4th Polish Conference on Artificial Intelligence

Optimized mutation operator in evolutionary approach to Stackelberg Security Games

Adam Żychowski, Jacek Mańdziuk

a.zychowski@mini.pw.edu.pl, j.mandziuk@mini.pw.edu.pl

Faculty of Mathematics and Information Science

Warsaw University of Technology

April 2023

Security Games

- Two asymmetrical players: **Defender and Attacker**
- 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 σ_P $(P \in \{D, A\})$ is a sequence of their actions in consecutive time steps: $\sigma_P = (a_1, a_2, \ldots, a_m)$.

- **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

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

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

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

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

Goal: find optimal Defender's strategy

Real-life applications

Federal Air Marshal Service

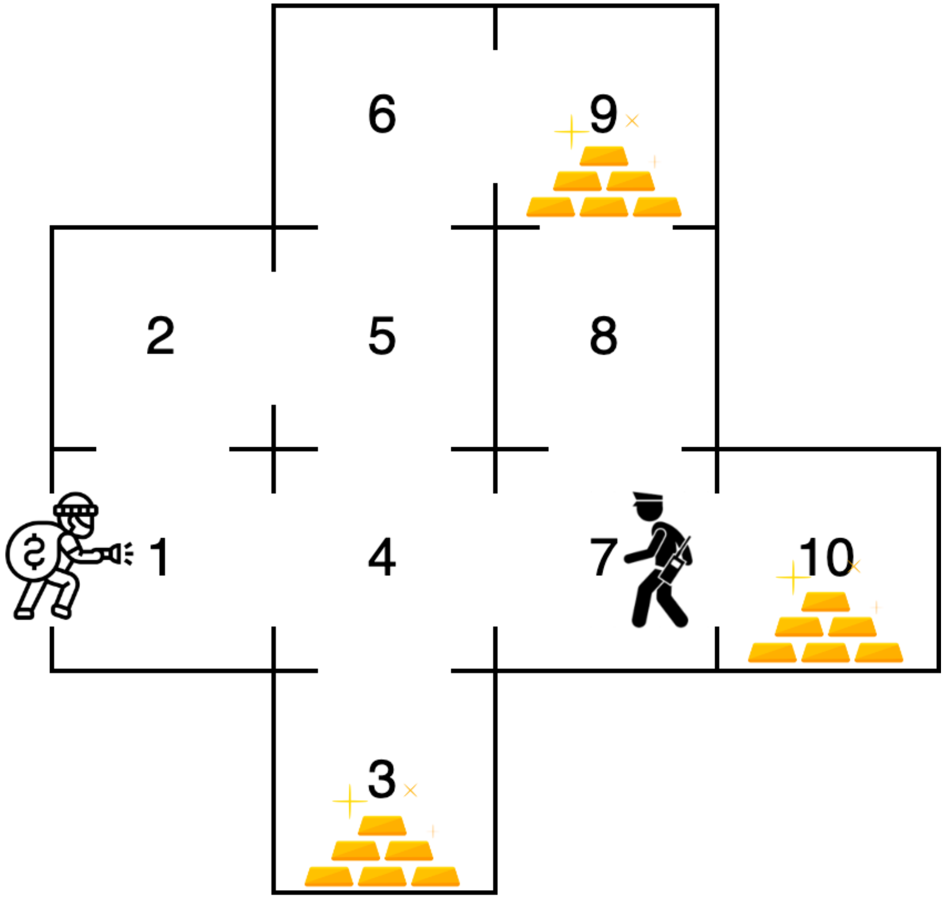
US Coast Guard in Boston Harbor

Los Angeles Airport

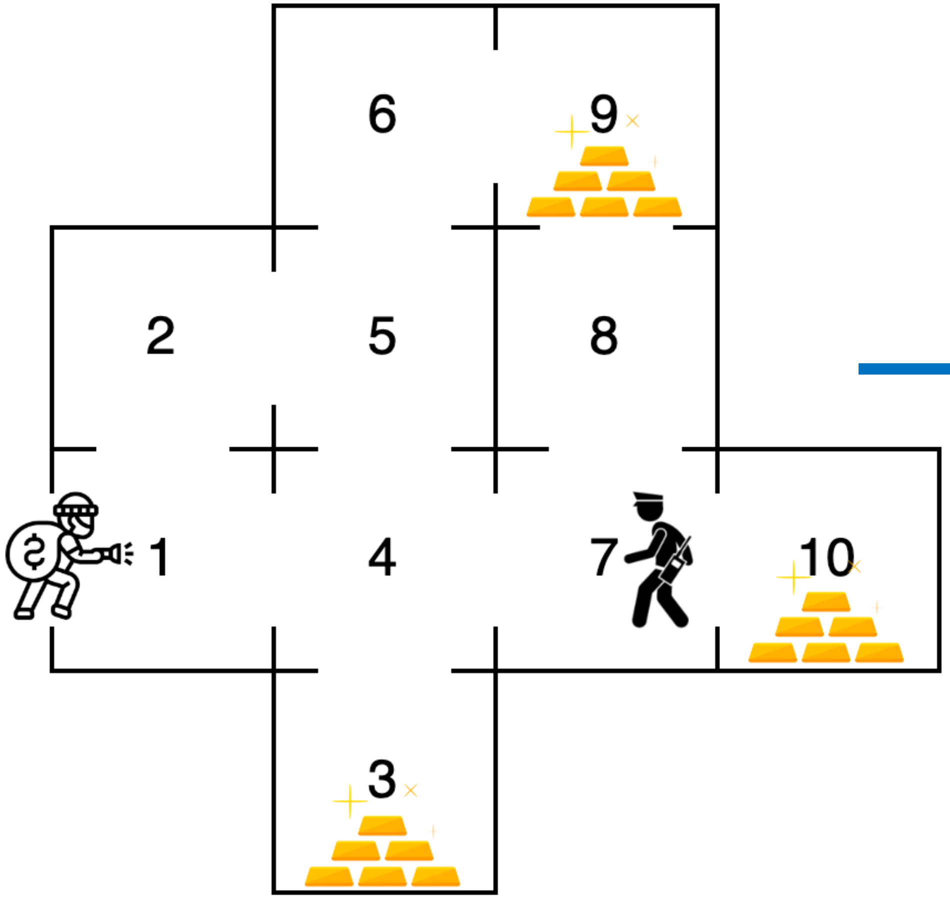
Poaching in Uganda

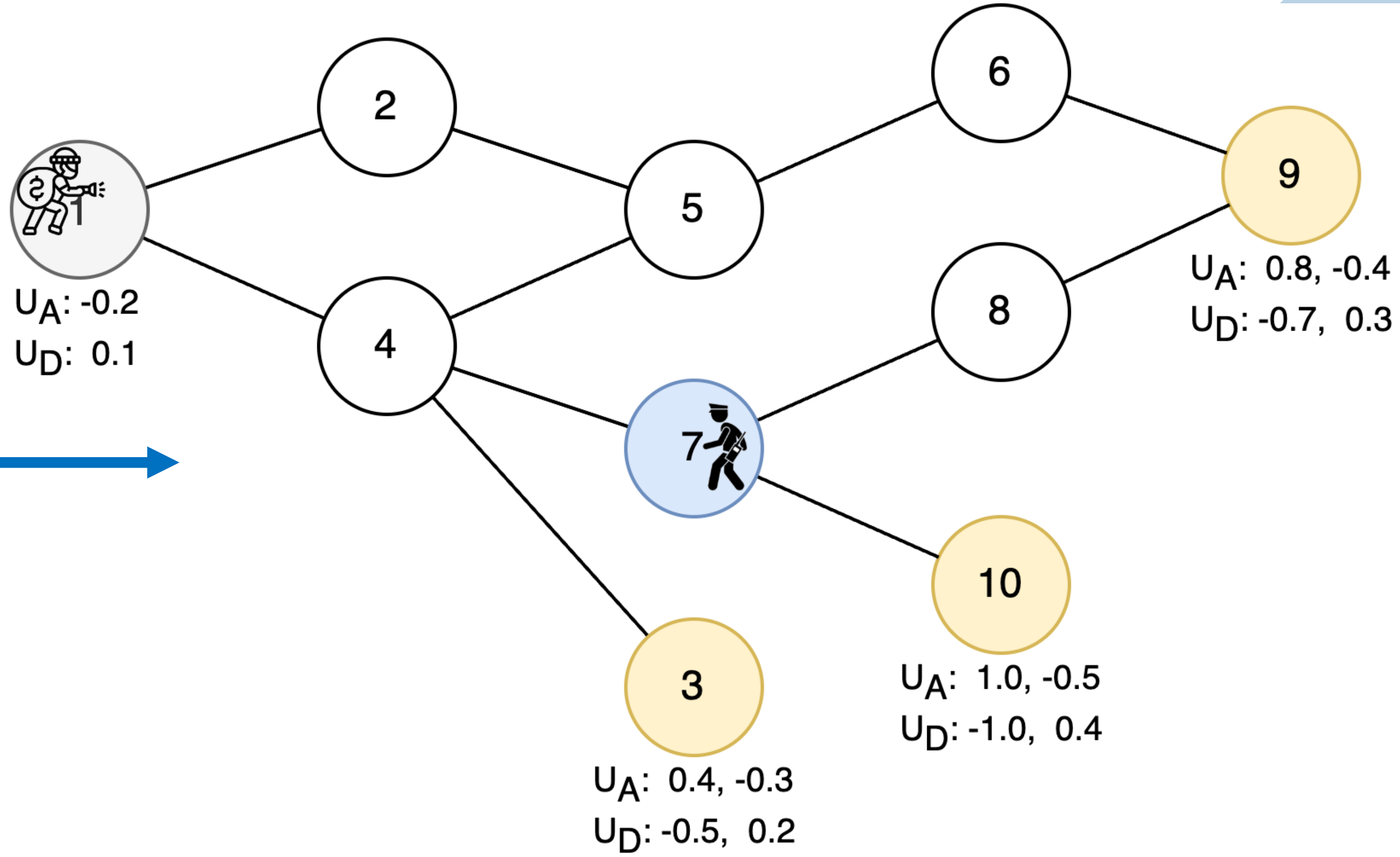
Tickets control in Los Angeles

Example

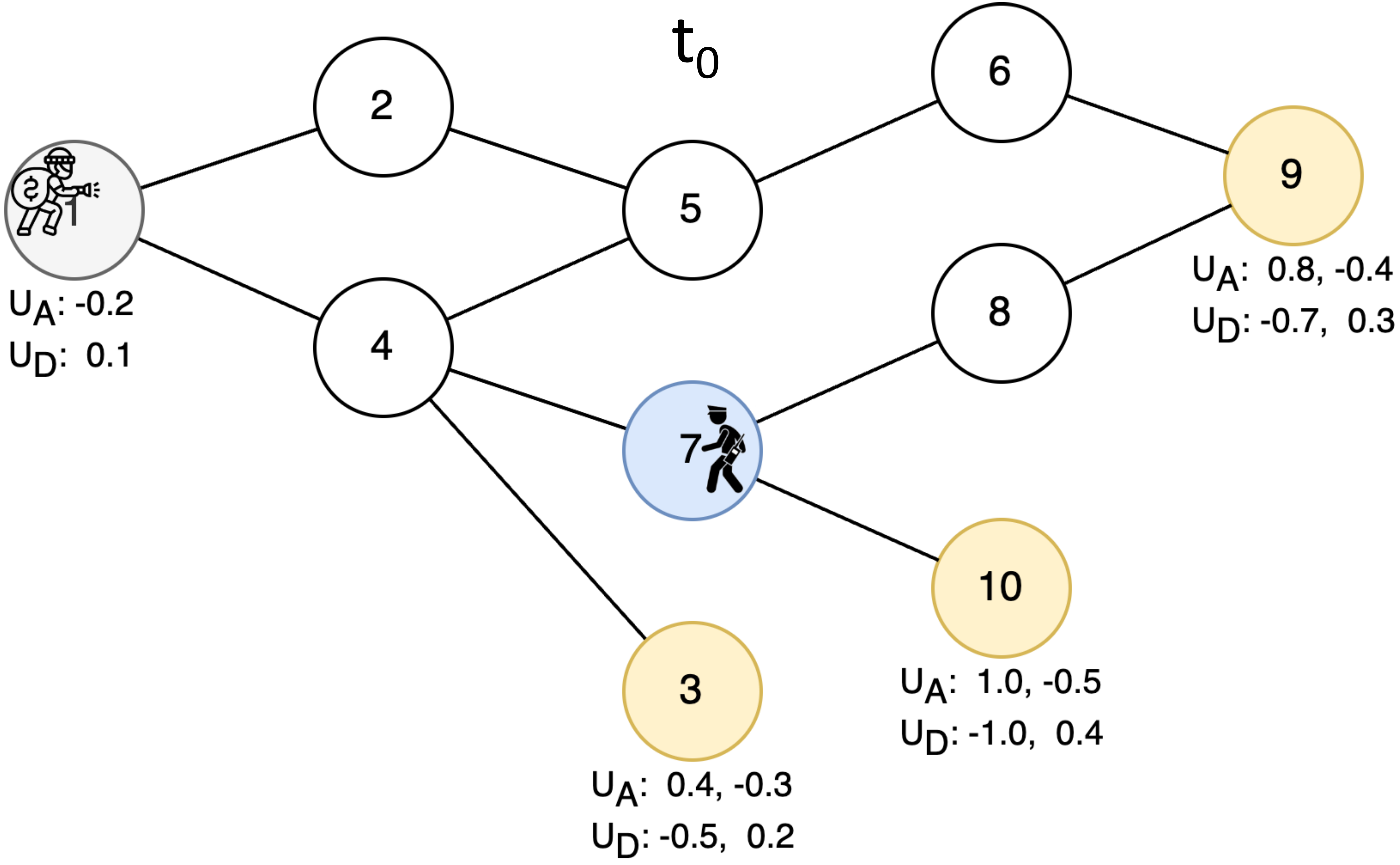


Example

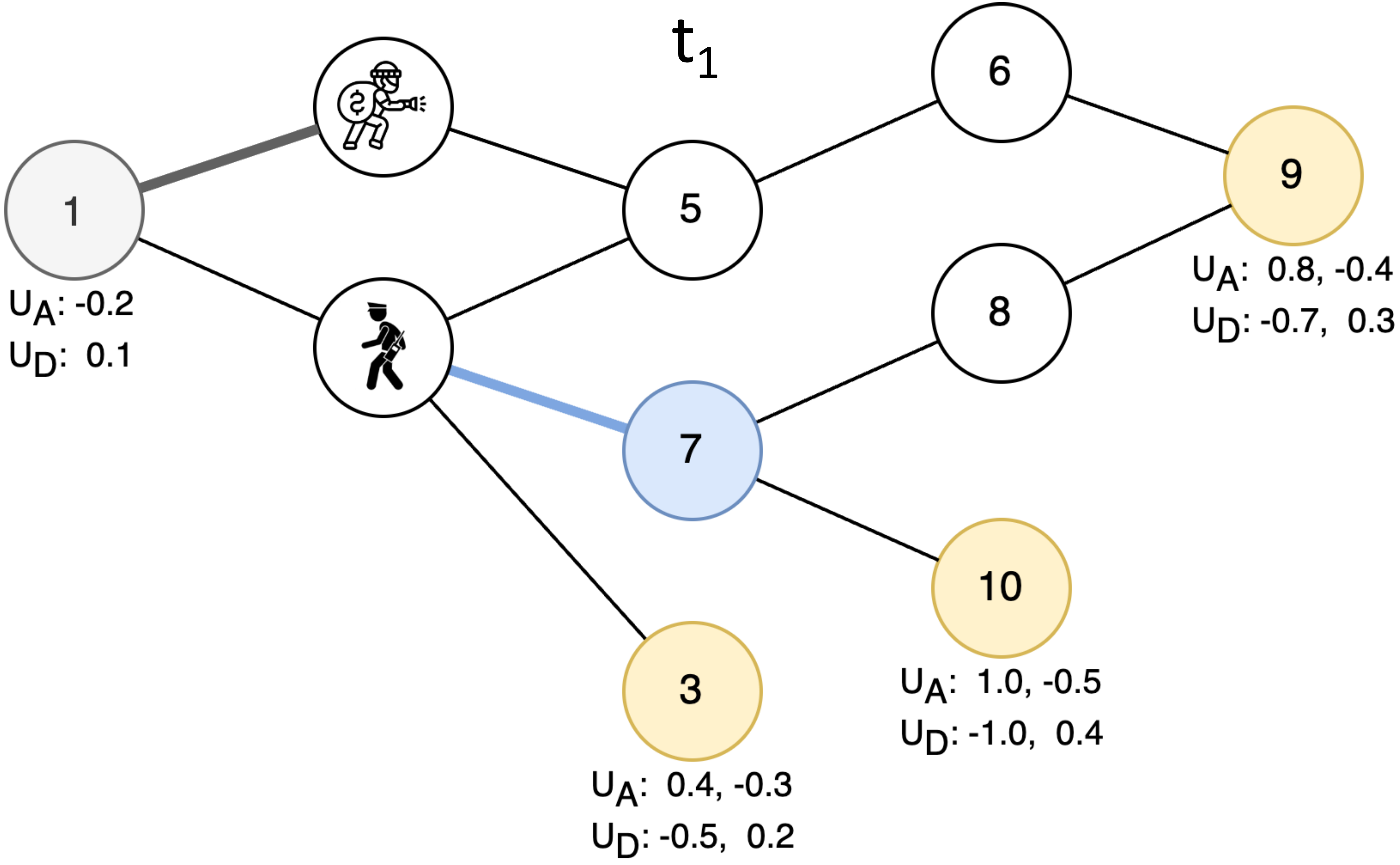

6
9
2
5
8
1
4
7
10
3


1
U_A: -0.2
U_D: 0.1
2
4
5
6
7
8
3
U_A: 0.4, -0.3
U_D: -0.5, 0.2
9
U_A: 0.8, -0.4
U_D: -0.7, 0.3
10
U_A: 1.0, -0.5
U_D: -1.0, 0.4

