ITM Web of Conferences **12**, 03001 (2017) DOI: 10.1051/itmconf/20171203001
ITA 2017

Computing Optimal Mixed Strategies for Terrorist Plot Detection Games with the Consideration of Information Leakage

MingChu Li[1a] , Zekun Yang[2b], Kun Lu*[3c], Cheng Guo*[4d]

[1]*School of Software Technology， Dalian University of Technology, Dalian, China*
[2]*School of Software Technology， Dalian University of Technology, Dalian, China*
[3]*School of Software Technology， Dalian University of Technology, Dalian, China*
[4] *School of Software Technology， Dalian University of Technology, Dalian, China*
[a]*mingchul@dlut.edu.cn,* [b]*zekunnyang@gmail.com,* [c]*lukun@dlut.edu.cn,* [d]*guocheng@dlut.edu.cn*

Abstract: The terrorist's coordinated attack is becoming an increasing threat to western countries. By monitoring potential terrorists, security agencies are able to detect and destroy terrorist plots at their planning stage. Therefore, an optimal monitoring strategy for the domestic security agency becomes necessary. However, previous study about monitoring strategy generation fails to consider the information leakage, due to hackers and insider threat. Such leakage events may lead to failure of watching potential terrorists and destroying the plot, and cause a huge risk to public security. This paper makes two major contributions. Firstly, we develop a new Stackelberg game model for the security agency to generate optimal monitoring strategy with the consideration of information leakage. Secondly, we provide a double-oracle framework DO-TPDIL for calculation effectively. The experimental result shows that our approach can obtain robust strategies against information leakage with high feasibility and efficiency.

1. Introduction

In the past few years, an increasing threat is originated from the terrorist organization, which is continually training and directing their supporters to launch coordinated attacks in their home countries, especially in European countries. To detect and thwart such attacks, domestic security agencies need to allocate security resources to monitor potential terrorists. Among all of the important factors, confidentiality is a basic requirement for security stuff during executing the monitoring task. A spotted security stuff cannot collect information from alerted terrorists, he will be even cheated by intentional terrorists with wrong information. Hence, the security agency fails to monitor the plot, which results in a huge risk to public security. Unfortunately, the security agency probably leak their information unconsciously. For example, Snowden[1] whose disclosure revealed several classified program of NSA. Consequently, the defender strategies become fragile and easy to attack. To sum up, designing robust strategy against the leakage becomes crucial to security agencies.

Recent years, security game theory has been widely used to protect large scale critical infrastructure and targets such as airport [2], transportation network [3], coast ports [4], etc. Coordinated attack is a rising hotspot for academic research, there are already some literature about this problem. There has been some research [5, 6] on security game mechanism against coordinated attack. For example, Wang et al. [5] proposed a Terrorist Plot Detect(TPD) game model for security agencies to monitor the potential terrorists. Guo et al.[6] introduced a coalitional security game (CSG) to address the issue that attackers can form coalitions that can dramatically increase their ability to achieve malicious goals. Most of the models of Stackelberg security games assume the attacker is not able to observe the defender's real-time pure strategy, so the attacker makes decision only based on his knowledge about the defender's mixed strategy. However this assumption cannot explain the leakage we mentioned above. The information leakage effect was ignored in most of the literature about coordinated attacks. Xu et al. [7] first introduced the concept of "information leakage"(IL) in security game domain, they also discussed the model and the computation of the leakage in the simplest defender-attacker security game. However, the effect of the information leakage in other security game setting are missing in the present study, and the efficient algorithms to handle it in the specify case still needs to be investigated.

This paper develops the optimal defender strategy in Terrorist Plot Detect game taking the information leakage into account. In the presented model, the information leaks as the attacker can discover specific terrorists' monitoring information. For the sake of simplicity, we assume that at the same time there is only

© The Authors, published by EDP Sciences. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (http://creativecommons.org/licenses/by/4.0/).

one terrorist's monitoring information that can be leaked, but all terrorists in the network have the probability to discover its monitoring status.

