Security Games with Mobile Patrollers

(Extended Abstract)

Ondřej Vaněk
Agent Technology Center, Dept. of Cybernetics, FEE Czech Technical University
Technická 2, 16627 Praha 6, Czech Republic
vanek@agents.felk.cvut.cz

ABSTRACT

To optimally secure large and complex infrastructures against crime activities, a scalable model for optimal defender allocation is needed. Game theory is successfully used to formalize the problem as a two-player game between an attacker and a defender. We consider both player to be mobile and we focus on proper path intersection modeling and we observe the trade-off between fidelity and computational complexity. We search for the a Nash Equlibirium of the game using oracle based algorithms and we evaluate the robustness of the solution in a multi-agent simulation where some assumptions made do not strictly hold.

Categories and Subject Descriptors

I.2.11 [**Artificial Intelligence**]: Distributed Artificial Intelligence

General Terms

Algorithms, Economics, Security, Performance

Keywords

game theory, reasoning

1. INTRODUCTION

In recent years, with rise of many crime activities, the effective security of important infrastructures, such as public airlines, city infrastructures or maritime transit corridors is growing on importance. These networks – already large and complex – are constantly growing and gaining additional complexity, so the conventional methods for securing these networks, such as human generated schedules, are rendered useless. New computer-aided methods for optimal security resource allocation and area patrolling are needed.

There is an ongoing research focusing on scalable solutions for optimal defender resource allocation in various domains. The problem is modeled as a game between two players: the attacker and the defender. While the attackers movement is usually explicitly considered and accounted for, the defender is mostly static, i.e. he is allocated to a particular place to guard and he is not allowed to move.

We focus on models, where both the attacker as well as the defender – more appropriately called the patroller – is mobile, i.e. we explicitly consider movements of both players and focus on proper path intersection modeling. This model allows us to consider additional constraints of both players, such as the requirement of the attacker to reach a particular destination or the necessity of the patroller to periodically return to its base. We term this game model *transit game* which we introduced in [7, 8]. The main advantage of this approach is the formalization of the domains with finer granularity; however, this comes with the cost of additional complexity in the computation process.

To be able to solve large games representing real-world scenarios, we are using oracle-based algorithms [4]. These iterative algorithms are solving a set of small *sub-games* and they do not require explicit enumeration of all strategies. Consequently, they are able to solve large games that would not fit into the memory when using conventional linear programming methods. The performance of the algorithms heavily depends on fast oracles, providing best response strategy for any sub-game. Unfortunately, there is a trade-off between the fidelity of the game model – more specifically the fidelity of the utility computation – and best response computation time. We fight this problem from both sides: (1) we are looking for a reasonable compromise of the fidelity of the utility function and (2) we look for fast "good-enough" responses for sub-game expansion which still lead to an optimal solution.

Finally, to properly validate the game model, we implant the computed solution into a multi-agent simulation of a particular domain and evaluate its effectiveness in a richer environment. This last step provides a necessary bridge between theoretical models and real-world deployment.

2. RELATED WORK

Security games [3] are able to model a variety of security scenarios ranging from allocation airport security to terminals [5] to placing checkpoints in a city grid [6]. In our paper [2], we extend the latter approximate approach to provide an optimal solution using precise definition of the utility function and the double-oracle algorithm. In broader context, there exist many game models generally denoted as pursuit-evasion games that are relevant to our approach. The closest games with both mobile players are infiltration games [1], however no additional constrains are considered for the movement of the patroller. Moreover, we have further

Cite as: Security Games with Mobile Patrollers (Extended Abstract), Ondřej Vaněk, *Proc. of 10th Int. Conf. on Autonomous Agents and Multiagent Systems (AAMAS 2011)*, Tumer, Yolum, Sonenberg and Stone (eds.), May, 2–6, 2011, Taipei, Taiwan, pp. 1371-1372.

enriched our model by associating interception probability with each node and edge in the graph, thus considering additional real-world property.

3. GAME MODEL

The transit game is a zero-sum game played in a connected transit area represented by an arbitrary graph with defined entry and exit zones and a base location. There are two players that move in the area: the evader (corresponding to the attacker) and the patroller. The evader's objective is to reach any exit zone from any entry zone without encountering the patroller. The patroller's objective is to intercept the evader's transit by strategically moving through the transit area. In addition, because of its limited endurance, the patroller has to repeatedly return to the base.