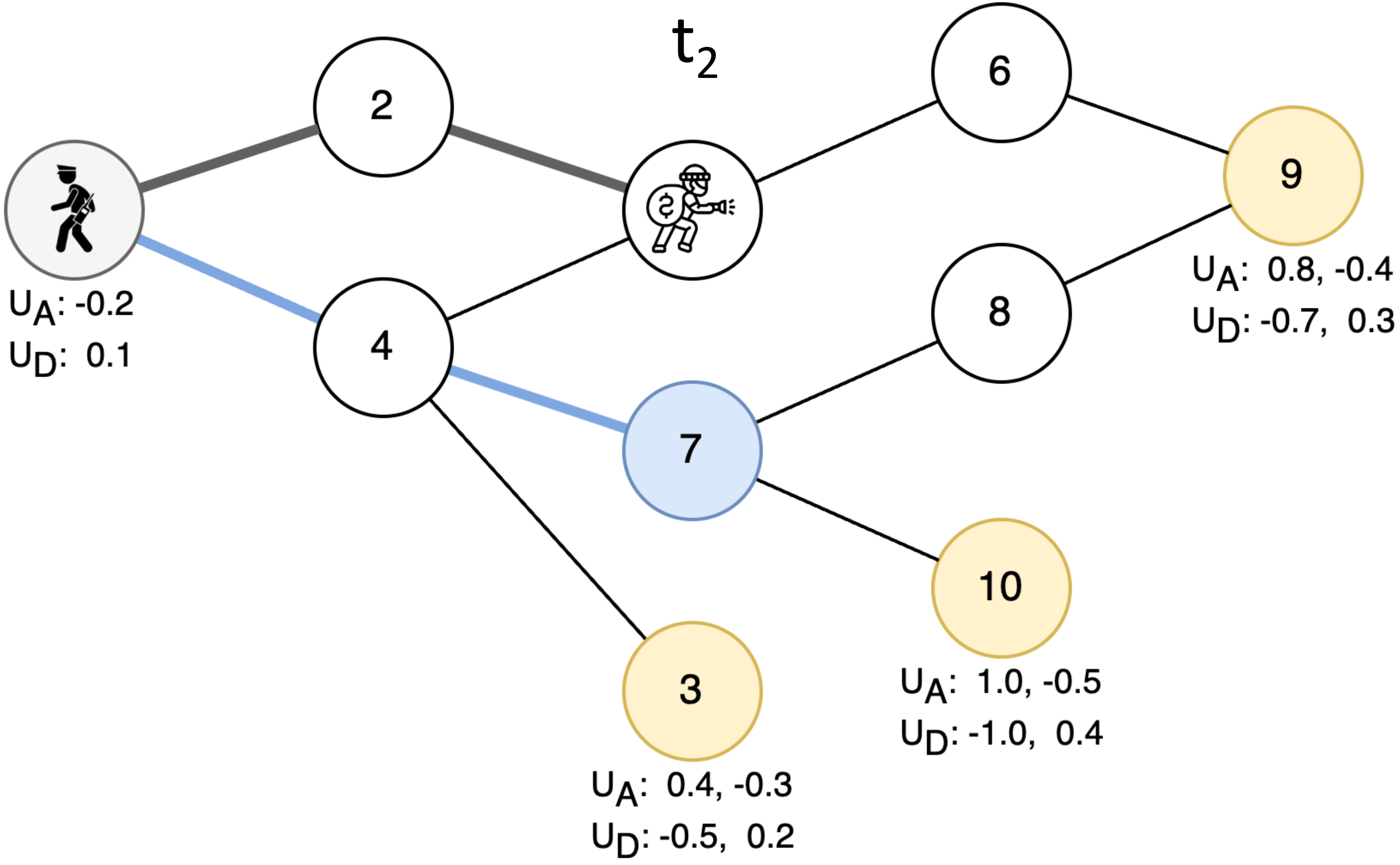
Example – scenario 1



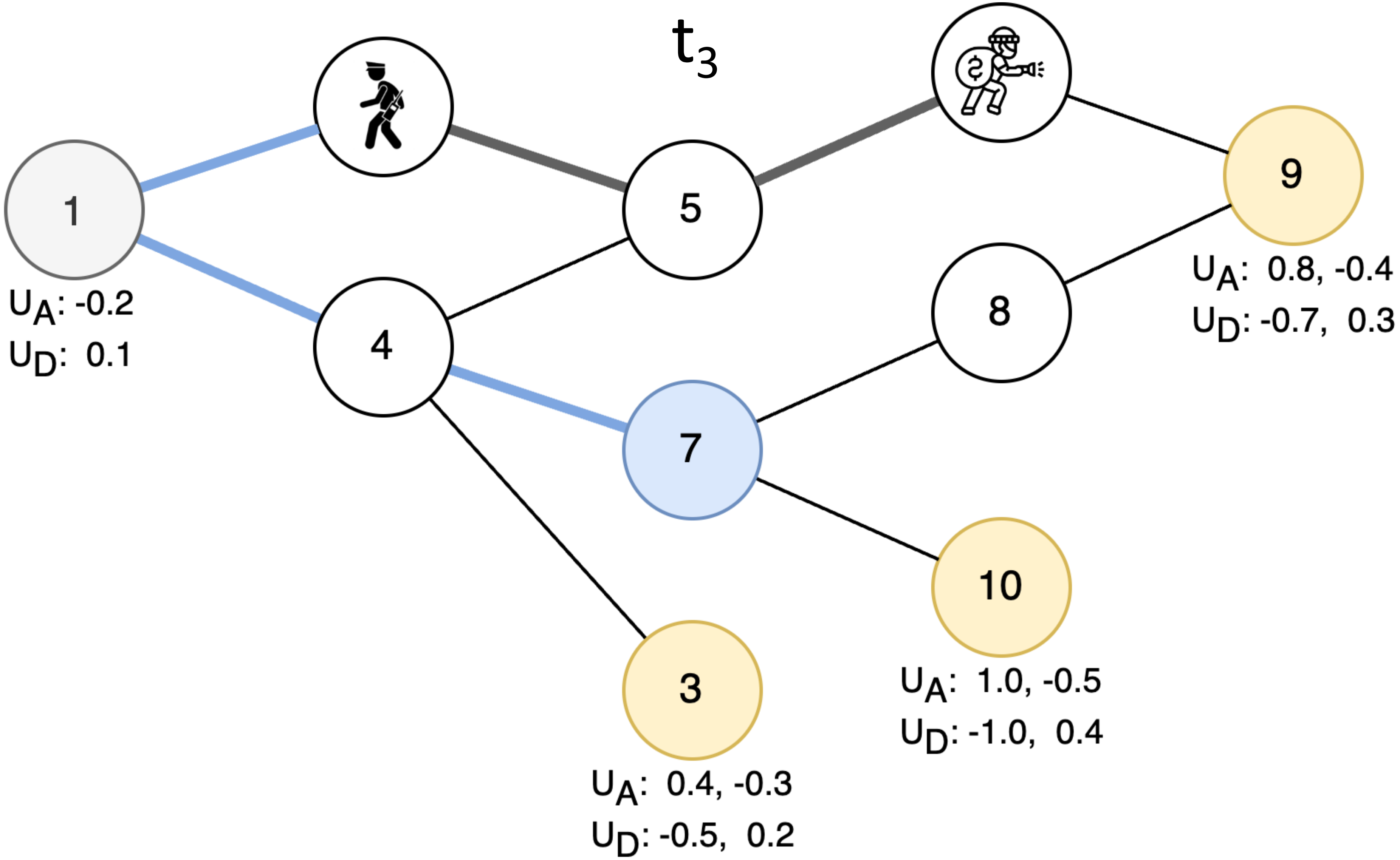
Example – scenario 1



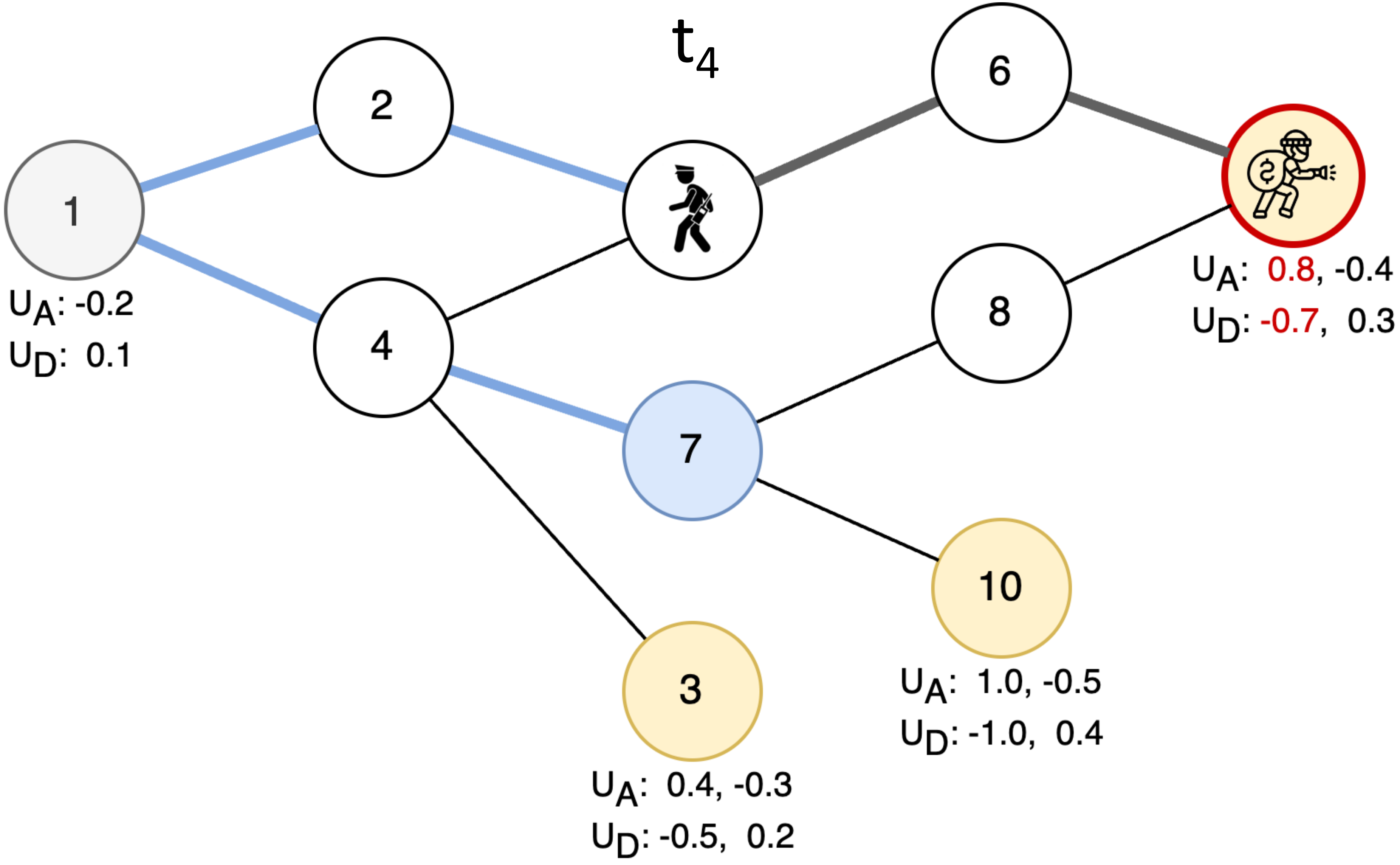
Example – scenario 1



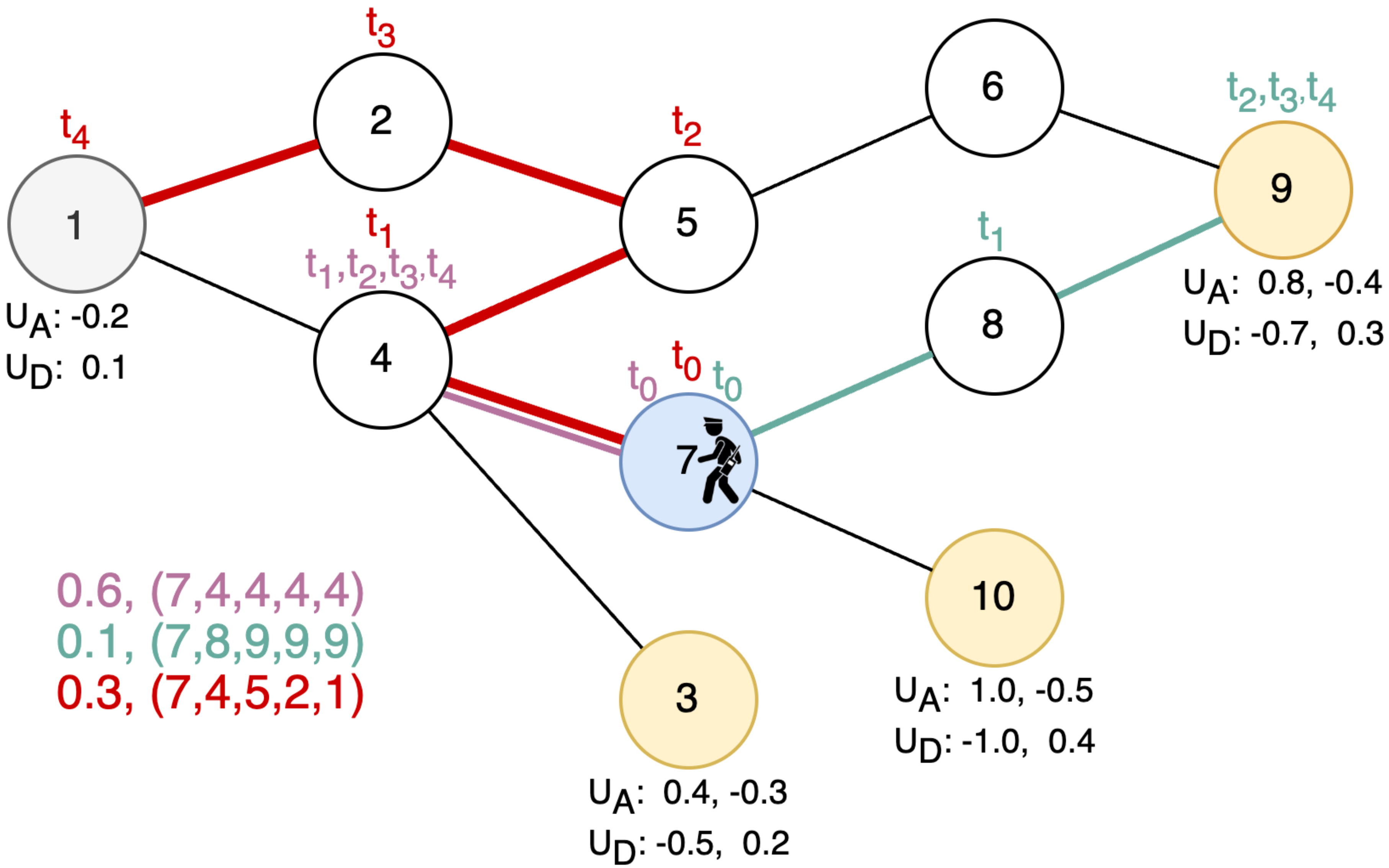
Example – scenario 1



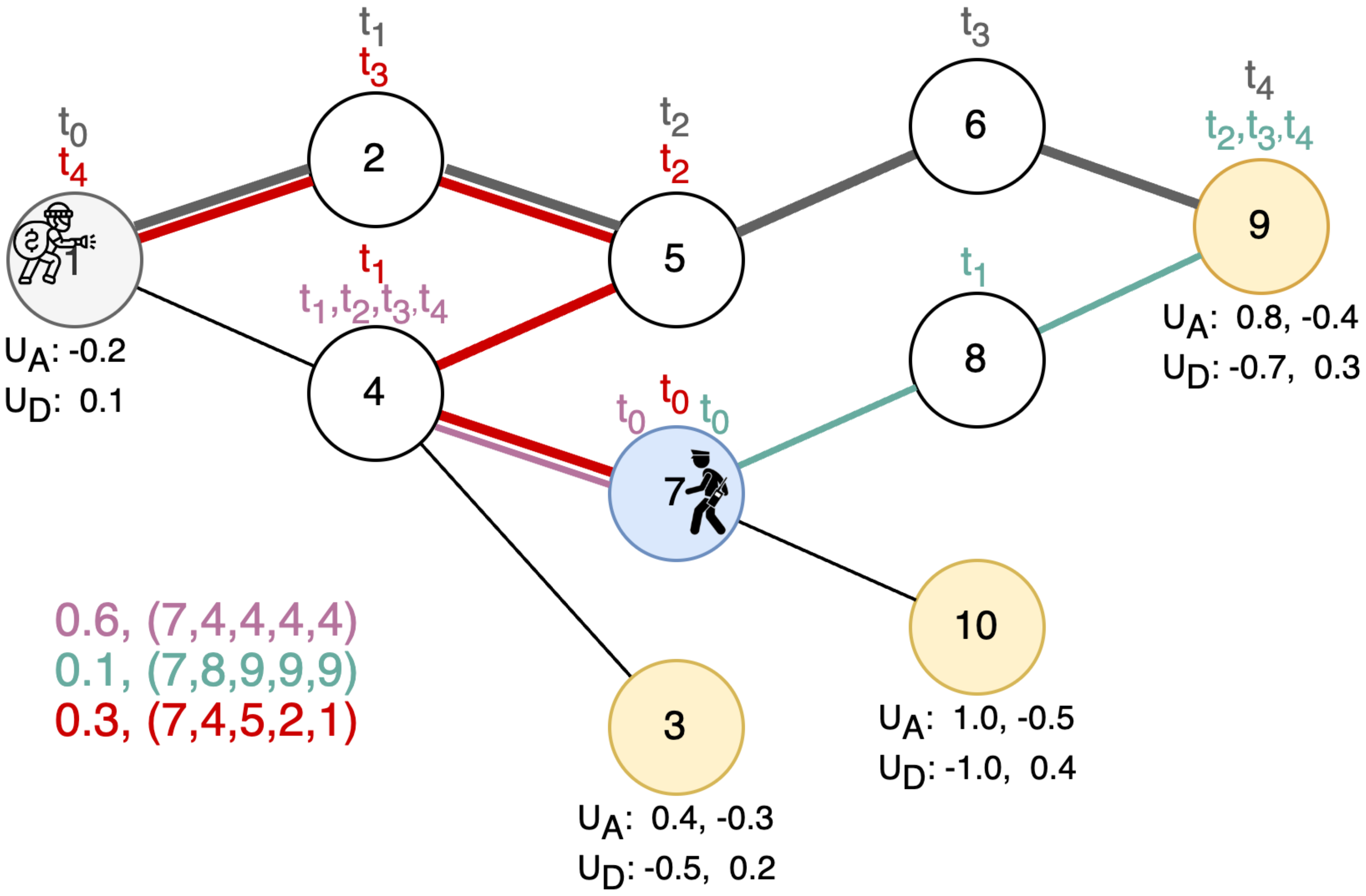
Example – scenario 1



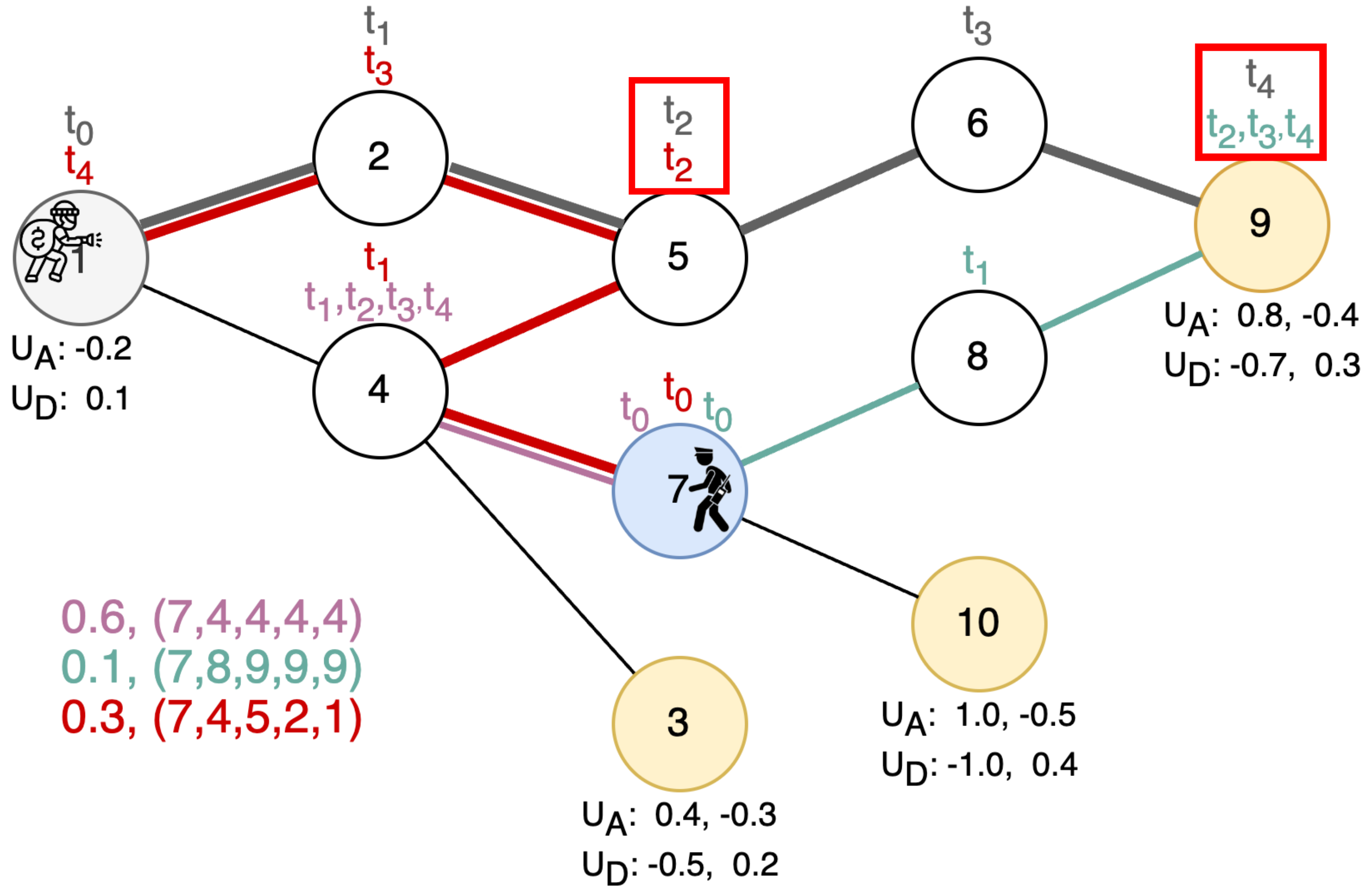
Example - mixed strategy



Example - mixed strategy



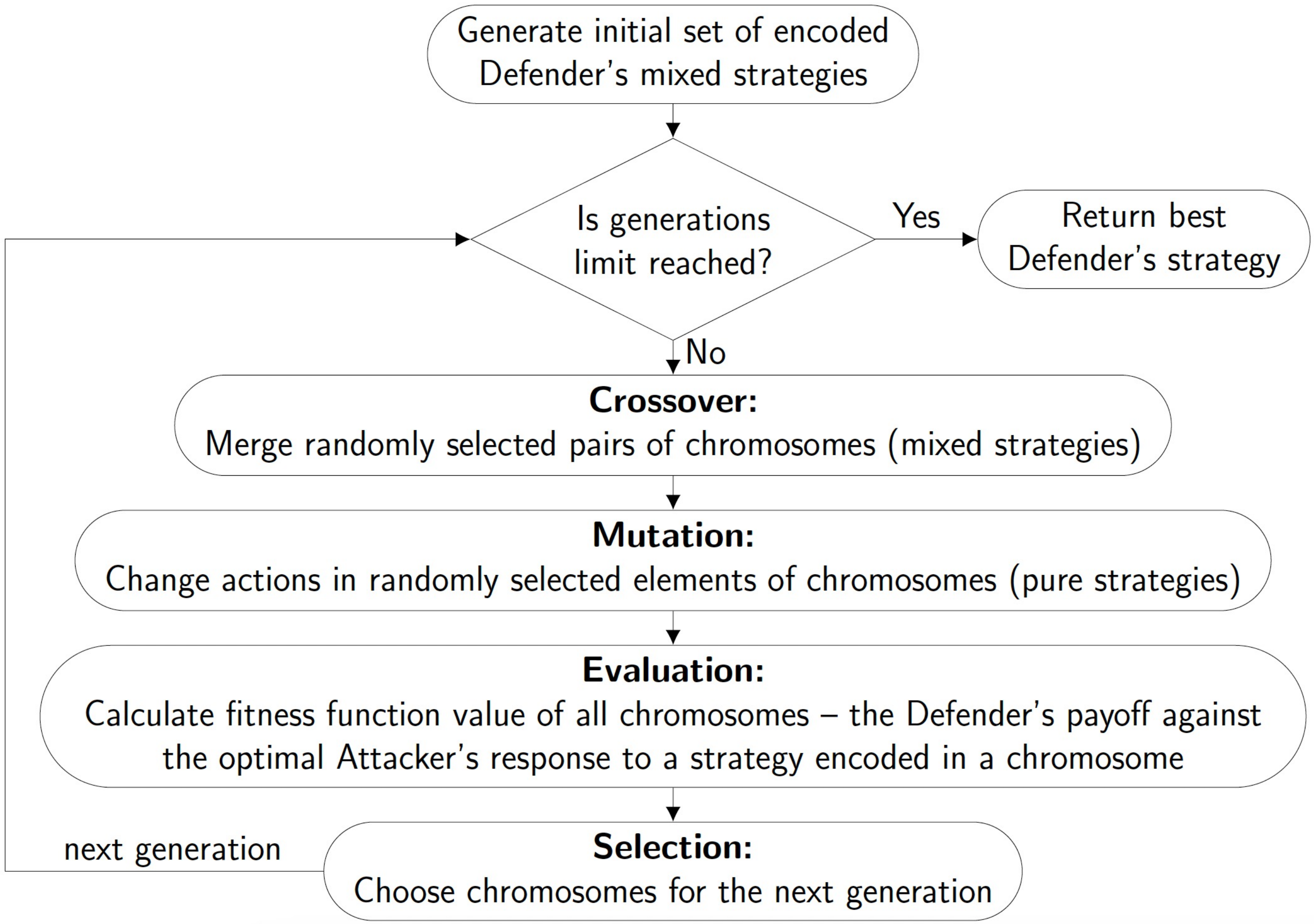
Example - mixed strategy



$$U_A(\pi_D, \pi_A) = 0.3 \cdot -0.2 + 0.1 \cdot -0.4 + 0.6 \cdot 0.8 = 0.38$$

$$U_D(\pi_D, \pi_A) = 0.3 \cdot 0.1 + 0.1 \cdot 0.3 + 0.6 \cdot -0.7 = -0.36$$

