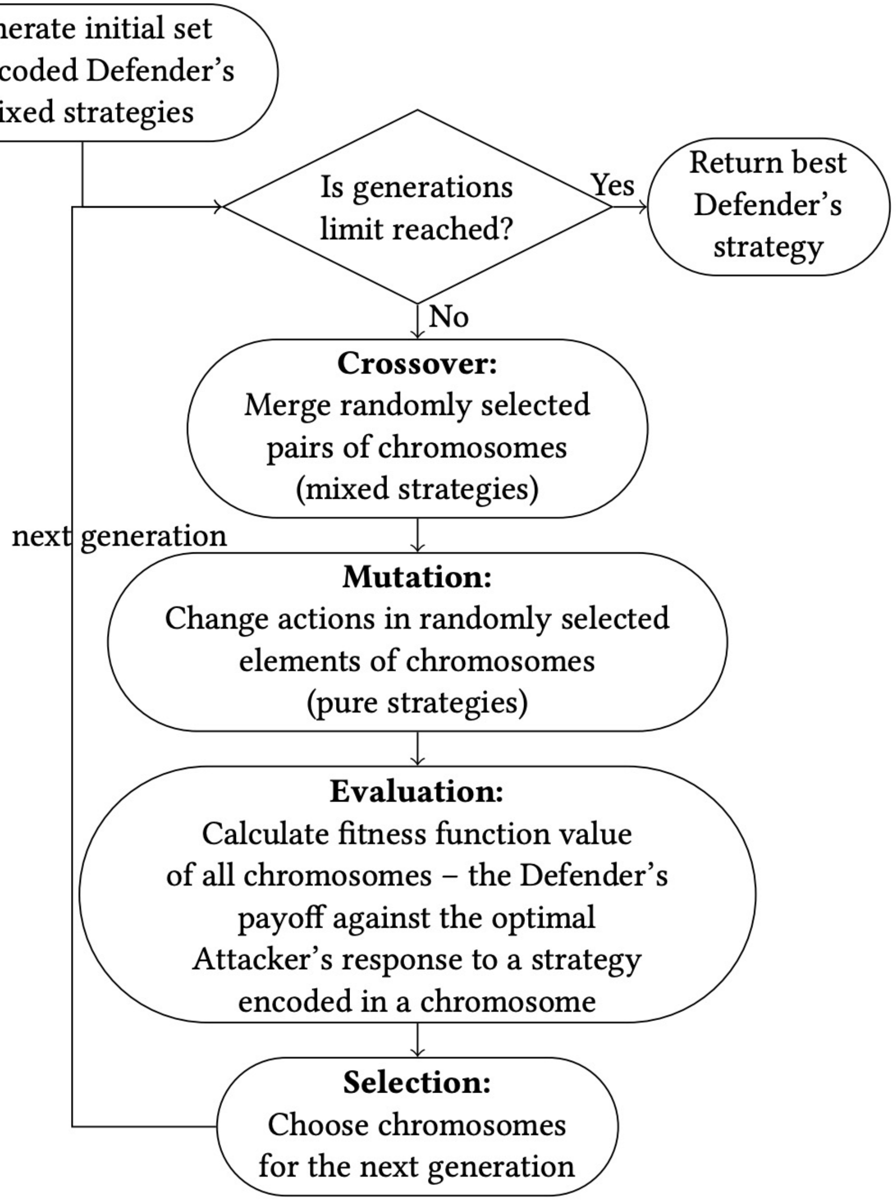
Poaching in Uganda

Tickets control in Los Angeles

Basic evolutionary approach (EASG)

A. Żychowski, J. Mańdziuk. *Evolution of Strategies in Sequential Security Games.* (AAMAS 2021), 1434-1442. 2021.

- Defender’s mixed strategy optimization encoded as a list of pure strategies with corresponding probabilities
- For any Defender’s mixed strategy there exists at least one Attacker’s **pure strategy** which is the optimal response
- To evaluate given Defender’s strategy it is sufficient to iterate over all Attacker’s pure strategies



Motivation

Looking for the optimal Attacker's response is **the most time-consuming algorithm step** (requires iteration over all possible Attacker's strategies and compute payoffs for each of them)

