Security Games and Contagion

(Extended Abstract)

Jason Tsai
University of Southern California
jasontts@usc.edu

ABSTRACT

Many real-world situations involve attempts to spread influence through a social network. For example, viral marketing is when a marketer selects a few people to receive some initial advertisement in the hopes that these 'seeds' will spread the news. Even peacekeeping operations in one area have been shown to have a contagious effect on the neighboring vicinity. Each of these domains also features multiple parties seeking to maximize or mitigate a contagious effect by spreading its own influence among a select few seeds, naturally yielding an adversarial resource allocation problem. As past researchers of security resource allocation have done, I propose using game theory to develop such policies and model the interconnected network of people as a graph.

Unlike this past work in security games, however, actions in these domains possess a probabilistic, non-local impact that makes even payoff determination an NP-Hard problem. My thesis proposes novel techniques for solving this type of game for real-world problem sizes by building upon the latest research in security games and influence blocking maximization. I have also advanced the understanding of contagion phenomena by developing empirical evaluation methods for computational contagion models. Finally, my thesis formalizes an entirely new class of security games with wide-ranging applications from marketing to peacekeeping.

Categories and Subject Descriptors

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

General Terms

Algorithms, Security, Optimization

Keywords

Game Theory, Security, Stackelberg Games, Contagion, Social Networks

1. INTRODUCTION

Many adversarial domains exhibit 'contagious' actions for each player. For example, word-of-mouth advertising / viral marketing has been widely studied by marketers trying to understand why one product or video goes 'viral' while others go unnoticed [10]. Recent work has even shown that peacekeeping operations in one nation reduces the probability of conflict arising in nearby areas by 70% [2]. In these domains, multiple intelligent parties attempt to leverage the same social network to spread their message, necessitating an adversary-aware approach to strategy generation.

I use a game-theoretic approach and develop algorithms to generate resource allocation strategies for large-scale, real-world networks. I model the interaction as a graph with one player attempting to spread influence while the other player attempts to stop the probabilistic propagation of that influence by spreading their own influence. This 'blocking' problem models situations faced by governments/peacekeepers combatting the spread of terrorist radicalism and armed conflict with daily/weekly/monthy visits with local leaders to provide support and discuss grievances [6].

This follows work in security games from recent years [1, 3, 5, 7] including deployed systems such as IRIS, which I helped develop for the United States Federal Air Marshal Service [9, 13]. While some of my own work in security games also modeled interactions on a graph [14], I extend the approach into a new area where actions carry a 'contagion' effect. The situation becomes a type of influence blocking maximization (*IBM*) problem [4], which are a competitive extension of the widely studied influence maximization problem [8]. Past work in *IBM* has looked only at the best-response problems and has not produced algorithms to generate the game-theoretic equilibria necessary for this repeated-interaction domain.

2. CONTRIBUTIONS

My work has provided contributions towards solving these problems in three specific ways: (i) novel algorithms for security games with contagious actions; (ii) real-world data driven quantitative comparison of competing contagion models; and (iii) efficient heuristics to scale-up game-theoretic solutions to real-world problem sizes for graph-based security games.

Novel algorithms for security games with contagious actions: A major contribution of my work is to open up a new area of research that combines recent research in security games with the latest work in influence blocking maximization and contagion studies. Drawing from the security games literature, I propose using a double oracle algorithm where each oracle produces a single player's best-response to the opponent's strategy and incrementally cre-

Appears in: *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems (AAMAS 2012)*, Conitzer, Winikoff, Padgham, and van der Hoek (eds.), 4-8 June 2012, Valencia, Spain.

ates the payoff matrix being solved. Thus, my algorithms are able to handle very large network sizes under practical time constraints. More importantly, this approach allows me to directly leverage advances in *IBM* research that has focused entirely on fast best-response calculations.

Quantitative comparison of competing contagion models: To strategize in domains where both players' actions have a contagious effect, the primary assumption is that the mechanics of the contagion are known. However, this is a poor assumption and understanding the spreading effect is an open research problem with new models constantly being proposed and a severe lack of a ground-truth for rigorous evaluation. To address this issue, I developed the ESCAPES evacuation simulation system [12] that I used to evaluate competing models of emotional contagion [11]. I use the simulation to reproduce data from *real* crowd evacuations and show that one of the models outperforms all others in accurately reproducing the *both* scenes. I also examined the components of the different models evaluated by testing variations of each of the models with features added/removed. This work is the only known empirical comparison of computational emotional contagion models.

