5th Polish Conference on Artificial Intelligence

Hall of Fame in Coevolutionary Algorithm for Stackelberg Security Games

Adam Żychowski[1], Jacek Mańdziuk[1], Andrew Perrault[2]

[1] Warsaw University of Technology, Faculty of Mathematics and Information Science
[2]The Ohio State University, Department of Computer Science and Engineering

19 April 2024

Abstract

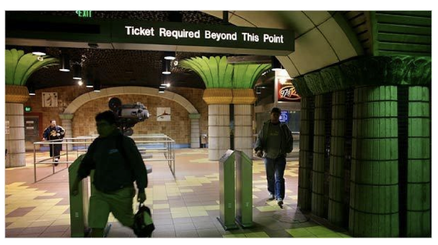
Stackelberg Security Games is a popular game-theoretic model for strategic interactions between a Defender and an Attacker. The computational challenges of identifying optimal strategies for larger games led to the development of the CoEvoSG coevolutionary method [1]. This paper introduces an extension to CoEvoSG, incorporating a **Hall of Fame (HoF) mechanism with Mixed Nash Equilibrium**. **The HoF stores successful strategic configurations, enhancing algorithm robustness.** Results across distinct game types demonstrate that the proposed method consistently outperforms the baseline CoEvoSG algorithm with standard HoF approach. This improvement is achieved with minimal computation time increase.

Federal Air Marshal Service

US Coast Guard in Boston Harbor

Los Angeles Airport

Poaching in Uganda



Tickets control in Los Angeles

Stackelberg Security Games

- Two asymmetrical players: **Defender (D) and Attacker (A)**
- Each game is composed of m time steps.
- Each player chooses an action to be performed in each time step.
- A player's *pure strategy* $\boldsymbol{\sigma_P}$ ($\boldsymbol{P \in \{D, A\}}$) is a sequence of their actions in consecutive time steps: $\boldsymbol{\sigma_P = (a_1, a_2, \ldots, a_m)}$.

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 players leads to his/her result deterioration.

$$(\pi_D^*, R(\pi_D^*)) \in \Pi_D \times \Pi_A$$

$$\pi_D^* = \text{argmax}_{\pi_D \in \Pi_D} U_D(\pi_D, R(\pi_D))$$
$$R(\pi_D) = \text{argmax}_{\pi_A \in \Pi_A} U_A(\pi_D, \pi_A)$$

Π_P - a set of player's P all mixed strategies
U_P - payoff of player P, $P \in \{D, A\}$

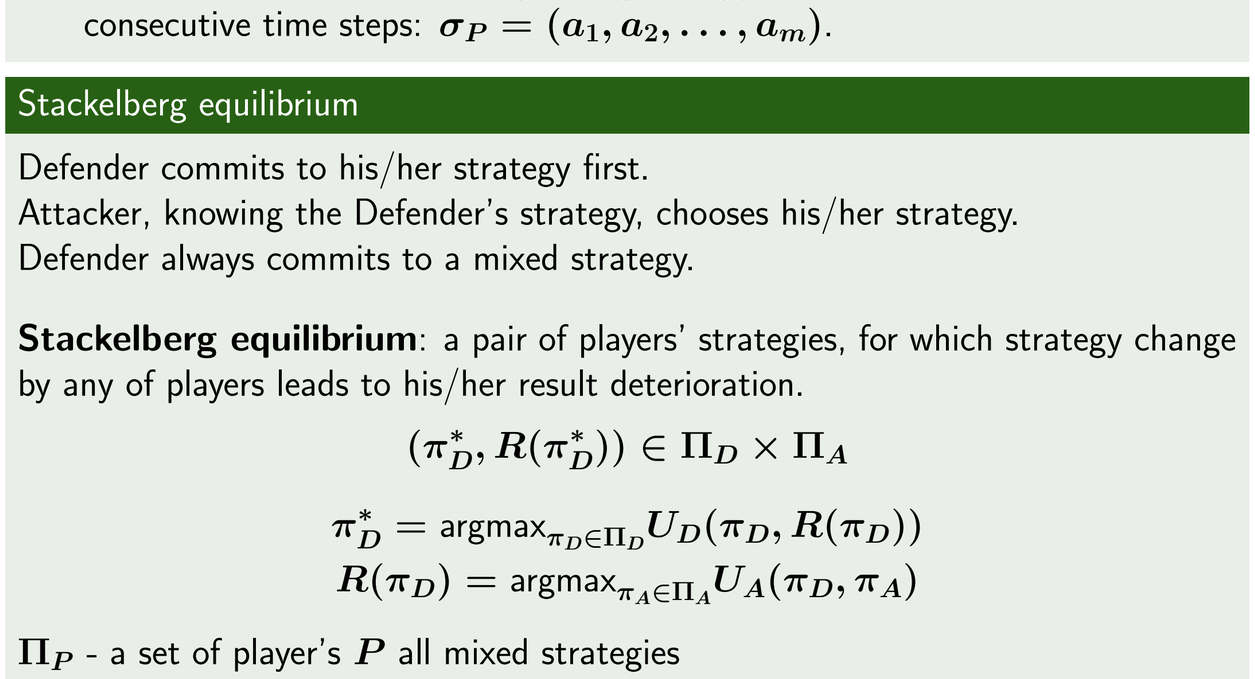


Figure: An overview of the CoEvoSG+HoF method.