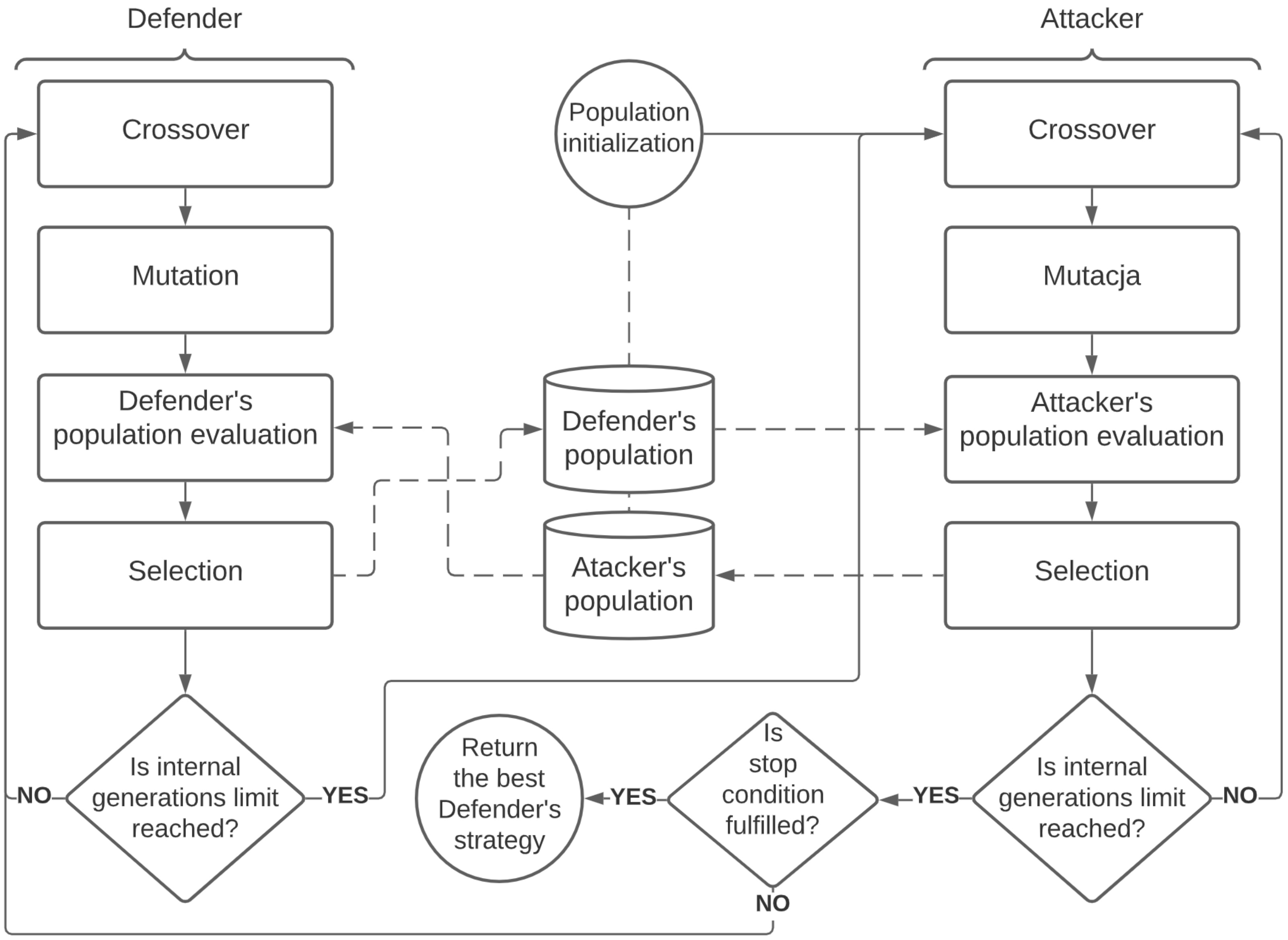
There may be many Attacker's strategies (even infinitely many)

Usually **most of Attacker's strategies are irrelevant** (weak) or similar

There is a need for a method which is able to correctly identify relevant strategies

solution: **coevolution** – competing populations of Defender's and Attacker's strategies

Coevolutionary approach (CoEvoSG)



Coevolutionary approach - operators

- Defender's population and their evolutionary operators – no changes
- **Crossover** in Attacker's population: one-point crossover