Efficient heuristics for graph-based security games: I have introduced graph-based techniques for game-theoretic resource allocation in two domains. First, I have worked on urban road network security, where police forces must place vehicle checkpoints throughout a city to prevent adversaries en route to their attack destinations. In such a domain, each player has a massive number of potential actions (paths to travel, sets of edges to cover). I developed a polynomial-time algorithm based on graph-based techniques, RANGER, and accompanying sampling techniques that are provably optimal under specific conditions [14]. My algorithm provided the first useable solution technique in the urban road network security domain and remains the *only* polynomial-time algorithm with provable guarantees. Also, in addressing the contagion mitigation game outlined in Section 1, I have developed a heuristic estimation algorithm LSMI for influence blocking maximization problems that is based on shortest-paths calculations. This is used within the aforementioned double-oracle approach to once again provide the first set of game-theoretic allocation algorithms for real-world domain sizes.

3. FUTURE WORK

Thus far my work has provided the first solution methods for security games with contagion. In the future, I intend to move forward along two directions: (i) novel algorithms with quality guarantees and improved efficiency; (ii) novel algorithms to address 'inoculation' games and 'competitive contagion' games.

First, although the size of leadership networks used in the real-world are limited to a few hundred nodes, general social networks such as those used for viral marketing can be tens or hundreds of thousands of nodes. This requires improved scalability over current methods. Quality guarantees on the solutions provided are also very important for real-world deployment and will also be a focus of my work.

Second, the mitigation game introduced here is only one of three contagion games one can consider. 'Inoculation' games, where only one player has contagious actions have been well-studied in epidemiology, but generally without a complete game-theoretic treatment. 'Competitive contagion' games, where both players seek to maximize their own influence, have only recently been studied. I hope to extend my work into both of these variants of security games with contagion to provide generalized solution methods for all types of contagion games.

4. REFERENCES

[1] N. Basilico and N. Gatti. Automated abstractions for patrolling security games. In *AAAI*, 2011.

[2] K. Beardsley. Peacekeeping and the contagion of armed conflict. *The Journal of Politics*, 73(4):1051–1064, October 2011.

[3] B. Bosanský, V. Lisý, M. Jakob, and M. Pechoucek. Computing time-dependent policies for patrolling games with mobile targets. In *AAMAS*, pages 989–996, 2011.

[4] C. Budak, D. Agrawal, and A. E. Abbadi. Limiting the spread of misinformation in social networks. In *WWW*, pages 665–674, 2011.

[5] V. Conitzer and T. Sandholm. Computing the optimal strategy to commit to. In *ACM EC-06*, pages 82–90, 2006.

[6] N. J. Howard. *Finding optimal strategies for influencing social networks in two player games.* Masters thesis, MIT, Sloan School of Management, June 2011.

[7] M. Jain, J. Tsai, J. Pita, C. Kiekintveld, S. Rathi, M. Tambe, and F. Ordóñez. Software assistants for randomized patrol planning for the lax airport police and the federal air marshals service. *Interfaces*, 40:267–290, 2010.

[8] D. Kempe, J. M. Kleinberg, and É. Tardos. Maximizing the spread of influence through a social network. In *KDD*, pages 137–146, 2003.

[9] C. Kiekintveld, M. Jain, J. Tsai, J. Pita, M. Tambe, and F. Ordóñez. Computing Optimal Randomized Resource Allocations for Massive Security Games. In *AAMAS-09*, 2009.

[10] M. Trusov, R. E. Bucklin, and K. Pauwels. Effects of word-of-mouth versus traditional marketing: Findings from an internet social networking site. *Journal of Marketing*, 73, September 2009.

[11] J. Tsai, E. Bowring, S. Marsella, and M. Tambe. Empirical evaluation of computational emotional contagion models. In *IVA-11*, 2011.

[12] J. Tsai, G. Kaminka, S. Epstein, A. Zilka, I. Rika, X. Wang, A. Ogden, M. Brown, N. Fridman, M. Taylor, E. Bowring, S. Marsella, M. Tambe, and A. Sheel. ESCAPES: Evacuation Simulation with Children, Authorities, Parents, Emotions, and Social Comparison. In *AAMAS-11*.

[13] J. Tsai, S. Rathi, C. Kiekintveld, F. Ordóñez, and M. Tambe. IRIS A Tool fpr Strategic Security Allocation in Transportation Networks. In *AAMAS-09 (Industry Track)*, 2009.

[14] 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 *National Conference on Artificial Intelligence (AAAI)*, 2010.