The rest of the paper is organized as follows. In section 2 we give a brief introduction to the TPD models, then we propose our TPDIL (Terrorist Plot Detect game considering Information Leakage) model. In section 3, a DO-TPDIL (Double Oracle algorithm for TPD games considering Information Leakage) framework is proposed based on double-oracle framework to solve the problem efficiently. Our experiments in section 4 show that the model can decrease the loss of defender's utility, which verify the feasible of our approach.

2. Model

In this section, firstly, we will introduce the Terrorist Plot Detect(TPD) game model proposed by Wang et al.[5]. Then we will give the Terrorist Plot Detect game with the consideration of Information Leakage (TPDIL) model and LP formulation to calculate the optimal strategy for defender given the probability of IL.

2.1 TPD Game Model

As introduced by Wang et al. [5], a Terrorist Plot Detect(TPD) game is a Stackelberg game between a leader (security agency, defender) and a follower (terrorist plot planner, attacker). The defender first allocates R resources to monitor the attacker's social network $G=(V,E)$, where V is the set of vertices(potential terrorists) and E is the set of edges(relations between terrorists). Then the attacker chooses a connected subgraph to launch a coordinated attack based on his knowledge of the defender schedule. The defender's pure strategy $S=\langle S_v\rangle$ is a $|V|$ -dimensional 0-1 vector of R monitoring resources, and defender will monitor terrorist i if $S_i=1$ an $\text{å}_{i\hat{\text{I}}V} S_i = R$. The defender's mixed strategy is a probability distribution over pure strategies, $x=\langle x_S\rangle$, x_S is the probability that pure strategy S is played, and $\text{å}\ x_S=1$. The attackers pure strategy is a connected subgraph $V'\hat{\text{I}}\ V$ denoted by a 0-1 vector $A=\langle A_i\rangle$, $A_i=1$ means terrorist $i\,\hat{\text{I}}\ V$ will attend the plot, 0 otherwise. The attacker's mixed strategy is denoted by a probability distribution $y=\langle y_A\rangle$, and y_A is the probability of playing attacker pure strategy A .

The utility of TPD game is defined as follows: TPD game is a zero-sum game, the attacker gains exactly the defender loses. Given a defender allocation S and an attacker subgraph A , if there is no intersection between S and A , i.e., $S\ ?\ A\quad ?$, which means the defender fails to detect the plot, the attacker will win $P(A)$. $P(A)$ is a subgraph utility function and the definition can be found in [5], the defender's cost is $-\ P(A)$. Otherwise the defender wins and the reward of destroying the plot is 0, attacker's utility is also 0.

Without information leakage, given the attacker's strategy space A and the defender's strategy space S , the defender's optimal mixed strategy can be calculated by the following linear programming(LP) (1) formulation.

$$\begin{array}{lll} \max & U & \\ s.j. & U\ ?\ U_d(x,A) & A\ ?\ \text{A} \\ & \underset{s\hat{\text{I}}\,\text{s}}{\text{å}}\ x_S = 1 & \\ & x_S\ ?\ 0 & S\ ?\ \text{S} \end{array} \qquad (1)$$

2.2 Model of Information Leakage

Xu et al. [7] introduced the two related IL model: PRobabilistic Information Ieakage (PRIL) model and ADversarial Information Leakage (ADIL) model. Let $p_i(p_i\ ^3\ 0)$ denote the probability that vertex i's "monitoring status" is being leaked, in other words, attacker is aware of whether terrorist i is being watched or not. With probability $p_0 = 1-\ \text{å}_{i\hat{\text{I}}V}\,p_i$, no vertices leak information. In PRIL model, every single vertex has probability to leak its information, thus we have a $(n+1)$ -dimensional probability vector $\overset{\text{r}}{p}=(p_0,p_1,...,p_n)$ where $n=|V|$. $\overset{\text{r}}{p}$ is usually given by domain experts and may be determined by the nature or capability of terrorists. ADIL is a special case that only one chosen vertex 's status is being leaked, let i be the vertex, then $p_i > 0$, for any v构$i,v\quad 0$, $p_v=0$, and $p_0 = 1-\ p_i$. This model captures the fact that few attacker own counter-reconnaissance or surveillance ability. With certain probability, they succeed in observing a specific high-value vertex's status, like the ringleader of the plot or someone who has been arrested before.