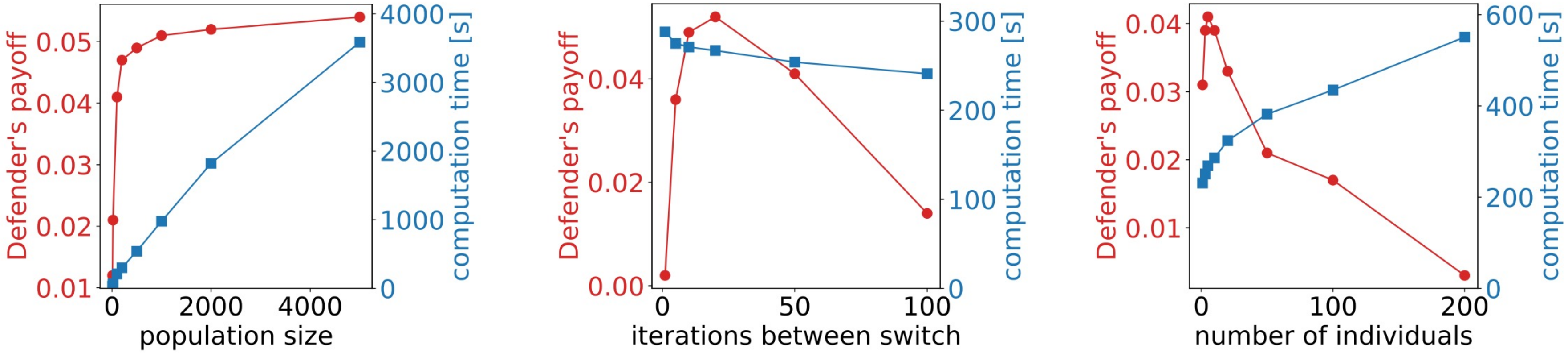
$$\pi_A^1 = (a_1^1, a_2^1, \ldots, a_m^1) \times \pi_A^2 = (a_1^2, a_2^2, \ldots, a_m^2)$$

$$\pi_A'^1 = (a_1^1, a_2^1, \ldots a_i^1, a_{i+1}^2, \ldots, a_m^2) \quad \pi_A'^2 = (a_1^2, a_2^2, \ldots a_i^2, a_{i+1}^1, \ldots, a_m^1)$$

- **Mutation** in Attacker's population: change of action to another one (chosen randomly)
- Attacker's strategy **evaluation**: maximum of Attacker's payoff vs N_{top} = 10 best strategies from Defender's population

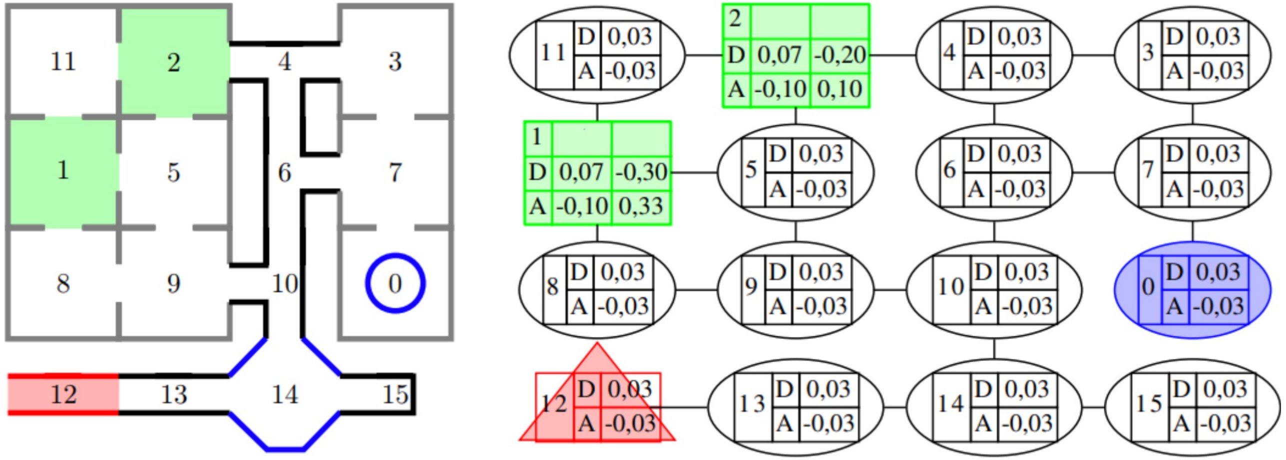
Parameterization

- Defender’s population size: 200
- Attacker’s population size: 200
- Crossover probability: 0.8
- Mutation probability: 0.5
- Selection: binary tournament with selection pressure 0.9
- Elite size: 2
- Maximal number of generations: 1000
- Maximal number of generations without improvement: 20
- Number of consecutive generation for each player: 20
- Number of the best individuals from the Defender’s population involved in the Attacker’s strategies evaluation: 10



Warehouse Games (WHG)

