Description for the general public

Globalization of threats to homeland security, such as international terrorism, smuggling of weapons or drugs, or large-scale thefts became one of the main challenges for security forces in the 21st century. Rising global threats require adequate measures to be taken in order to maintain the expected level of security. In effect, modern and scientifically grounded methods for fighting organized crime and terrorist threats have been proposed and developed in recent years. One of rapidly developing related research areas are Security Games (SG), which consist in modeling tactical security issues in the form of a game between security forces (secret service, police, etc.) and the organized attackers (terrorists, military groups, etc.).

The main objective of this research project is development of a new approach to SG, which relies on massive Monte-Carlo simulations.

The starting point of the proposed research is the Mixed-UCT method proposed by the grant principal investigator and his research assistant. The baseline idea refers to applying massive Monte-Carlo simulations within the so-called UCT algorithm, which is a popular approach to perfect-information games. Initial experimental evaluation of the Mixed-UCT method proved its potential in the case of a certain SG variant considered in the tests.

The project aims at further extension of the SG model and adequate adaptation of the Mixed-UCT method which, in particular, will allow consideration of the influence of external factors (independent of the game players decisions) on the current game state. Furthermore, the game model (and Mixed-UCT method) will be extended towards modeling bounded rationality of the Attacker. Classical game equilibrium models, including Stackelberg Equilibrium, assume perfect rationality of the players. In real-life, however, the opponent is a human, whose decisions may not be fully rational, due to time pressure, stress, or improper assessment of the situation.

The next research direction planned in the project is related to the issue of partial observability of the Attacker by the Defender by means of unintentionally leaving some kind of traces by the Attacker in the locations (graph nodes) recently visited by them.

In each project's step the benchmark sets adequate for a given SG model will be developed, along with the development of the solving method (modifications and variants of the Mixed-UCT approach) allowing for a thorough evaluation of the proposed extensions. This set of well motivated benchmarks developed during project's realization will be freely accessible on a dedicated project's webpage in order to lay foundations for a common platform for reliable comparison for the current and future methods in the area of SG.