In a simplest TPD game, let $t_{iu}(\text{Ø}t_{iv})$ denote the status that terrorist i is being monitored (not being monitored). The defender's utility of PRIL model is defined as Eq.(2) :

$$DefU = p_0u_0 + \overset{n}{\underset{i=1}{\text{å}}}\ p_i(u_i+v_i) \qquad (2)$$

where $u_0 = \min_{A_k} U_d(x,A_j)$ is the defender's utility when there is no information leakage. The defender's utility when terrorist i leaks out its monitoring status as t_i ("being watched") is defined as Eq.(3):

$$u_i = \min_{A_k}[U_d(x_{iu},A_k)Pr(x_{iu}\,|\,t_{iu})] \qquad (3)$$

And the defender's expected utility when target i leaks as status $Øt_i$ (i.e., not being monitored) is defined as Eq.(4) :

$$v_i = \min_{A_k}[U_d(x_{iv}, A_k)Pr(x_{iv} \mid t_{iv})] \qquad (4)$$

Which means that defender choose the minimax strategy to minimize attacker's best response.

Given a defender mixed strategy x and a attacker's pure strategy A, let $U_d(x, A)$ denote defender's payoff. According to the definition, $U_d(x, A) = \text{å}\ x_S U_d(S, A)$, and $U_d(S, A) = P(A)$ if the vertices in S fails to overlap the nodes in A, otherwise $U_d(S, A) = 0$. Given a defender mixed strategy $x = \langle x_S \rangle$, let $x_u\,(x_v)$ denote the defender's mixed strategy probability distribution after observing t_{i*} (* = u or v)., the new distribution can be calculated as follows.

$$x_{*S} = \frac{x_S \Pr(x_S \mid t_{i*})}{\text{å}\ x_S \Pr(x_S \mid t_{i*})} \qquad (5)$$

Notice that comparing to the simplest security game discussed in [7], the leakage message(only one node's status) in TPDIL is the same. However, instead of considering the number of targets, the defender now have to take a much more complex attacker strategy space, which grows up in an exponential way, into consideration. A direct challenge is that we can't use the origin compact matrix representation in [7], because the marginal coverage probability is helpless to describe the relationship between both player's pure strategy in our model. The ADIL model is defined in a similar way. Let terrorist i denote the special terrorist whose monitoring status is being leaked, $DefU = p_0u_0 + (1- p_0)(u_i + v_i)$, where u_i and v_i is defined as above.

2.3 Equilibrium

Under zero-sum condition, the Stackelberg equilibrium (SSE) is equivalent to maximin equilibrium and minimax equilibrium, thus the optimal defender mixed strategy x in TPDIL game can be calculated by solving the following LP(6).

$$\begin{array}{lll}
\max & p_0u_0 + \sum_{i=1}^{n} p_i(u_i + v_i) & \\
s.j. & u_0 \le U_d(x, A) & \forall A \in \mathcal{A} \\
 & u_i \le \min_A(U_d(x_{iu}, A)\Pr(x_{iu} \mid t_{iu})) & \forall A \in \mathcal{A} \\
 & v_i \le \min_A(U_d(x_{iv}, A)\Pr(x_{iv} \mid t_{iv})) & \forall A \in \mathcal{A} \\
 & \sum_{S \in \mathcal{S}} x_S = 1 & \\
 & x_S \ge 0 & \forall S \in \mathcal{S}
\end{array}$$

(6)

However, the LP(6) contains $(2|L|+1)\times|X|\times|Y|$ restrains, where $|L|$ is the number of information leakage cases, in our model, is the network size $|V|$. The $|X|$ stands for the defender strategy space S , which grows exponentially with the number of resources R, and $|Y|$ is the attacker strategy space, which grows exponentially with $|V|$. As a result, it is impractical to directly to solve this LP.