Evolutionary Algorithm for Security Games (EASG)



Żychowski A., Mańdziuk J. *Evolution of Strategies in Sequential Security Games*. Proceedings of the 20th AAMAS conference, pages 1434-1442. 2021

EASG - crossover

- Crossover role: combining existing solutions
- Each individual takes part in crossover with crossover rate probability p_k

$$CH_{1-2} = \{(\sigma_1^1, \frac{p_1^1}{2}), \ldots, (\sigma_{l_1}^1, \frac{p_{l_1}^1}{2}), (\sigma_1^2, \frac{p_1^2}{2}), \ldots, (\sigma_{l_2}^2, \frac{p_{l_2}^2}{2})\}$$

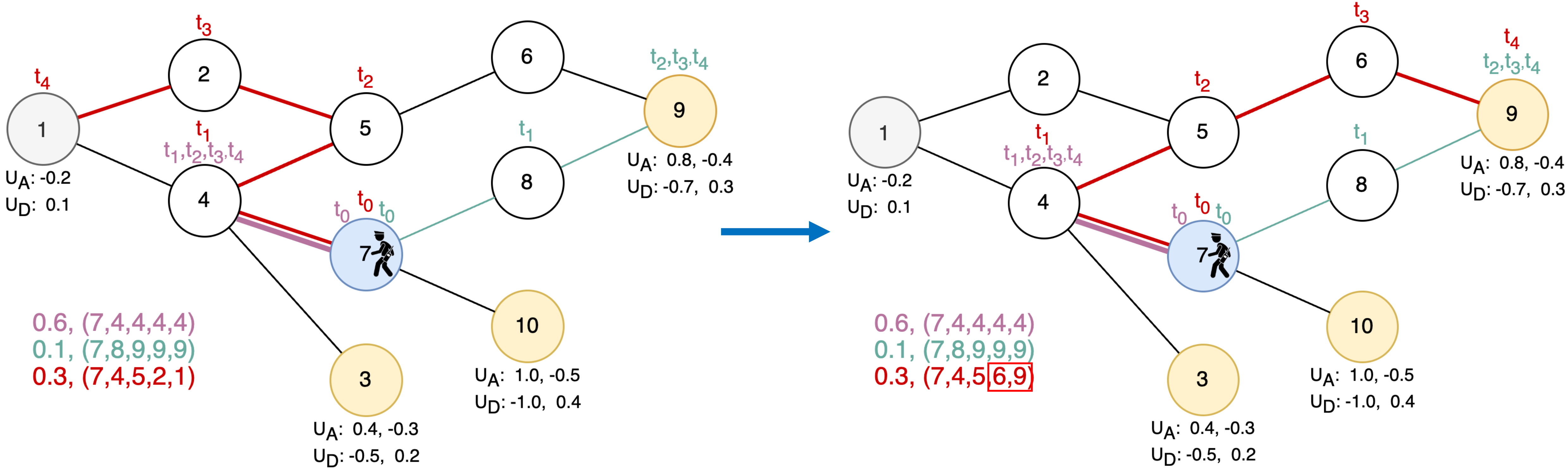
- After crossover each pure strategy may be deleted with probability equal to $(1-p_i^q)^2$