- Game played on undirected graphs
- Set of distinct vertices – targets
- Action (in each time step): move to one of the neighbour vertices or stay in current one
- Game ends if:
  - both players are located in the same vertex in the same time step
  - the Attacker reaches one of the targets and is not caught
  - none of above conditions is satisfied in given time steps



FlipIt Games (FIG)

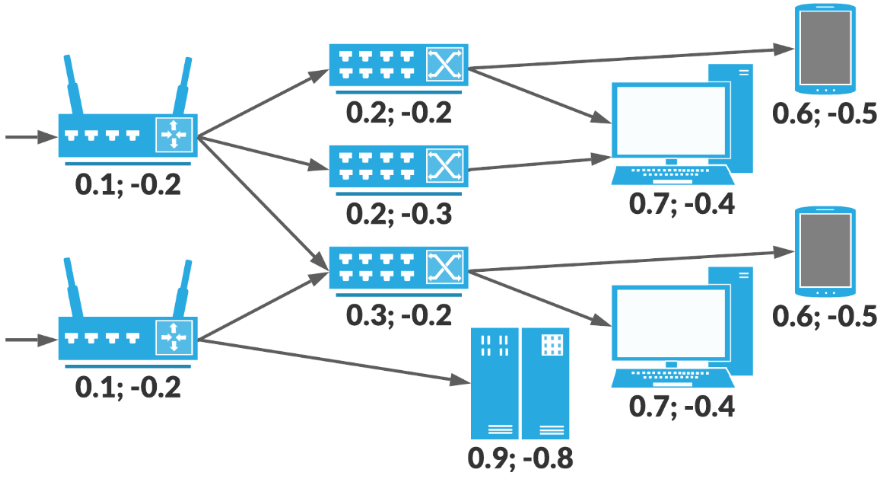
- Cybersecurity scenario inspiration
- Game played on directed graph
- Each player (in subsequent rounds) chooses one node which they want to take control of (*flip* the node)
- Taking control over the vertex (flip action) is successful only if
  - the player controls at least one of predecessor vertices (unless it is an entry node),
  - the current owner of this vertex does not take the flip action on it in the same time step

Final payoff: the rewards in all nodes controlled by that player after each time step and the costs of all flip attempts (either successful or not).

$$U_g = \sum_{s \in \{1,\ldots,m\}} \sum_{v \in R_s(g)} U_v^+ + \sum_{s \in \{1,\ldots,m\}} U_{v_s^g}^-$$

$R_s(g)$ - a subset of nodes controlled by player g in round s

v_s^g - a node which player g tries to take control in round s



Experimental setup

- 240 WHG games
  - time steps: 3, 4, 5, 6, 8, 10, 15, 20
  - vertices: 15, 20, 25, 30, 40, 50

- 280 FIG games
  - time steps: 3, 4, 5, 6, 8, 10, 15, 20
  - vertices: 5, 10, 15, 20, 25, 30, 40

- Payoffs drawn randomly from interval [-1,1]
- Random Watts–Strogatz graphs with an average vertex degree $d_{avg} = 3$

Results - payoffs

WHG				
$\|V\|$	**C2016**	**O2UCT**	**EASG**	**CoEvoSG**
15	0.052	0.051	0.051	0.050
20	0.054	0.053	0.052	0.050
25	0.048	0.046	0.045	0.043
30	-	0.044	0.042	0.039
40	-	-	0.040	0.036
50	-	-	-	0.029

FIG				
$\|V\|$	**C2016**	**O2UCT**	**EASG**	**CoEvoSG**
5	0.890	0.887	0.886	0.886
10	0.854	0.851	0.847	0.845
15	0.811	0.807	0.802	0.798
20	-	0.784	0.780	0.772
25	-	-	0.754	0.746
30	-	-	-	0.730
40	-	-	-	0.722

Average Defender's payoffs with respect to the number of graph vertices

Optimal result:

WHG: 38/60
FIG: 29/45

Averaged difference:

