Security Games with Contagion: Handling Asymmetric Information

(Extended Abstract)

Jason Tsai¹, Yundi Qian¹, Yevgeniy Vorobeychik², Christopher Kiekintveld³, Milind Tambe¹

¹University of Southern California, Los Angeles, CA 90089
{jasontts, yundi.qian, tambe} @usc.edu
²Sandia National Laboratories, Livermore, CA
yvorobe@sandia.gov
³University of Texas at El Paso, El Paso, TX
cdkiekintveld@utep.edu

ABSTRACT
Counterinsurgency, which is the effort to mitigate support for an opposing organization, is one such domain that has been studied recently and past work has modeled the problem as an influence blocking maximization that features an influencer and a mitigator. While past work has introduced scalable heuristic techniques for generating effective strategies using a double oracle algorithm, it has not addressed the issue of uncertainty and asymmetric information, which is the topic of this paper.

Categories and Subject Descriptors
I.2.11 [Artificial Intelligence]: Distributed Artificial Intelligence

General Terms
Algorithms, Security, Performance

Keywords
Game theory, Social contagion, Influence maximization

1. INTRODUCTION
The spread of information and social behaviors has been studied extensively in many disciplines in the context of phenomena such as viral marketing, rumor spreading and the Arab Spring [9, 12, 13]. Counterinsurgency, the competition for the support of local leadership, has also been studied as a game with two strategic players [6, 5, 14]. Although many aspects of this problem are highly active areas of research, the key computational question is to decide which local leaders to influence to achieve each player’s primary goal: maximize influence for one player, and mitigate the first player’s influence for the other player.

These ‘counter-contagion’ games have received recent attention in the security games literature [14] and has been modeled as a graph where nodes represent leaders and edges between the nodes representing the probability of influence. This line of research, however, has not yet examined the impact of asymmetric information. Informational challenges abound in counterinsurgency, where the insurgents are typically an indigenous group that has an informational advantage and the mitigators often have uncertainty about their knowledge of the social network [6]. Figure 1, for example, shows a realistic social network for the leadership of a set of local villages in Afghanistan [6]. Given real-world information constraints, the counterinsurgency team may not have perfect information of the graph and be uncertain about some set of edges.

In our work, the mitigator’s uncertainty about the graph structure is modeled as a Bayesian game with each Bayesian type representing a separate instantiation of the graph. The mitigator’s strategy must now reason over the distribution of types. The influencer’s (insurgent’s) perfect knowledge of the graph structure allows him to specify a behavioral strategy which conditions the strategy used on the specific type. This results in Bayesian games with an exponential number of types where each game is already extremely challenging to solve efficiently. We aim to address this class of problems efficiently and effectively.

Figure 1: Example Afghani leadership network

2. RELATED WORK
Recent work in game-theoretic security allocation have also dealt with domains that were modeled as graphs [1, 7, 4], however their actions were all deterministically defined and did not feature a probabilistic contagion component. The work in uncertainty in security games is also relevant [8, 10, 15], but once again do not feature the contagion component found in our domain.

This contagion process has been studied outside of the security
games literature and is known as influence maximization, in which a player attempts to optimize a selection of beginning ‘seed’ nodes from which to spread his influence in a known graph. This class of problems were first introduced as a discrete maximization problem by Kempe et al. (2003) who showed submodularity of the maximization problem, enabling a major dimension of difficulty. Specifically, because the uncertainty occurs over graph instances, the number of influencer types can be exponentially large. Since each individual game is already very challenging to solve as per Tsai et al. 2012, exponentially many of them exacerbates this challenge. Handling this uncertainty efficiently and effectively remains a major open challenge to real-world application of these techniques.

4. CHALLENGE

Though these Bayesian counter-contagion games are zero-sum and, therefore, amenable to linear programming solutions, the asymmetric information component adds a major dimension of difficulty. Specifically, because the uncertainty occurs over graph instances, the number of influencer types can be exponentially large. Since each individual game is already very challenging to solve as per Tsai et al. 2012, exponentially many of them exacerbates this challenge. Handling this uncertainty efficiently and effectively remains a major open challenge to real-world application of these techniques.

5. REFERENCES