3. Approach

As we discussed above, both player's strategy space grows in the exponentially way, which make solving the problem in a large scale network become impractical. The double oracle framework is a normal form for solving zero-sum games with large strategy space. To solve the TPD game in a real-world scale network, Wang et al. [5] presented an algorithm DO-TPD(an Double Oracle algorithm for TPDs) to obtain solution for both players. DO-TPD initials with solving the equilibrium with a small and limited game, then both player compute the improving strategies and add them to the strategy space iteratively, and finally the solution meets the global equilibrium when no improving strategies can be found. However, the solutions obtained from DO-TPD don't consider the information leakage. We extend DO-TPD to DO-TPDIL(an Double Oracle algorithm for TPD games considering Information Leakage) in a novel way. Next, we start with an overview of DO-TPDIL, and then present its components.

3.1 DO-TPDIL Overview

Our DO-TPDIL algorithm is sketched in Algorithm 1. DO-TPDIL also initials the small strategy space $\langle S', A' \rangle$ by solving the linear program LWA-LP presented by Wang et al.[5], where the attacker is restricted to use "lone-wolf" attack represented as a single vertex. In the initialization procedure, the game degenerates to the simplest form of security game because the attacker ignores the network structure. The defender strategy can be represented by marginal coverage probability of each vertex, and the mixed strategy can be efficiently sampled with Comb Sampling algorithm[8].

Algorithm 1 DO-TPDIL overview

```
Initialize $S'$ , and all $A_i \subset A_{\cup}'$ using $LWA$-LP
repeat
    $(x, y_{\cup}) \leftarrow CoreLP(S', A_{\cup})$
    for leak case $i$, $x_i \subset x$, $y_i \in y_{\cup}$ do
        $S^+ \leftarrow betterOD(x_i, y_i)$
        if $S^+ = \emptyset$ then
            $S^+ \leftarrow bestOD(x_i, y_i)$
        $S' \leftarrow S' \cup S^+$
        $A_i^+ = attackerOracle(x_i, y_i)$
        $A_i = A_i \cup A_i^+$
        $A_{\cup} = A_{\cup} \cup A_i^+$
until $S^+ = \emptyset$ and $A_i^+ = \emptyset$ for all leak case $i$
return $(x, y_{\cup})$
```

Here we regard t_{iu} and t_{iv} as two separated cases, thus there are totally $2|V|+1$ possible cases. Let A_i denotes the attacker's best response in each case i, then we have $A_{\cup'} = A_0 \cup A_1 \cup \cdots \cup A_{2n}$, where A_0 is the attacker's response with no leakage, i.e., the origin attacker's solution in TPD. Then DO-TPDIL solves CoreLP with the above restricted strategy space. The attacker's strategy space $A_{\text{È}}$' has only $|V|$ strategies first, so the restricted CoreLP can be solved efficiently. Obviously, the "restricted version" solution is not enough to form the origin TPDIL's SSE solution. To improve both player's utilities, DO-TPDIL calls the subsequent oracles to find improving strategies. The process repeats until no improving strategies can be found in all case, and the obtained solution is a minimax equilibrium solution [9], and is equivalent to SSE and NE strategies in zero-sum game [10].

3.2 CoreLP

The CoreLP in TPDIL is computed as follows. Firstly, the defender computes its mixed strategy x against $A_{\text{È}}$' by solving LP(1) with S = S¢ and A = $A_{\text{È}}$. Then the attacker updates all the A_i Î $A_{\text{È¢}}$ respectively. Specifically, let case j denote the case t_{iu} (t_{iv}), i.e., the terrorist i leaks as being monitored (not being monitored). The attacker first incurs the defender strategy space S_j which only contains the defender pure strategy that can be used in case j. S_j can be calculated by Eq.(5). Then he can obtain his optimal mixed strategy y_i in this case by solving LP(1) with S = S_j and A = A_i . $y_{\text{È}}$ is the collection of the attacker's mixed strategy probability distribution in each case.