EASG - mutation

- Mutation role: introduce some random perturbation to explore new areas of the search space
- Each individual is mutated with mutation rate probability p_m
- Random pure strategy σ_i^q is chosen which is modified starting from the random time step

$$\sigma'^q_i = (a_1, a_2, \ldots, a_{s-1}, a'_s, a'_{s+1}, \ldots, a'_m)$$

EASG mutation - example



Mutation enhancements

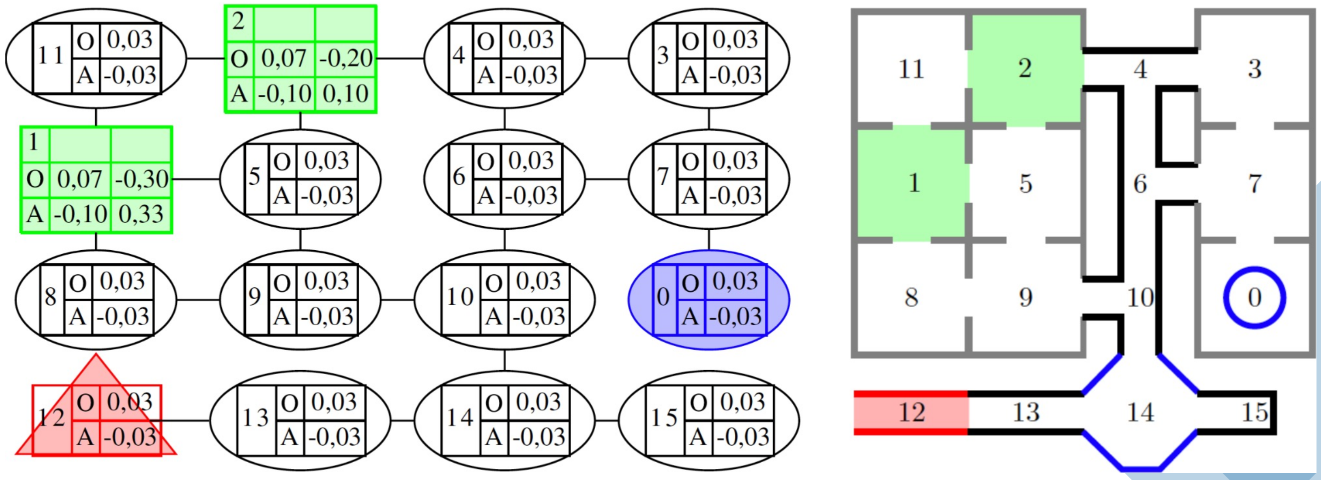
- **$EASG_n$** - EASG algorithm with repeated mutation.
- **$MANPS_1$, $MANPS_n$** - *mutation adds new pure strategy* - a uniformly selected pure strategy is added with a uniformly sampled probability.
- **MCP_1, MCP_n** - *mutation changes probability* - a probability of randomly selected pure strategy is uniformly changed.
- **MSP_1, MSP_n** - *mutation switches probability* - probabilities of two randomly chosen pure strategies are switched.
- **$MDPS_1$, $MDPS_n$** - *mutation deletes pure strategy* -a randomly chosen pure strategy is removed.
- **MCWPS** - *mutation changes the weakest pure strategy* - mutation is applied only to a pure strategy with the lowest payoff.
- **MDWPS** - *mutation deletes the weakest pure strategy* - pure strategy with the lowest payoff is deleted

Experimental setup

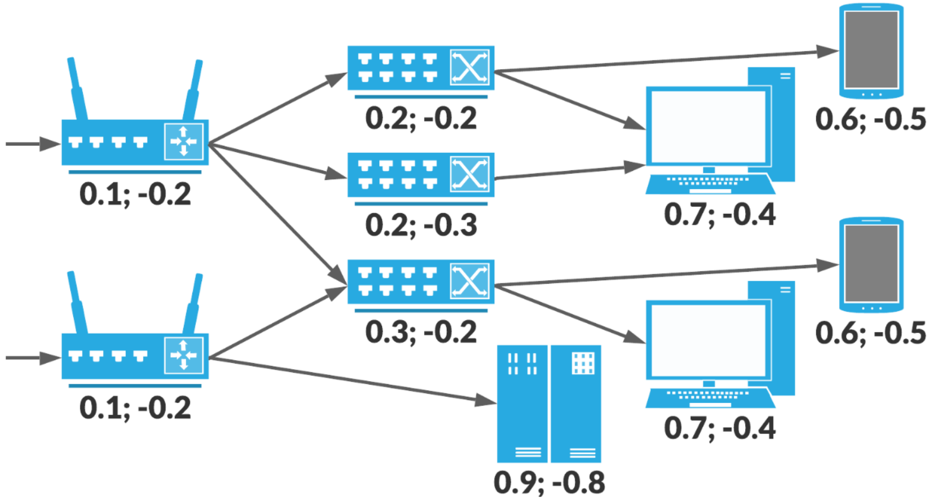
300 test game instances of 3 types:

- 150 Warehouse Games (WHG)
- 90 Search Games (SEG)
- 60 FlipIt Games (FIG)

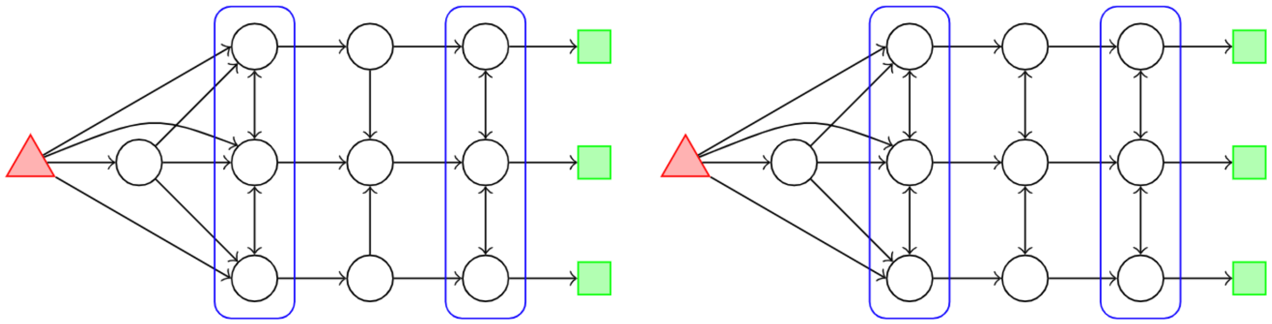
30 independent runs for each game instance



Warehouse Games



FlipIt Games



Search Games

Results

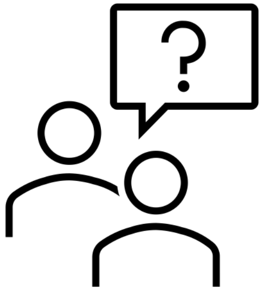
	Defender's payoff			Computation time [s]		
	WHG	SEG	FIG	WHG	SEG	FIG
EASG	**0.017**	0.108	0.031	152	2534	328
$EASG_n$	**0.017**	<u>0.135</u>	**<u>0.037</u>**	1206	21913	3051
$MANPS_1$	0.014	0.059	0.031	156	2548	313
$MANPS_n$	0.016	**<u>0.139</u>**	<u>0.036</u>	1366	21892	2988
MCP_1	0.015	0.074	0.030	148	2422	336
MCP_n	0.016	<u>0.131</u>	**<u>0.037</u>**	1285	22651	3008
MSP_1	0.013	0.099	0.024	156	2583	316
MSP_n	0.016	0.108	**<u>0.037</u>**	1332	21447	2931
$MDPS_1$	0.013	0.052	0.029	147	2620	313
$MDPS_n$	0.013	0.053	0.026	1283	22026	2900
MCWPS	0.013	0.046	0.030	148	2612	321
MDWPS	0.008	0.058	0.018	139	2361	299

The average Defender's payoff and the computation time for various mutation operators. The best results are **bolded**. Results that are better than the baseline version of the algorithm (EASG) are <u>underlined</u>. In cases where the difference between the baseline version (EASG) and a given variation is statistically significant the result is highlighted with a gray background.

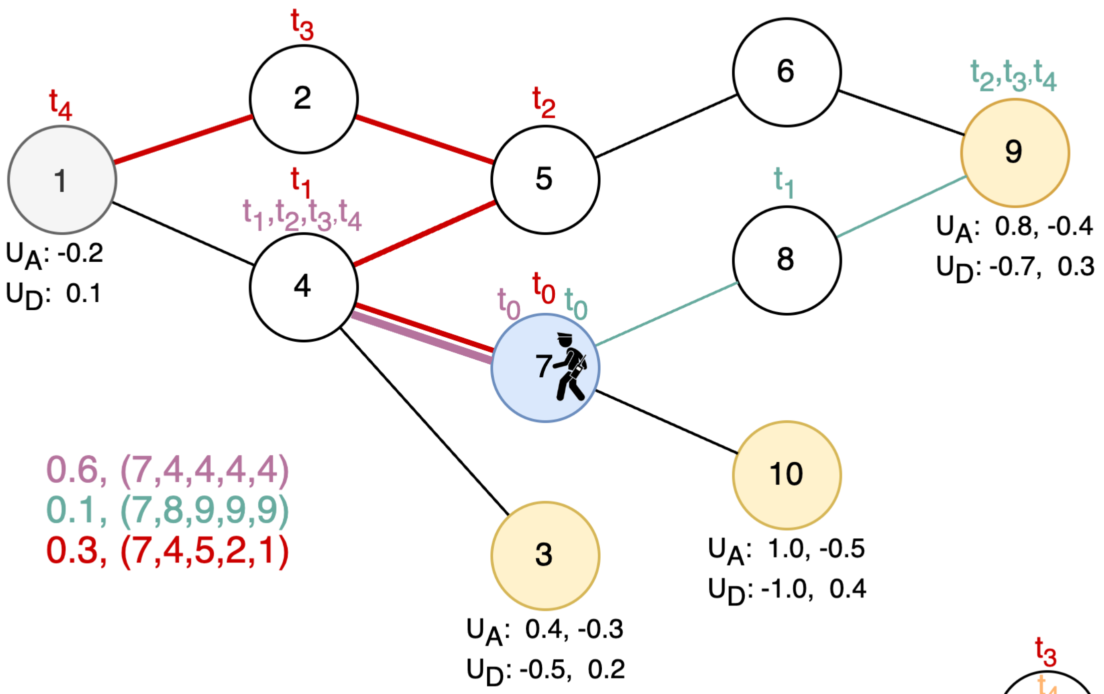
Conclusions

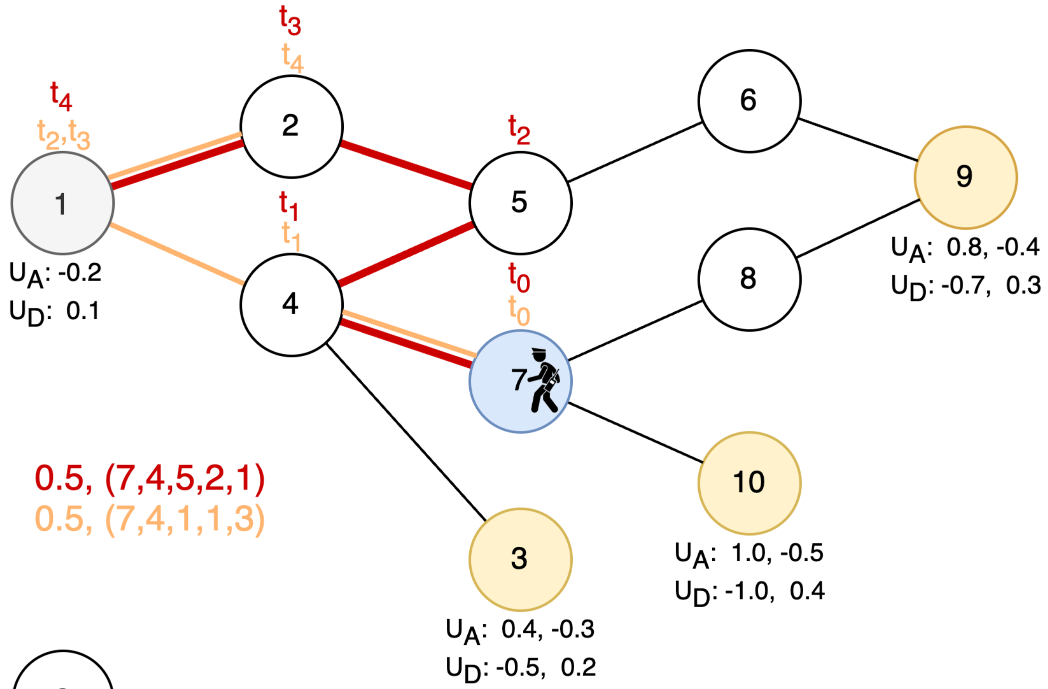
- **Repetition of mutation operation leads to improvement of SSGs outcomes**, though at the expense of significant increase in computation time.
- The proposed modifications offer a **viable alternative to the base EASG formulation** for cases when computational cost is less important.