Contribution summary

- We expanded the CoEvoSG [1] algorithm by incorporating the Hall of Fame archive mechanism featuring Nash Equilibrium.
- Tested on 3 different game types: FlipIt Games, Search Games and Warehouse Games with various sizes (up to 50 nodes).
- Improved results of the baseline CoEvoSG algorithm without significant time increasement.
- Similar idea can be used for coevolutionary algorithms in other domains [2].

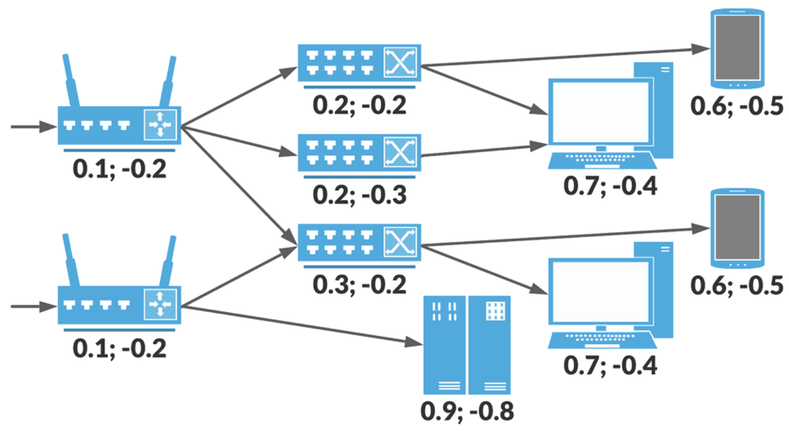


Figure: Example FlipIt game.

Results

	C2016	O2UCT	EASG	CoEvoSG	CoEvoSG+HoF	**CoEvoSG+NEHoF**
5	0.890	0.887	0.886	0.886	0.886	0.887
10	0.854	0.848	0.847	0.845	0.845	0.849
15	0.811	0.805	0.802	0.798	0.801	0.806
20	-	0.779	0.780	0.772	0.775	0.776
25	-	-	0.754	0.746	0.751	0.754
30	-	-	-	0.730	0.732	0.735
40	-	-	-	0.722	0.726	0.733

Table: Averaged Defender's payoff with respect to game nodes for FlipIt games.

	C2016	O2UCT	EASG	CoEvoSG	CoEvoSG+HoF	**CoEvoSG+NEHoF**
15	0.122	0.116	0.115	0.115	0.115	0.116
20	0.117	0.107	0.106	0.101	0.104	0.106
25	-	0.119	0.117	0.115	0.116	0.119
30	-	-	0.136	0.135	0.135	0.135
40	-	-	-	0.150	0.152	0.156
50	-	-	-	0.139	0.144	0.146

Table: Averaged Defender's payoff with respect to game nodes for Search games.

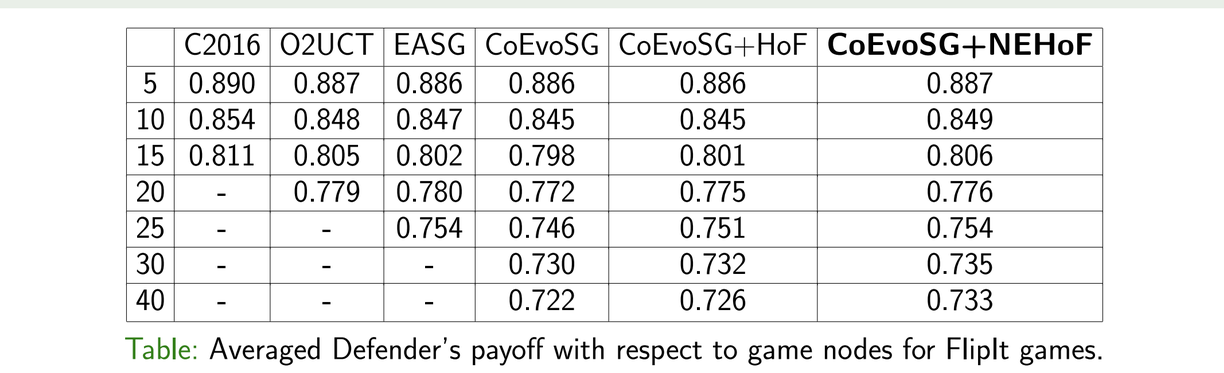


Figure: Computation times with respect to game nodes (N) for FlipIt and Search games.

References

[1] A. Żychowski, J. Mańdziuk. Coevolution of Players Strategies in Security Games. Journal of Computational Science 68, 101980. 2023.
[2] A. Żychowski, A. Perrault, J. Mańdziuk. Coevolutionary Algorithm for Building Robust Decision Trees under Minimax Regret. AAAI 2024, 21869-21877. 2024.