3.3 Defender Oracle

The goal of the defender oracle is to find pure strategy that can improve the player's utility, however finding the improving strategy is different between TPD game and TPDIL game. One problem is that the solution generated by the defender oracle in DO-TPD may be pointless in a specific leakage case. For example, if the attacker observes the case t_{iu} , then a defender pure strategy that doesn't contain the leak point i will be meaningless. We need to add particular restrains in defender oracle to discard these invalid solution. Given a specific leakage case j and the related attacker's strategy space A_j , the best defender oracle in DO-TPDIL(denoted as bestOD) will solve the defender best oracle in DO-TPD[5] (denoted as TPD-*bestOD*) as the MILP (7).

The variables in this MILP have the same meaning with the TPD-bestOD, and the idea is that defender chooses an allocation which can overlap the attacker's subgraphs as much as possible. I is an 0-1 indicator, $I = 1$ when case j is terrorist i leaks as being monitored(i.e., t_{iu} case), and this ensures that the strategy can be used in case j to against the specific attacker A_j , and $I = 0$ is on the contrary(i.e., t_{iv} case). If there is no leakage, the defender will call LP(7) by removing the last restrain, and setting $A_j = A_0$.

$$\begin{aligned}
\max \quad & -\sum\nolimits_{A \in A_{\cup'}} (1 - Z_A) y_A P(A) \\
s.j. \quad & z_A \le \sum_{u \in V} A_u S_u \qquad\qquad \forall A \in A_j \\
& \sum_{u \in V} A_u S_u \le R \\
& S_u \in \{0,1\}, z_A \in [0,1] \\
& S_i = I
\end{aligned} \tag{7}$$

Unfortunately, the bestOD problem is still NP-hard, because the process still has to search the whole network to find the best response, including or excluding the leak point has a negligible effect on network scale. To speed up the oracle process, we propose a fast oracle called betterOD. The idea is finding some sub-optimal("better") solutions to meet the criterion $U_d(S,y) > U_d(x,y)$ in each leakage case, while it can be solved within much less time than bestOD process. The bestOD process only needs to be called when betterOD fails to find an answer.

3.4 Better OD

In our betterOD algorithm, we need to use the algorithm TPD-betterOD presented by Wang et al. [5]. The TPD-betterOD algorithm provides us an approach to find defender's sub-optimal strategy given attacker's mixed strategy y. Notice that, the defender searches the whole network to find pure strategy depends on attacker's mixed strategy y in TPD-*betterOD*. We add C as the candidate nodes range instead of the whole network to prevent pointless strategies which break the leakage precondition.

Our betterOD is shown in Algorithm 3. Firstly, the betterOD algorithm sets the candidate nodes, if the node leaks as case t_{iv} , then betterOD will restrict the candidate nodes as $C = V \setminus \{i\}$ to prevent meaningless strategies in lines 2~3. Secondly, betterOD calls TPD-betterOD to search strategy by selecting vertices that bring the maximum marginal utility in a greedy way. Finally, in t_{iu} case, if the strategies obtained from line 4 don't contain the leak point i , betterOD will discard these strategy and return the rest part.

Algorithm 3 *betterOD* (x, y, i)

```
1. $S_{better} = \emptyset$, $C = V$
2. if $i$ is leaked as $t_{iv}$ then
3.     $C = C \setminus \{i\}$
4. $S_{better}$ = TPD-betterOD$(x, y, C)$
5. if i is leaked as $t_{iu}$ then
6.     for all $S \in S_{better}$ do
7.     if $S$ doesn't contains leak point $i$ then
8.         $S_{better} = S_{better} \setminus \{S\}$
9. return $S_{better}$
```

3.5 Attacker Oracle(AO)

The attacker oracle algorithm for TPDIL works in the same way with DO-TPD. In each leakage case i , the attacker only considers the defender's probability distribution x_i after observing t_{iu} or t_{iv} . Then he will call the attacker better oracle to find improving strategies, if fail, he will turn to the attacker best oracle. The algorithm detail we refers to [5].