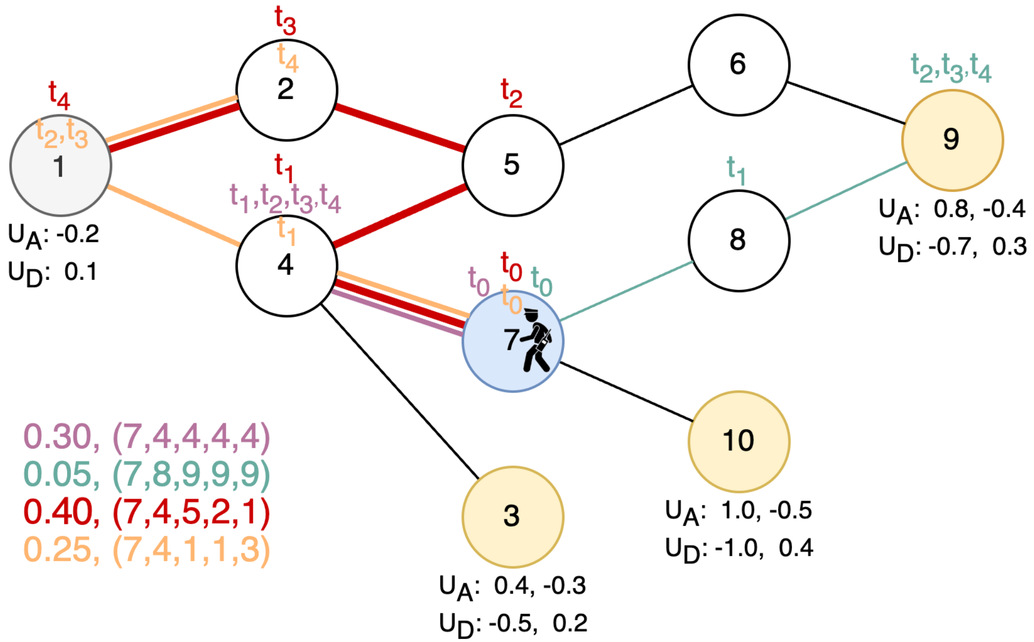
Thank you



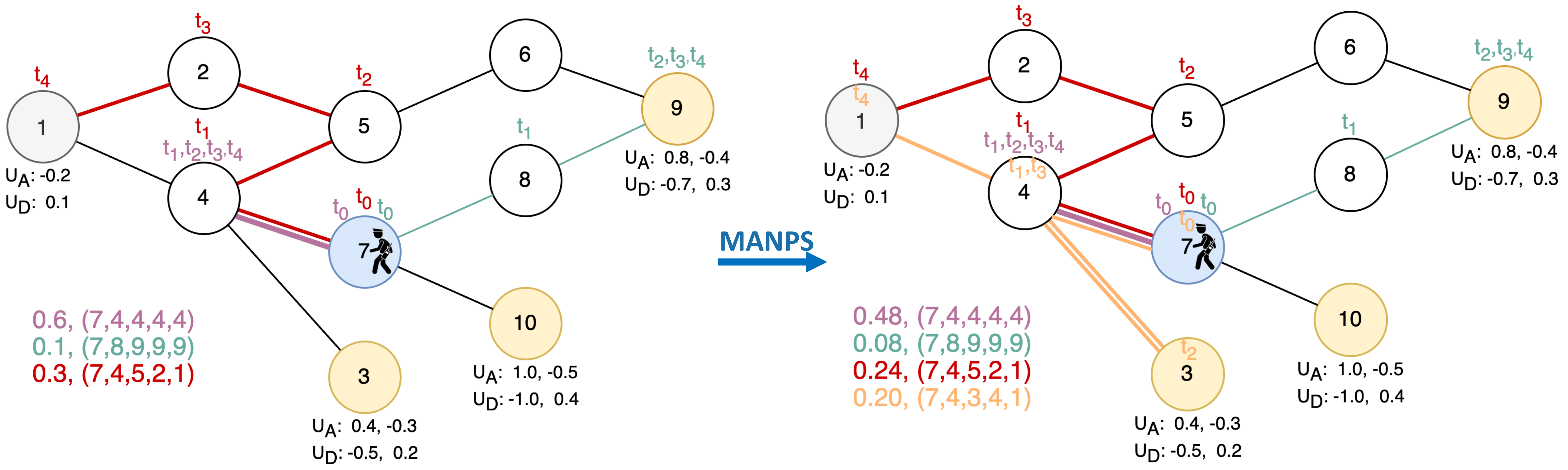
EASG crossover - example



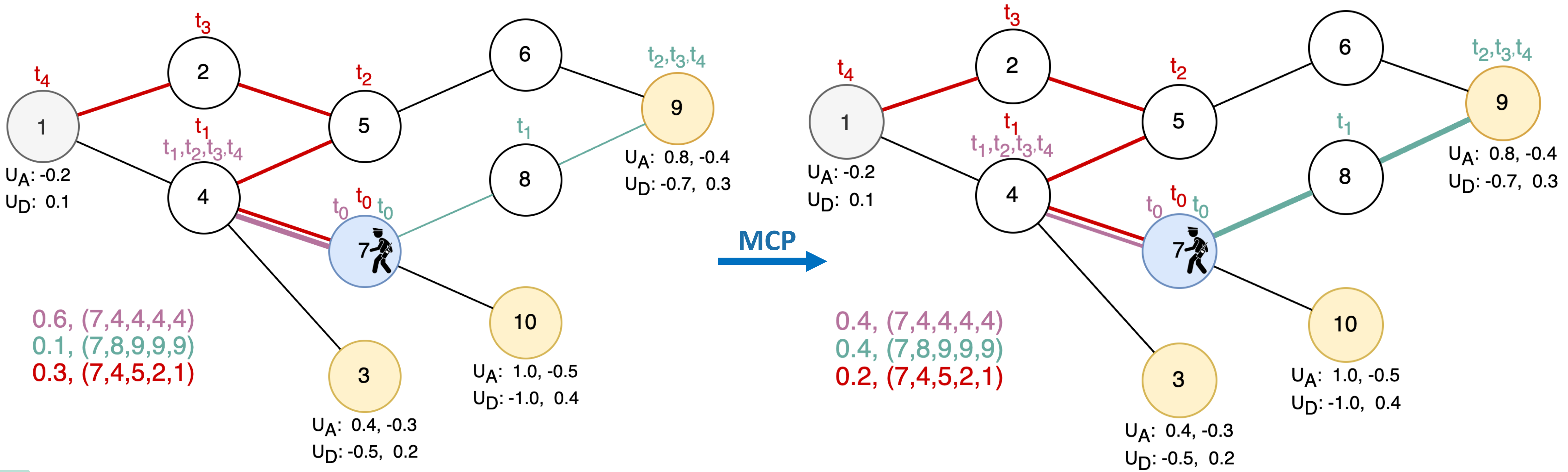




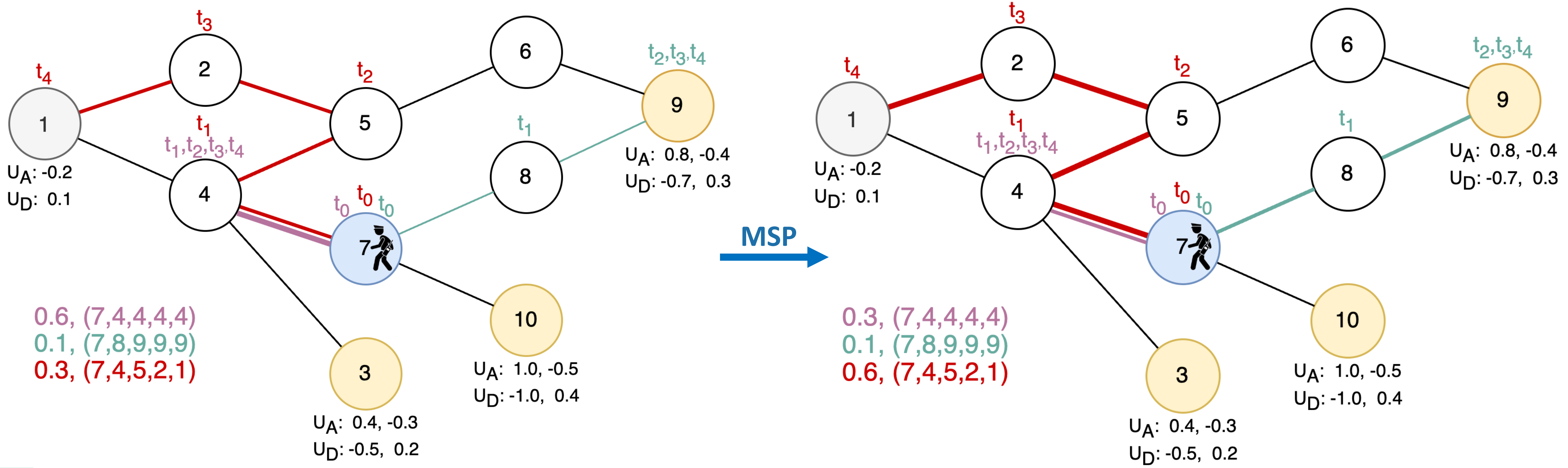
MANPS - *mutation adds new pure strategy* - a uniformly selected pure strategy is added with a uniformly sampled probability



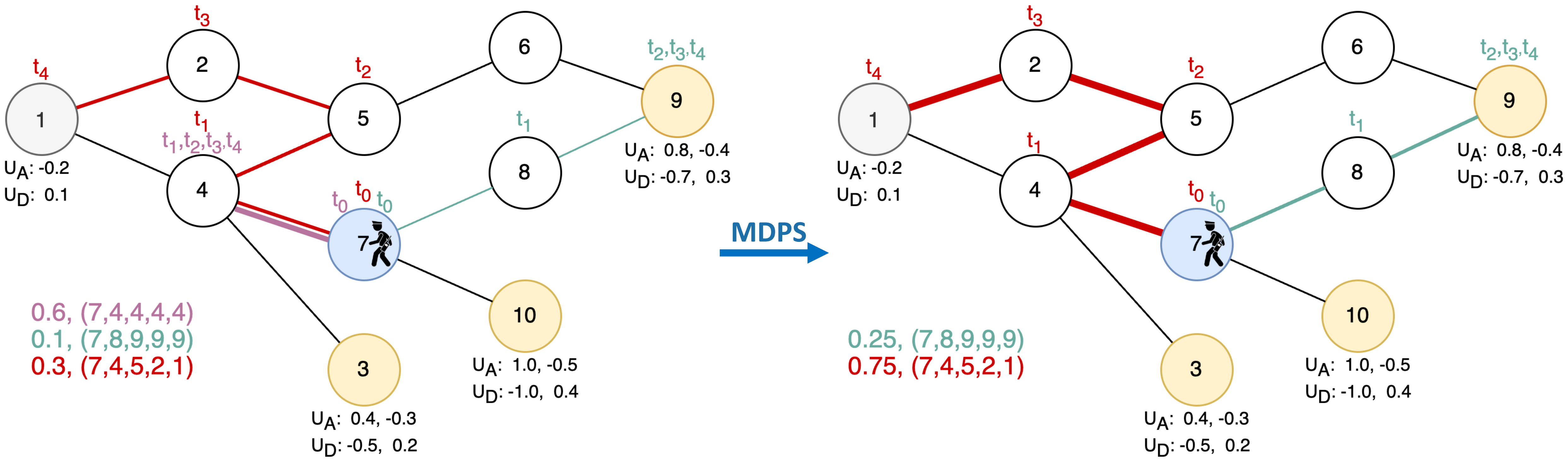
MCP - *mutation changes probability* - a probability of randomly selected pure strategy is uniformly changed



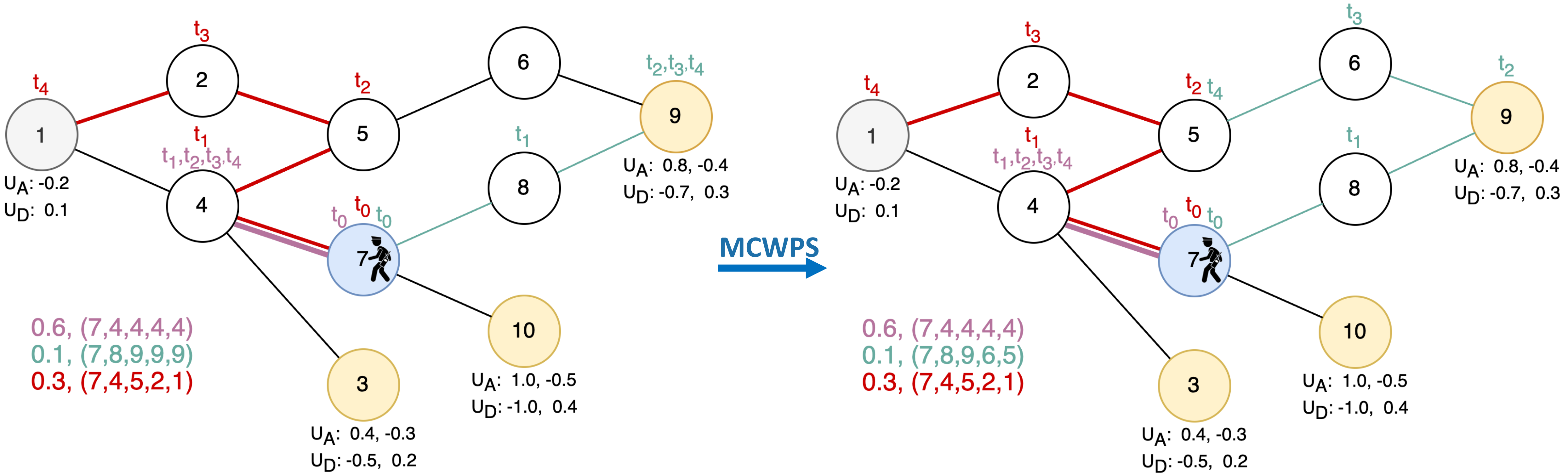
MSP - *mutation switches probability* - probabilities of two randomly chosen pure strategies are switched