The strategy set of the evader is a set of all paths from entry to exit zones and the strategy set of the patroller are all closed walks originating in the base. The utility function can vary from simplistic definitions, summing the number of joint nodes of players' paths, to complex ones, taking into account relative movement of the players and incorporating interception probability If the utility is simple enough then the strategy space can be represented by a more compact set of strategy components and by additional network-flow constrains in the LP formulation (described in [7]). In this case, the oracle can provide the best response fast and the algorithm is scalable. If the utility function is computed more precisely, the strategies cannot be decomposed and represented compactly. In this case, the oracle-based algorithms cannot provide the solution in polynomial time thus restricting the scalability.

For the static defender resource allocation, we explored the trade-off between the complexity of the utility function in [2], where we have shown that the approximate utility definition can result in an unbounded error in the defender resource allocation. However, when defining the utility exactly, the best-response oracles were proven to be NP-hard, which resulted into a much lower scalability.

4. SOLUTION ALGORITHMS

Instead of searching for the Nash Equilibrium (NE) of the full game, oracle-based algorithms iteratively construct and solve a growing succession of smaller sub-games until they reach a sub-game whose NE is also the NE of the full game. The sub-games are constructed by considering only a subset of all pure strategies for one or both players. In each iteration, the oracle finds the best response (in form of a pure strategy) for a player and this strategy is added to the current sub-game. Depending on the structure of players' strategy spaces, a NE of the full game may be found (long) before the full game needs to be constructed and solved thus significantly reducing the computation time. Two important assumptions are made: (1) computation of NE is significantly faster for the sub-games than for the full game and (2) the best responses are provided fast. As we discuss in our work, assumption (2) does not always hold, which limits the usage of the oracle-based algorithms.

5. EVALUATION APPROACH

It is usual to consider the finding of a NE the final step of the problem solution. However it is not often seen to test the solution of the game outside the game-theoretic framework. It is necessary to deploy the solution of the game into a richer representation of the real-world problem and evaluate the effectiveness of the solution in a more realistic environment.

In our work, we use multi-agent simulations of various domains to test the computed solution. The agents implement a behavioral model based on the strategy computed from the game. They move on the graph, however, the graph is placed over the area it represents and the agents are following a continuous path. Additionally, the simulation allows to slightly violating other assumptions made, such as giving different speeds to the players, extending visibility range of the patroller etc. When evaluating the effectiveness of the patroller strategies, the attacker does not use the precomputed solution; it behaves adaptively, searching for a potential "hole" in patroller's behavior, possibly present due to the different conditions of the simulated world.

6. CONCLUSION

We have proposed a game-theoretic framework of transit game to optimally solve large and complex security problems. We have extended the oracle-based algorithms to achieve faster algorithm convergence and we have evaluated the solution of the game in a multi-agent simulation.

In the close future, we will further explore the trade-off between the complexity of the utility functions and the computational requirements of the computation process. We will extend oracle-based algorithms to be able to provide responses fast and expand the sub-games more effectively, thus speeding the convergence process. This approach will lead to effective and scalable algorithms able to design security and patrol schedules for infrastructures of today's world.

7. REFERENCES

[1] S. Alpern. Infiltration Games on Arbitrary Graphs. *Journal of Mathematical Analysis and Applications*, 163:286–288, 1992.

[2] M. Jain, D. Korzhyk, O. Vaněk, V. Conitzer, M. Pěchouček, and M. Tambe. Double oracle algorithm for zero-sum security games on graphs. In *Proceedings of AAMAS*, 2011.

[3] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, F. Ordóñez, and M. Tambe. Computing optimal randomized resource allocations for massive security games. In *Proceedings of AAMAS*, 2009.

[4] H. B. McMahan, G. J. Gordon, and A. Blum. Planning in the Presence of Cost Functions Controlled by an Adversary. In *Proc. of ICML*, pages 536–543, 2003.

[5] J. Pita, M. Jain, F. Ordóñez, C. Portway, M. Tambe, C. Western, P. Paruchuri, and S. Kraus. Using game theory for los angeles airport security. *AI Magazine*, 30(1), 2009.

[6] J. Tsai, Z. Yin, J. young Kwak, D. Kempe, C. Kiekintveld, and M. Tambe. Urban Security: Game-Theoretic Resource Allocation in Networked Physical Domains. In *Proceedings of AAAI*, 2010.

[7] O. Vaněk, B. Bošanský, M. Jakob, and M. Pěchouček. Transiting Areas Patrolled by a Mobile Adversary. In *Proceedings of IEEE CIG*, 2010.

[8] O. Vaněk, M. Jakob, V. Lisý, B. Bošanský, and M. Pěchouček. Iterative game-theoretic route selection for hostile area transit and patrolling (extended abstract). In *Proceedings of AAMAS*, 2011.