4. Experimental Evaluation

We evaluate the performance of our approach through extensive evaluations. All LP and MILP computations are solved by CPLEX 12.60.

All computations are run on a machine with 2.2 GHZ Intel qual core CPU and 8 GB memory. The parameters keep the same with [5]. All the experiments are run with the ADIL model. The leak point is random chosen from the network, and the $p_i = 0.5$ unless otherwise stated. All the results are sampled over 20 times.

Our experiments use the following three types of network: (i) Random trees (RT), where each new node is connected to a random picked existing node. (ii) Erdös-Rényi random graphs(ER(V, M)) [11], where M links are randomly assigned between all possible vertices pairs, we use the networks with $M = V$ labelled as ER(1). (iii) Barabási-Albert scale-free network(BA(k))[12], where each new node is connected to k existing nodes with the proportional to the edges the existing node already has, we use BA scale-free network with parameters $k = 1$ labeld as BA(1). By default, the capability of each vertex t_v is randomly chosen in [1, 5], and the network externality measure $d = 0.1$.

4.1 Scale-Up Analysis

In Figure. 2, we test our algorithm in different network. Results show that our algorithm can help to reduce the complexity of solving the problem. The naive FullLP's runtime increases in an exponentially way, and it runs out of memory when the network size is about 20. Our approach can help the player to solve the problem with the network size of 40.

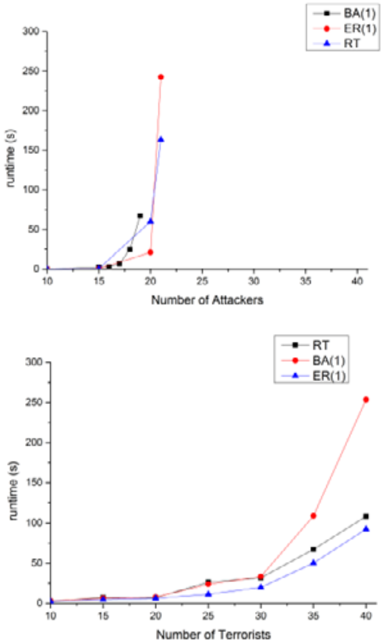

Figure 1. Runtime in different networks: (a)FullLP (b) DO-TPDIL approach.

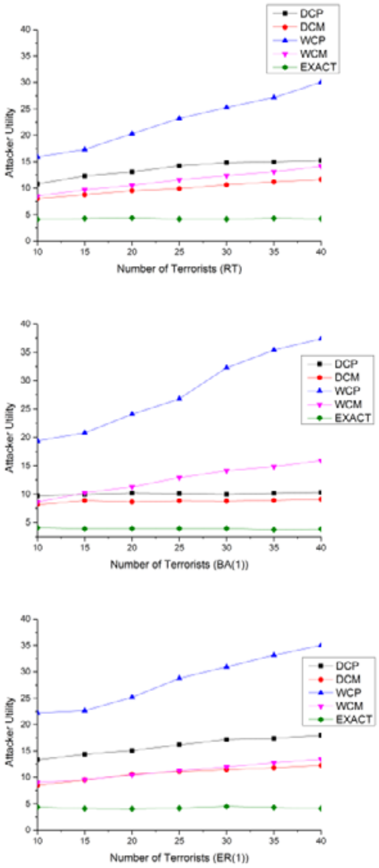

Figure 2. Attacker utility against different defenders (a) RT network, (b) BA(1) network, (c) ER network

4.2 Solution Quality Analysis

We use the following centrality measure based heuristic baselines proposed by [5] to evaluate the solution quality of our approach: (i) DCP: defender only monitors the vertices with top R degree values. (ii) DCM: a defender mixed strategy where the vertex marginal coverage probability is normalized degree centrality; (iii) WCP: defender only monitors vertices with top R node capability values. (iv) WCM: a defender mixed strategy where the vertex marginal coverage probability is normalized weight centrality. All the mixed strategies are sampled by Comb Sampling algorithm[8]. The result by our approach is denoted by line EXACT.