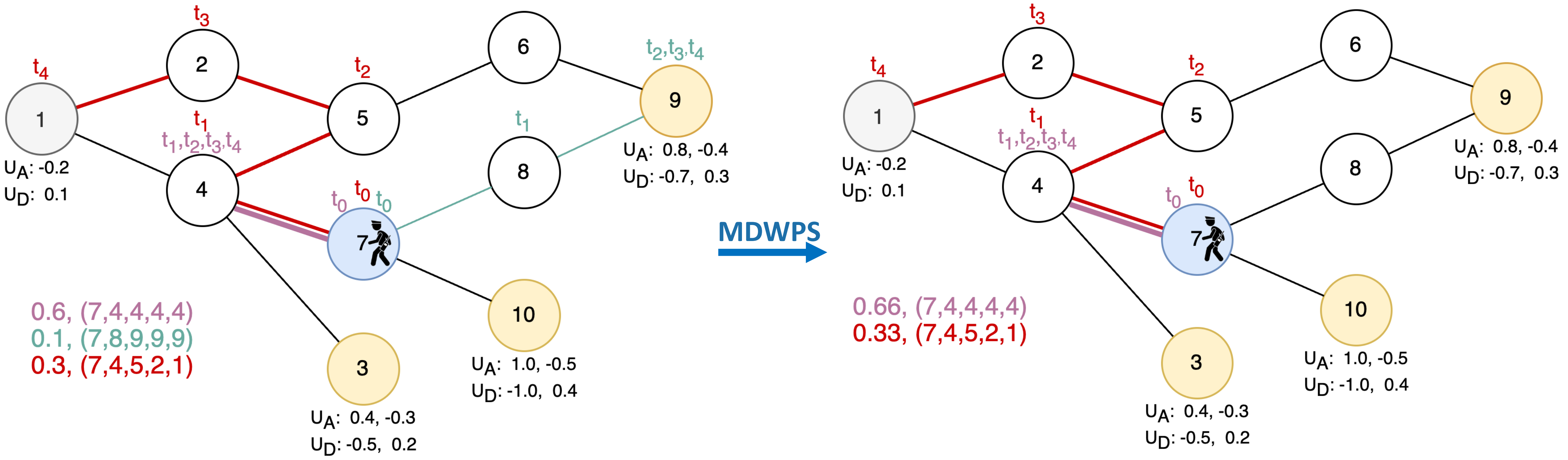
MDPS - *mutation deletes pure strategy* -a randomly chosen pure strategy is removed



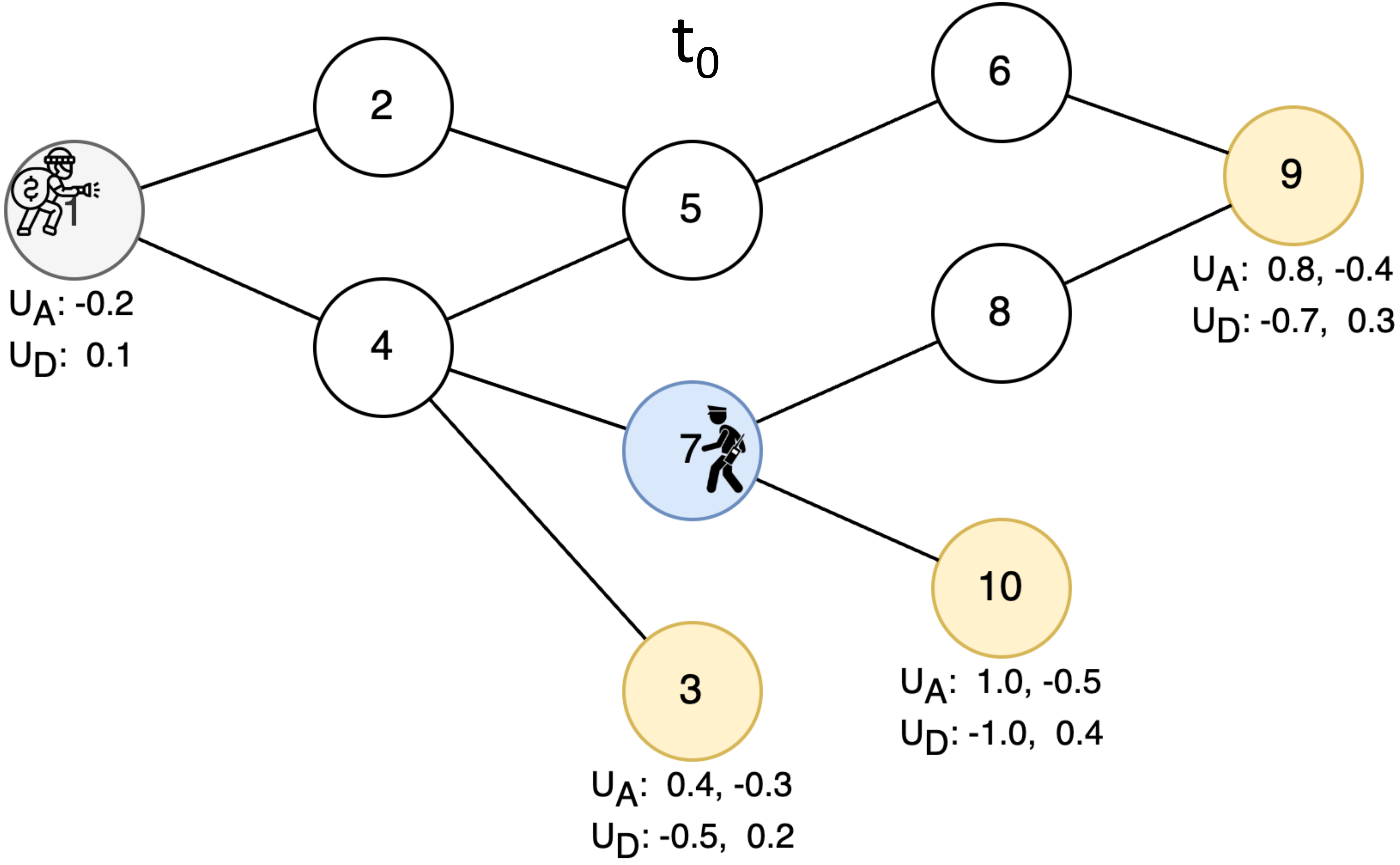
MCWPS - *mutation changes the weakest pure strategy* - mutation is applied only to a pure strategy with the lowest payoff



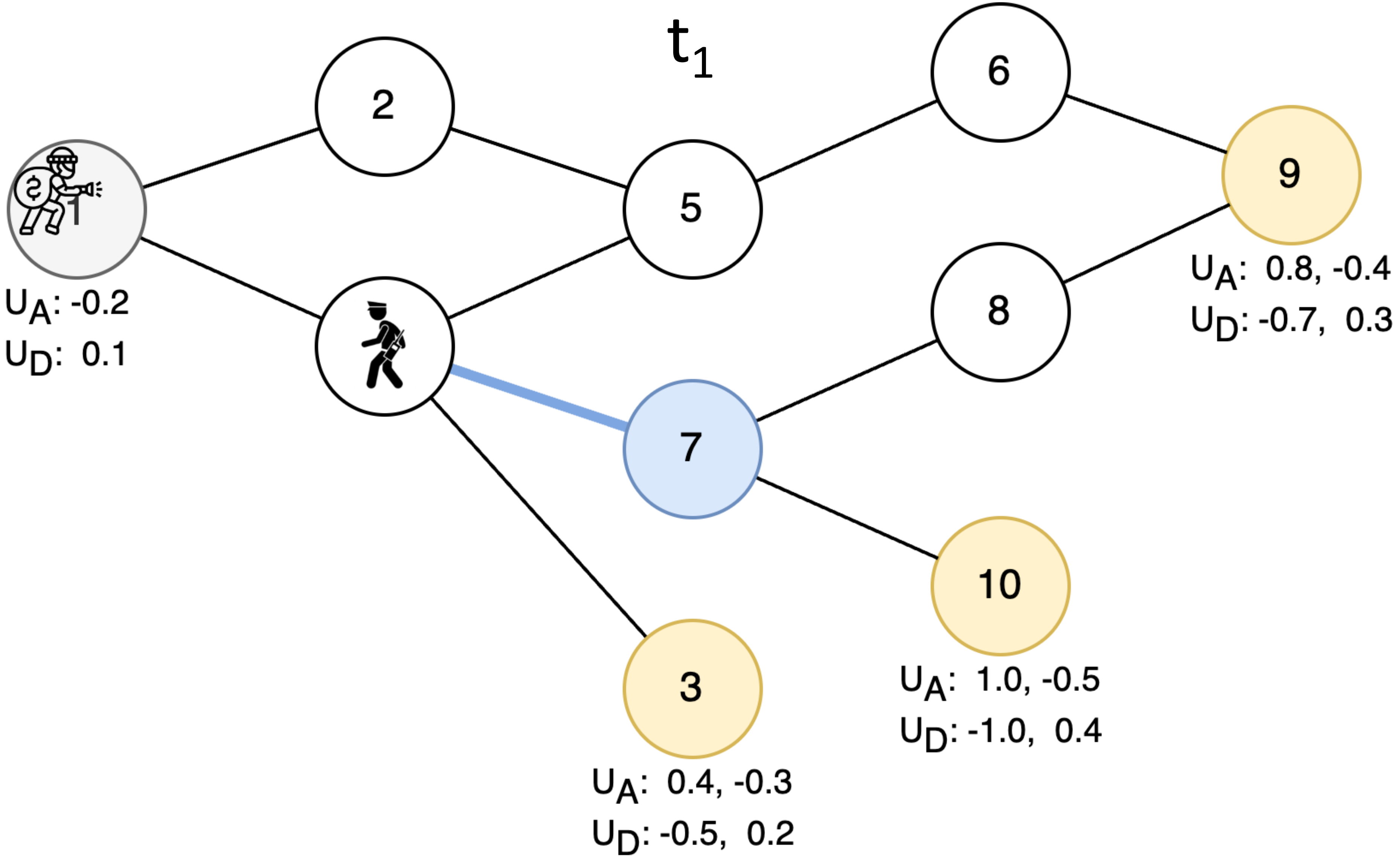
MDWPS - *mutation deletes the weakest pure strategy* - pure strategy with the lowest payoff is deleted