WHG: 0.0023

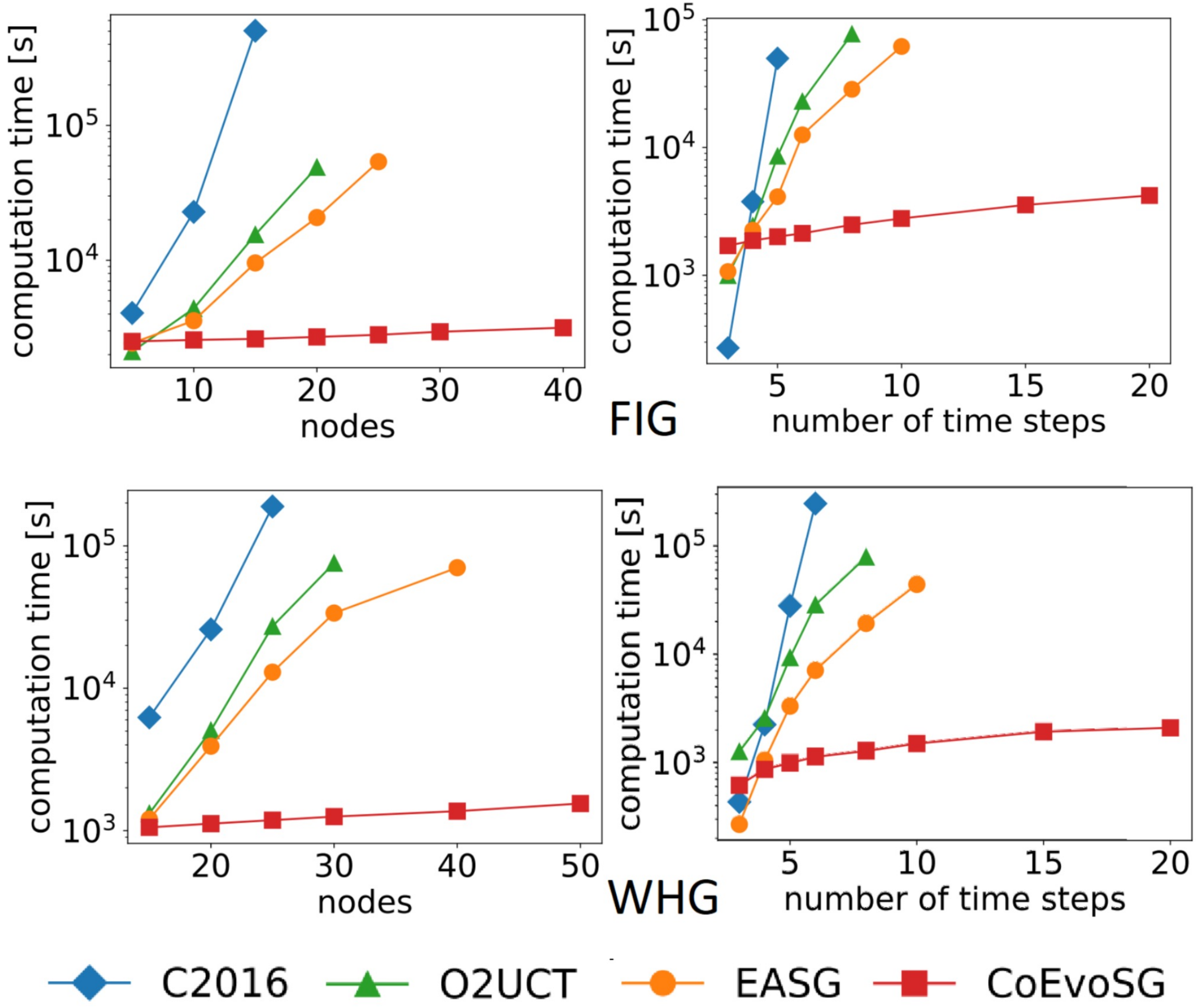
FIG: 0.0137

WHG				
m	**C2016**	**O2UCT**	**EASG**	**CoEvoSG**
3	0.043	0.043	0.043	0.043
4	0.052	0.050	0.050	0.049
5	0.055	0.054	0.053	0.052
6	0.058	0.056	0.054	0.051
8	-	0.053	0.051	0.048
10	-	-	0.048	0.044
15	-	-	-	0.040
20	-	-	-	0.038

FIG				
m	**C2016**	**O2UCT**	**EASG**	**CoEvoSG**
3	0.823	0.821	0.820	0.817
4	0.817	0.812	0.808	0.805
5	0.810	0.801	0.798	0.791
6	-	0.794	0.792	0.791
8	-	0.789	0.784	0.781
10	-	-	0.780	0.778
15	-	-	-	0.774
20	-	-	-	0.761

Average Defender's payoffs with respect to the number of time steps

Results – computation time



Conclusions

- Security Games is an interesting research area with important real-life applications
- new metaheuristic method
- better time and memory scalability
- viable alternative to exact methods and state-of-the-art heuristics
- despite a significant reduction of search space results are close to the optimal ones

Thank you