In Figure 2. , we compare the solution quality obtained from our approach and other 4 heuristic baselines. Results show that the solution obtained from the heuristic baselines performs badly in information leakage model, the performance becomes worse with the network size growing up. The defender utility from our approach can remain stable as the network grows, and the value indicates our approach's effectiveness. In all the three network, the mixed strategy (DCM, WCM) always performs better than the corresponding pure strategy. This shows the necessary of using randomized mixed strategy in TPD game even with the consideration of information leakage.

5. Conclusion

In this study, we considered partial information leakage in Terrorist Plot Detect games. We focused on the modeling and the computation of the new game to help defender decreasing the loss caused by leakage. We proposed an efficient double oracle framework to speed up finding efficient strategy, instead of searching strategy from the whole strategy space. The experimental results show the feasibility and efficiency of our approach.

Acknowledgment

This paper is supported by NSFC under grant numbers： 61272173， 61572095. Corresponding authors: Cheng Guo: guocheng@dlut.edu.cn, Kun Lu: lukun@dlut.edu.cn.

References

[1] Edward Snowden: Leaks that exposed US spy programme. http://www.bbc.com/news/world-us-canada-23123964

[2] J. Pita, M. Jain, J. Marecki, F. Ordóñez, C. Portway, M. Tambe, et al., "Deployed ARMOR protection: the application of a game theoretic model for security at the Los Angeles International Airport," in Proceedings of the 7th international joint conference on Autonomous agents and multiagent systems: industrial track, 2008, pp. 125-132.

[3] J. Tsai, C. Kiekintveld, F. Ordonez, M. Tambe, and S. Rathi, "IRIS-a tool for strategic security allocation in transportation networks," in AAMAS, 2009, pp. 37-44.

[4] B. An, F. Ordóñez, M. Tambe, E. Shieh, R. Yang, C. Baldwin, et al., "A deployed quantal response-based patrol planning system for the US Coast Guard," Interfaces, vol. 43, pp. 400-420, 2013.

[5] Z. Wang, Y. Yin, and B. An, "Computing Optimal Monitoring Strategy for Detecting Terrorist Plots," in AAAI, 2016, pp. 637-643.

[6] Q. Guo, B. An, Y. Vorobeychik, L. Tran-Thanh, J. Gan, and C. Miao, "Coalitional security games," in Proceedings of the 2016 International Conference on Autonomous Agents & Multiagent Systems, 2016, pp. 159-167.

[7] H. Xu, A. X. Jiang, A. Sinha, Z. Rabinovich, S. Dughmi, and M. Tambe, "Security games with information leakage: modeling and computation," presented at the Proceedings of the 24th International Conference on Artificial Intelligence, Buenos Aires, Argentina, 2015.

[8] J. Tsai, Z. Yin, J.-y. 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.

[9] H. B. McMahan, G. J. Gordon, and A. Blum, "Planning in the presence of cost functions controlled by an adversary," in ICML, 2003, pp. 536-543.

[10] Z. Yin, D. Korzhyk, C. Kiekintveld, V. Conitzer, and M. Tambe, "Stackelberg vs. Nash in security games: Interchangeability, equivalence, and uniqueness," in Proceedings of the 9th International Conference on Autonomous Agents and Multiagent Systems: volume 1-Volume 1, 2010, pp. 1139-1146.

[11] P. Erdös and A. Rényi, "On random graphs, I," Publicationes Mathematicae (Debrecen), vol. 6, pp. 290-297, 1959.

[12] A. L. Barabási and R. Albert, "Emergence of scaling in random networks," science, vol. 286, pp. 509-512, 1999.