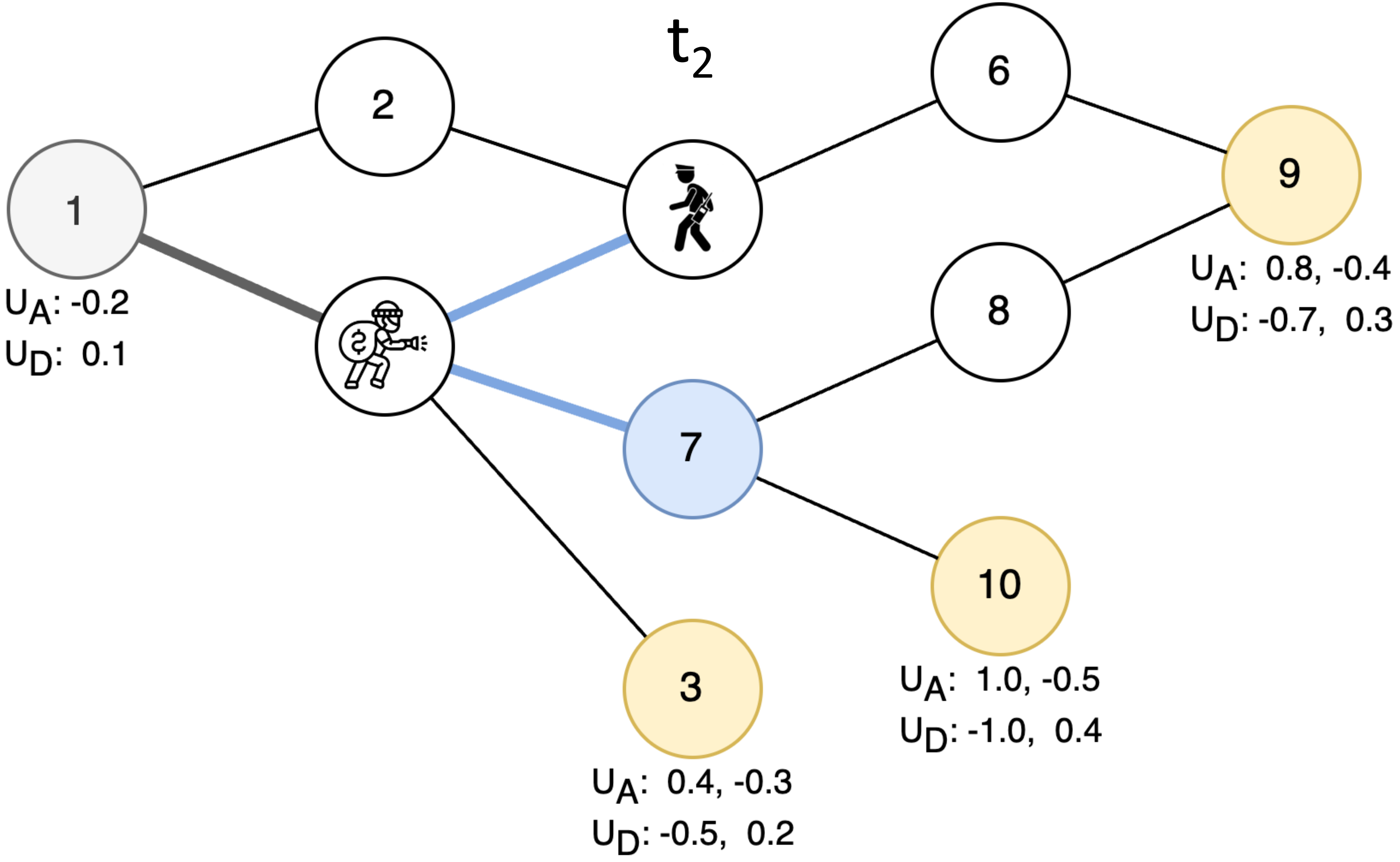
Example – scenario 2



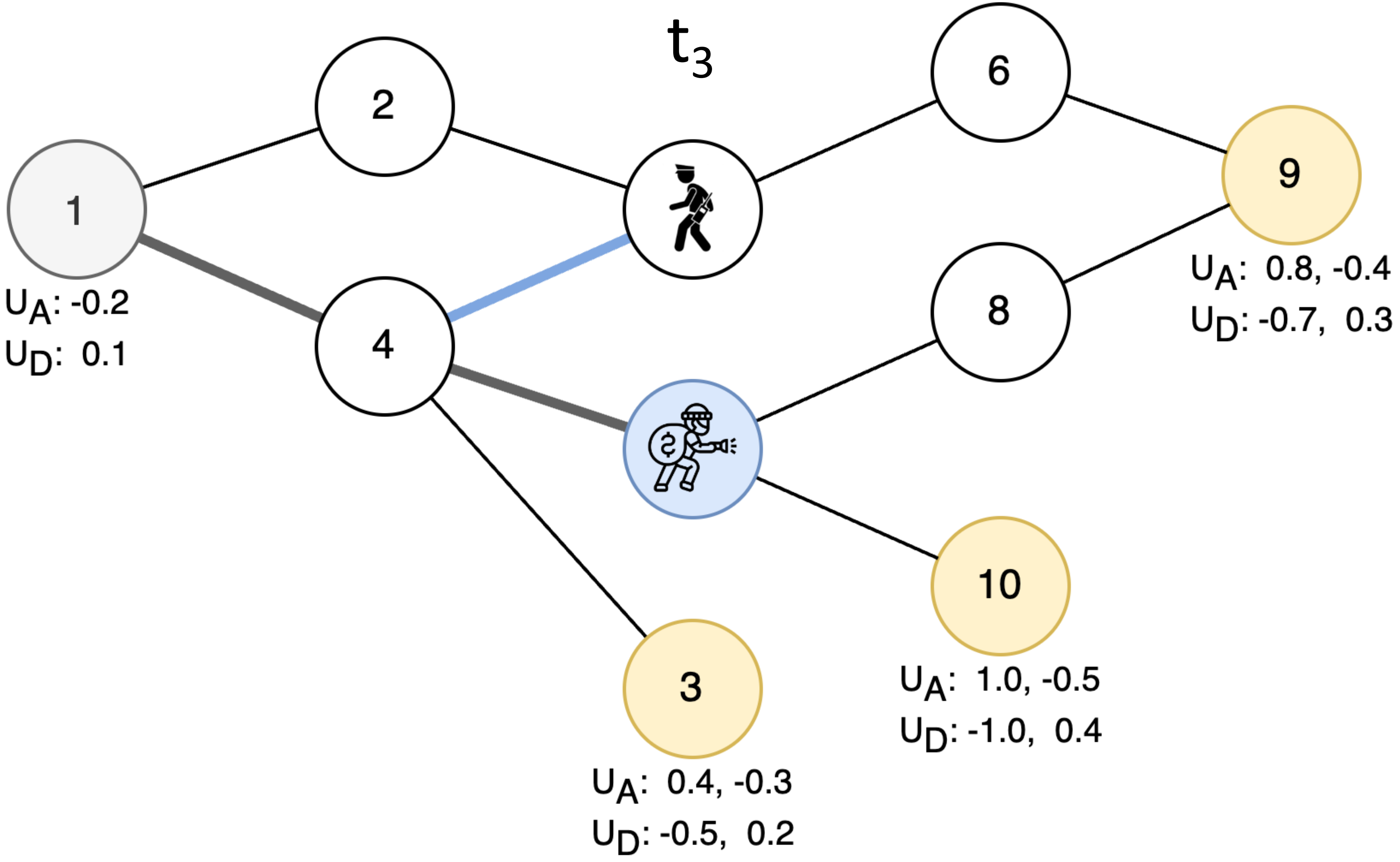
Example – scenario 2



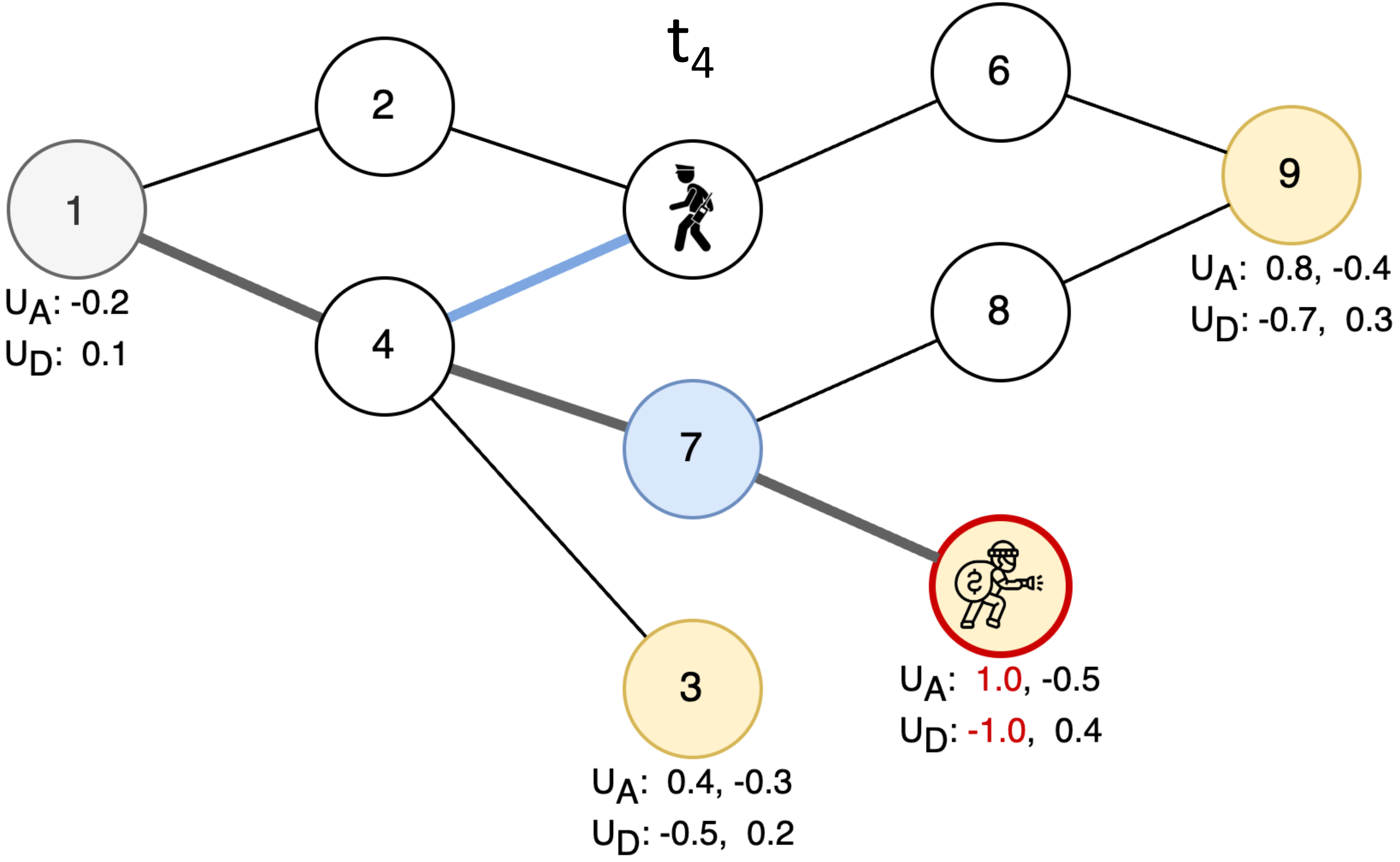
Example – scenario 2



Example – scenario 2



Example – scenario 2



References

[1] Jain, Manish, et al. "**Software assistants for randomized patrol planning for the LAX airport police and the federal air marshal service**." Interfaces 40.4 (2010): 267-290.

[2] Shieh, Eric, et al. ”**PROTECT: A deployed game theoretic system to protect the ports of the United States**." Proceedings of the 11th AAMAS Conference vol. 1. 2012.

[3] Pita, James, et al. "**Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport**." Proceedings of the *7th AAMAS Conference*. 2008.

[4] Fang, Fei, Peter Stone, and Milind Tambe. "**When security games go green: Designing defender strategies to prevent poaching and illegal fishing.**" Proceedings of the 24th IJCAI. 2015.

[5] Yin, Zhengyu, et al. "**Trusts: Scheduling randomized patrols for fare inspection in transit systems**." Proceedings of the 24th IAAI Conference. 2012.

[6] Conitzer, Vincent, and Tuomas Sandholm. "**Computing the optimal strategy to commit to.**” Proceedings of the 7th ACM conference on Electronic commerce. 2006.

[7] Paruchuri, Praveen, et al. "**Playing games for security: An efficient exact algorithm for solving Bayesian Stackelberg games**." Proceedings of the 7th AAMAS vol. 2. 2008.

[8] Bosansky, Branislav, and Jiri Cermak. "**Sequence-form algorithm for computing stackelberg equilibria in extensive-form games**." Proceedings of the 29th AAAI Conference. 2015.

[9] Cermak, Jiri, et al. "**Using correlated strategies for computing stackelberg equilibria in extensive-form games.**" Proceedings of the 30th AAAI Conference. 2016.

[10] Černý, Jakub, Branislav Boýanský, and Christopher Kiekintveld. "**Incremental strategy generation for stackelberg equilibria in extensive-form games**." Proceedings of the 2018 ACM Conference on Economics and Computation. 2018.

[11] Bondi, Elizabeth, et al. "**To signal or not to signal: Exploiting uncertain real-time information in signaling games for security and sustainability.**" Proceedings of the 34th AAAI Conference. 2020.

[12] Van Dijk, Marten, et al. "**FlipIt: The game of stealthy takeover.**" Journal of Cryptology 26.4: 655-713. 2013.